# الجريمة في الإنترنت

## وطرق الحماية منها

أ.د عبدالقادر بن عبدالله الفنتوخ

obeikandl.com

ⓒ مكتبة العبيكان، ١٤٣٣هـ

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

الفنتوخ، عبدالقادر بن عبدالله

الجريمة في الإنترنت وطرق الحماية منها. / عبدالقادر بن عبدالله الفنتوخ. - الرياض،

١٤٣٣هـ

١٣٢ص، ١٦,٥×٢٤سم

ردمك: ٩-٩٥٣٣-٠٠-٦٠٣ ٩٧٨

١. جرائم الحواسيب ٢. جرائم الإنترنت أ. العنوان

ديوي: ٣٤٣,٠٩٩٩

رقم الإيداع: ١٤٣٣/٢٦٢٢

الطبعة الأولى

١٤٣٣هـ/٢٠١٢م

جميع الحقوق الفكرية والطباعية محفوظة للناشر

الناشر

العبيكان Obeikan

الرياض، المحمدية، طريق الأمير تركي بن عبدالعزيز الأول

هاتف: ٤٨٠٨٦٥٤ فاكس ٤٨٠٨٠٩٥، ص.ب: ٦٧٦٢٢ الرمز: ١١٥١٧

موقعنا على الإنترنت

www.obeikanpublishing.com

متجر العبيكان على آبل

http://itunes.apple.com/sa/app/obeikan-store

التوزيع: مكتبة العبيكان Obeikan

الرياض، العليا، تقاطع طريق الملك فهد مع شارع العروبة

هاتف: ٤١٦٠٠١٨ فاكس ٤٦٥٠١٢٩

ص.ب: ٦٢٨٠٧ الرمز: ١١٥٩٥

لا يسمح بإعادة إصدار هذا الكتاب أو نقله في أي شكل أو واسطة، سواء أكانت إلكترونية أو ميكانيكية، بما في ذلك التصوير بالنسخ (فوتوكوبي)، أو التسجيل، أو التخزين والاسترجاع، دون إذن خطي من الناشر.

obeikandl.com

obeikandl.com

obeikandl.com

# مقدمة

ارتبط التقدم والازدهار —منذ القدم- بوجود الأمن، فلا سبيل لمجتمع يطمح إلى تحقيق نهضة تنموية وعلمية واجتماعية أن يصل إلى مطامحه إلا بوجود هذه العامل الرئيس، وفي عصرنا الراهن تعددت أوجه الأمن، فلم يعد مقصوراً على مفهوم الأمن الحسي المتمثل في الحفاظ على النفس والمال، بل بات مألوفاً أن نسمع عن الأمن الغذائي، والأمن الفكري، والأمن الاقتصادي، والأمن المائي، وغير ذلك من تفريعات، غير أن أمناً جديداً أفرزته تطورات العلم الحديث المتسارعة، غدا من أهم عناصر الأمن في المجتمعات الحديثة، التي أصبحت التقنية وتطبيقاتها محور العملية الاقتصادية والصناعية والفكرية، ومن هنا نشأت المخاطر الأمنية التي تستهدف وسائل التقنية وأدواتها ولاسيما تطبيقات الحاسب الآلي وشبكة الإنترنت التي تعد عصب الحياة المعرفية في وقتنا الراهن، فكثيراً ما حدثتنا الأخبار عن هجمات أو اختراقات تحدث أضراراً اقتصادية فادحة لبعض الجهات الحكومية أو الشركات العالمية أو حتى الأفراد، مما حدا بالمجتمع العالمي إلى تجريم هذه الأفعال وعدها جريمة خطيرة؛ تفوق أبعادها خطورة الجريمة التقليدية، فهي تتم بأيسر الوسائل وأهون الطرق، ولكن ضررها قد لا يحصى في حالات معينة، ولذا نشأ مفهوم أمن المعلومات ليكون دليلاً على أهمية الحفاظ على الممتلكات الواقعة في فضاء العالم الإلكتروني، وضرورة توفر عناصر الأمان فيه ليحقق راحة للمستخدم، وحرية للحياة الاقتصادية والمعرفية، وتقدماً علمياً يُسجَّل للحضارة البشرية جمعاء.

وضمن هذا الإطار يأتي كتاب (الجريمة في الإنترنت وطرق الحماية منها) ليقدم للقارئ العربي، صورة واضحة عن أبعاد المسألة الأمنية في الشبكة العنكبوتية، فيعرف بمفهوم الجريمة الواقعة في فضاء الإنترنت، ويحدد أسبابها ودوافعها، ثم يذكر أهم طرق الحماية منها، أو معالجتها.

ولهذا يعدّ الكتاب مكملا للجهود السابقة في بيان بعض جوانب الجريمة في الإنترنت. ورفدا للمكتبة العربية في مجال أمن المعلومات.

obeikandl.com

# المحتويات



obeikandl.com

obeikandl.com

## الفصل السابع : أدوات الجريمة



## الفصل الثامن : مراحل الاختراق



## الفصل التاسع : الشبكات الاجتماعية والسرية المفقودة



obeikandl.com

## الفصل العاشر : متطلبات الحماية للأجهزة الشخصية



## الفصل الحادي عشر : الحماية في القطاعات والمؤسسات



## الفصل الثاني عشر : ماذا يخبئ المستقبل على الإنترنت؟



## الفصل الثالث عشر : القوانين الدولية لمكافحة جرائم الإنترنت



obeikandi.com

# تمهيد

الجريمة ظاهرة اجتماعية تنخر المجتمعات المتخلفة والمتقدمة على حد سواء، فلا وجود لمجتمع خالٍ من السلوك الانحرافي أو من الجريمة. ومعلوم أن الجريمة لم تتخلف عن مرافقة بني الإنسان منذ هبوطه الأرض، بل واكبت تطوره وتأقلمت مع ظروفه، فبعد أن أُشرع باب الجرائم بحجر، صار القيام بأخطرها في عصرنا يتم بضغطة زر صغير من جهاز حاسب آلي.

وإذا كانت الجريمة بمعناها الواسع هي كل مخالفة لقاعدة من القواعد التي تنظم سلوك الإنسان في الجماعة؛ فإن لها العديد من الأبعاد والأوصاف المأخوذة من العلوم والشريعة.

**فالجريمة لغة**: من الجُرْم وهو التَّعدِّي والذنب، وكذا هي الكسب والقطع[1].

وقد عرَّف الماوردي الجريمة في الشريعة الإسلامية: الجرائم محظورات شرعية زجر الله عنها بحدٍّ أو تعزير[2].

وأما من الناحية القانونية، فقد عرَّف الجريمة الدكتور نجيب حسني بالقول: هي فعل غير مشروع صادر عن إرادة جنائية يقدر له القانون عقوبة أو تدابير[3]. وهي تشمل المخالفات والجنح والجنايات وهذه الأخيرة أشدها خطورة وأقساها عقوبة؛ وخصّ الفقهاء لفظ الجناية بما يقع على النّفس والأطراف، ولفظيّ الغصب والسّرقة بما يقع على المال، ولذا فالجريمة أعمّ من الجناية.

في حين نظر علم الاجتماع إلى الجريمة، فوجدها تعبيراً عن الصراع بين الفرد والظروف المحيطة به. ومن هذه النظرة نجد أن الركن الرئيس في الجريمة هو المجرم؛ ذاك الإنسان الذي

١ لسان العرب، مادة (جرم).
٢ الأحكام السلطانية، الإمام الماوردي، دار الكتب العلمية.
٣ شرح قانون العقوبات، محمود حسني، دار النهضة العربية.



obeikandl.com

يقدم على ارتكاب الجريمة سواء بالفعل، أو القول، أو التحريض، ودون إغفال الأركان الباقية، وهي: متضرر (مجني عليه)، وأداة الجريمة، ومكانها، وزمانها.

غير أن التطور المعرفي والتقني أرخى سدوله على الجريمة أيضًا، فانزاحت حدود الجريمة وأركانها التقليدية، وأصبحت تتخذ فضاءً افتراضيًا مسرحًا لها، فتلاشت أهمية المكان، واضمحلت قيمة الزمان.

وبانعقاد لقاء الجريمة مع الجانب المظلم من المعرفة والتطور، نتج ما اصطلح على تسميته بالجرائم الإلكترونية، ومنها نتج فرع يعرف بالجريمة في الإنترنت، ويمكن لنا تعريفها بالآتي: هي كل أشكال السلوك غير المشروع الذي يُنفَّذ باستخدام الوسائط الحاسوبية وشبكات الإنترنت لارتكاب جريمة أو التخطيط لها.

وأمّا العنصر الفاعل والمؤثر، فهو المجرم المعلوماتي الذي يوصف بأنه مجرم متخصص ذو قدرة كبيرة في المهارة التقنية، ويستغل مداركه ومهاراته في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية، وغيرها من الجرائم بغية المال، أو لمآرب أخرى.

فيما يكوّن جهاز الحاسب والإنترنت أداة الجريمة التي لا تبدو عليها -في كثير من الأحيان- بقايا آثار الجريمة. ويكمن دور الحاسب بكونه النافذة التي يلج منها المجرم المعلوماتي، فيما تمثّل شبكة المعلومات (الإنترنت) مسرح الجريمة.

وتقدم الإحصاءات عن الجريمة في الإنترنت واقعاً خطيراً يستلزم العمل بجد للحد من مخاطره، وعلى الرغم من وجود الكثير من الإحصائيات المتعلقة بموضوع الجريمة على الإنترنت إلا أنه من المتفق عليه بأن هذه الإحصائيات لا تعكس وضع الجريمة في الإنترنت بشكل سليم، وذلك لسببين رئيسين:

١- **اكتشاف الجريمة**: فالكثير من الجرائم في الإنترنت لا يتم اكتشافها، ومن ثم فإنه من الصعب إدخال هذه الفئة من الجرائم في الإحصائيات.



obeikandl.com

٢- **التبليغ عن الجريمة:** ففي أحيان كثيرة يتم اكتشاف الجريمة، غير أن الجهة المتعرضة لها لا تقوم بالتبليغ عنها خوفا على سمعتها أو لأي سبب آخر.

وعلى الرغم من أن هذين العاملين لهما دور في جعل الإحصائيات لا تعكس الحجم الحقيقي للجريمة على الإنترنت، فإن الإحصائيات المتوفرة حاليا، توضح انتشارها بشكل متزايد وملفت للنظر، مما يجعل المرء يتساءل ما هو الواقع الفعلي لانتشار الجريمة على الإنترنت ؟

وتظهر بعض الإحصائيات المتعلقة بمجال الجريمة في الإنترنت، ومجال حماية المعلومات، أرقاماً تستحق الوقوف عندها والتبصر بها، ففي الإحصائية المهمة التي أجراها معهد أمن الحاسبات (Computer Security Institute) (CSI)، والمختصة لجرائم وأمن الحاسب لعام ٢٠١٠/٢٠١١م، التي تستند نتائجها على ردود (٣٥١) ممارس أمن كومبيوتر في الشركات الأمريكية، والأجهزة الحكومية، والمؤسسات المالية، والمؤسسات الطبية، والجامعات من أصل (٥٤١٢) تم التواصل معهم.

تبيّن الإحصائية على سبيل المثال للعام ٢٠٠٨ أن حوادث أمن الكومبيوتر الأكثر تكلفة وإهدارًا للمال كانت المعنية بالاحتيال المالي الذي كان متوسط الخسارة فيها (٥٠٠,٠٠٠$). بينما كان متوسط الخسارة السنوية المبلغ عنها حوالي (٣٠٠,٠٠٠$).

وأظهرت الإحصائية أن حوادث الإصابة بفيروسات الحاسب كانت المتسبب الأكبر في حدوث مشاكل تقنية نتج عنها خسائر مادية لـ(٤٩ ٪) من المنظمات المستهدفة. ثم يلي ذلك استخدام الشبكات بنسبة (٤٤٪)، فسرقة الحواسب النقالة والأجهزة النقّالة الأخرى بنسبة (٤٢ ٪).

ومما جاء فيها أيضا أن واحدة من كل عشْر منظمات ذكرت بأنّها تعرضت لحادثة متعلقة بملكية اسم النطاق (DNS) بزيادة حوالي ٢ ٪ عن٢٠٠٧م، كما يتضح في جدول (١).

وتذكر الأغلبية المشاركة في المسح الخاص بتلك الإحصائية أن منظماتهم تمتلك سياسات



obeikandl.com

منية داخل منظماتهم (٦٨ ٪)، وأن (١٨ ٪) من المنظمات كانت تطوّر سياسة أمن معلومات رسمية. فيما لم تتعد (١٪) نسبة من قال بأنّهم ليس لديهم سياسة أمن. انظر الجدول (١).

| نوع العملية | ٢٠٠٤ | ٢٠٠٥ | ٢٠٠٦ | ٢٠٠٧ | ٢٠٠٨ | ٢٠٠٩ | ٢٠١٠ |
|---|---|---|---|---|---|---|---|
| تعطيل الخدمة | ٣٩٪ | ٣٢٪ | ٢٥٪ | ٢٥٪ | ٢١٪ | ٢٩٪ | ١٧٪ |
| سرقة الحاسب المحمول | ٤٨٪ | ٤٨٪ | ٤٧٪ | ٥٠٪ | ٤٢٪ | ٤٢٪ | ٣٤٪ |
| سوء استخدام الاتصالات | ١٠٪ | ١٠٪ | ٨٪ | ٥٪ | ٥٪ | | |
| الوصول غير المصرح به | ٣٧٪ | ٣٢٪ | ٣٢٪ | ٢٥٪ | ٢٩٪ | | |
| الفيروسات | ٧٨٪ | ٧٤٪ | ٦٥٪ | ٥٢٪ | ٥٠٪ | | |
| سوء الاستخدام المالي | ٨٪ | ٧٪ | ٩٪ | ١٢٪ | ١٢٪ | ٢٠٪ | ٩٪ |
| سوء الاستخدام الداخلي | ٥٩٪ | ٤٨٪ | ٤٢٪ | ٥٩٪ | ٤٤٪ | ٣٠٪ | ٢٥٪ |
| اختراق النظام | ١٧٪ | ١٤٪ | ١٥٪ | ١٣٪ | ١٣٪ | | |
| التخريب | ٥٪ | ٢٪ | ٣٪ | ٤٪ | ٢٪ | | |
| سرقة/ فقدان معلومات الملكية | ١٠٪ | ٩٪ | ٩٪ | ٨٪ | ٩٪ | | |
| من الأجهزة النقالة | | | | | ٤٪ | ٦٪ | ٥٪ |
| من المصادر الأخرى | | | | | ٥٪ | ٨٪ | ٥٪ |
| سوء استخدام الشبكات اللاسلكية | ١٥٪ | ١٦٪ | ١٤٪ | ١٧٪ | ١٤٪ | ٨٪ | ٧٪ |
| تشويه موقع الانترنت | ٧٪ | ٥٪ | ٦٪ | ١٠٪ | ٦٪ | ١٤٪ | ٧٪ |
| سوء استخدام تطبيقات الويب | ١٠٪ | ٥٪ | ٦٪ | ٩٥٪ | ١١٪ | | |
| البرامج الآلية bots | | | | ٢١٪ | ٢٠٪ | ٢٣٪ | ٢٩٪ |
| هجمات DNS | | | | ٦٪ | ٨٪ | ٧٪ | ٢٪ |
| سوء استخدام الرسائل الفورية | | | | ٢٥٪ | ٢١٪ | ٨٪ | ٥٪ |
| اشتقاق كلمة المرور | | | | ١٠٪ | ٩٪ | ١٧٪ | ١٢٪ |
| سرقة/ فقدان بيانات العملاء | | | | ١٧٪ | ١٧٪ | | |
| من الاجهزة النقالة | | | | | ٨٪ | ٥٪ | ٦٪ |
| من المصادر الاخرى | | | | | ٨٪ | ١٠٪ | ١١٪ |

جدول (١) أنواع الاختراقات ونسبها من عام ٢٠٠٤ وحتى ٢٠١٠

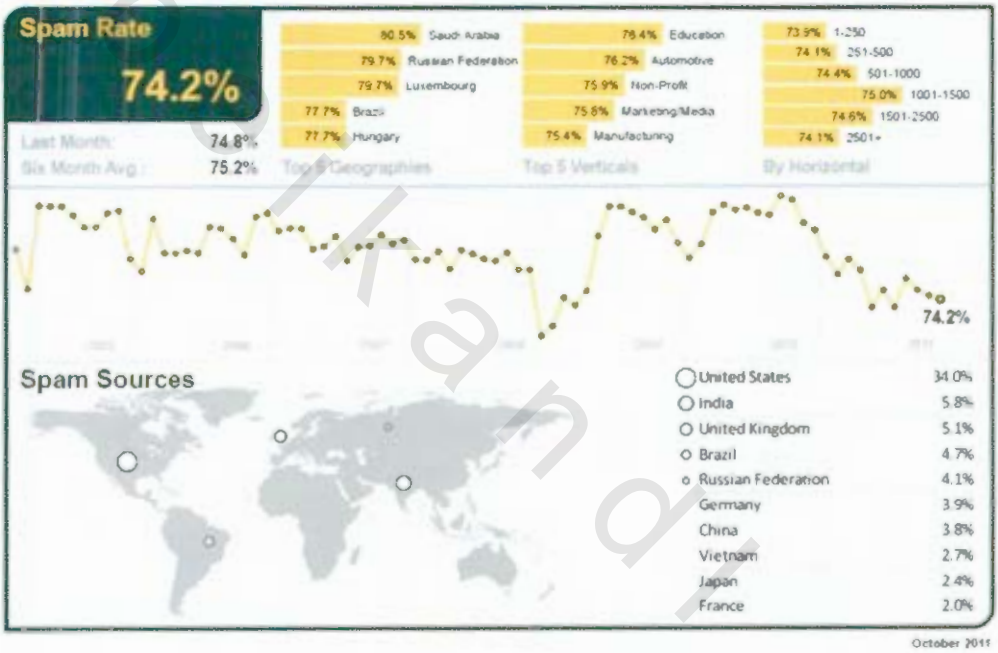
وجاء في التقرير أيضاً؛ أن (الحرب الباردة الإلكترونية) التي تشن على أجهزة الكمبيوتر في العالم تنذر بالتحول إلى أحد أكبر التهديدات الأمنية خلال العقد المقبل. ونوّه التقرير إلى أن نحو ١٢٠ دولة تقوم بتطوير طرق لاستخدام الإنترنت كسلاح لاستهداف أسواق المال ونظم الكمبيوتر والخدمات التابعة للحكومات، مضيفاً أن أجهزة المخابرات تقوم بالفعل باختبار شبكات الدول الأخرى بصورة روتينية بحثاً عن ثغرات وأن أساليبها تزداد تطوراً كل سنة.



obeikandl.com

وذكر التقرير أن الصين في صدارة الحرب الإلكترونية، وأن اللوم ألقي عليها في هجمات على الولايات المتحدة والهند وألمانيا، وتنفي الصين هذه المزاعم بصورة متكررة.

وأما على صعيد المنطقة العربية فقد جاء في إحصائية شهر أكتوبر ٢٠١٠ من التقرير الدوري لشركة سيمانتك، أن المملكة العربية السعودية هي أكثر دول العالم تعرضاً للرسائل الاقتحامية.




الشكل (١) إحصائية شركة سيمانتك حول الرسائل الاقتحامية

وعلى الرغم من اختلاف معدلات الرسائل الاقتحامية (SPAM) بحسب الموقع الذي يتم القياس فيه، إلا أن هذه الرسائل تمثل مشكلة خطيرة في المملكة. وبناء على المعلومات التي جمعها مقدمو خدمة الإنترنت، فإن معدل رسائل البريد الإلكتروني الاقتحامية في المملكة كان ٥٤٪. بينما أفادت مصادر أخرى، كموردي منتجات مكافحة الرسائل الاقتحامية، أن نسبة تلك الرسائل تتراوح بين ٤٠٪ - ٦٠٪. وعلى سبيل المثال، فإن التقارير المنقولة عن سيمانتيك

(Symantec) تفيد أن نسبة الرسائل الاقتحامية (SPAM) كانت ٥٩٪ في عام ٢٠٠٦م، بينما أفادت تقارير (Message Labs) أن الرسائل الاقتحامية (SPAM) في عام ٢٠٠٦م شكلت ٤٨٪ وفي عام ٢٠٠٧م (لغاية يوليو) شكلت ٤٣٪ من إجمالي عدد الرسائل المستلمة. وفي المقابل فإن الرسائل الاقتحامية (SPAM) المرسلة بالفاكس لم تعد بأنها مصدر رئيس للرسائل الاقتحامية، ومعدل إرسالها يقل عن ٦٪. وتشكل الرسائل التسويقية المباشرة النوع الرئيس من الرسائل الاقتحامية (SPAM) المستلمة في المملكة، وهذا يعكس الأغلبية العظمى للرسائل الاقتحامية التجارية على مستوى العالم. وبالنسبة للرسائل القصيرة الاقتحامية، فقد أفاد مشغلو خدمة الجوال أنها تشكل ما معدله ١,٧٪، حيث إن ٦٥٪ من هذه الرسائل النصية القصيرة هي تجارية، ٢٠٪ بذيئة، ٢٪ سياسية، ٣٪ دينية، ٥٪ تتعلق بأسواق الأسهم و٥٪ ذات أغراض أخرى[١].

وفي إحصائية عام ٢٠٠٧ لشركة (ترينـد مايكرو) الشهيرة في مجال الحماية ومحاربة الفيروسات، ورد أن السعودية والإمارات احتلتا المركزين الأول والثاني على التوالي على مستوى دول مجلس التعاون الخليجي في التعرض للجرائم الإلكترونية، إذ أشار التقرير إلى وجود أكثر من ٧٠٠ ألف حالة انهيار نظامي خلال تسعة شهور فقط في السعودية وحدها، بحيث بلغت السعودية المركز الأول بنسبة تصل إلى ٦٤٪، تلتها الإمارات بنسبة ٢٠٪. وتفيد توقعات بعض الخبراء والمحللين بأن الجرائم الإلكترونية قد تتسبب بخسارة دول مجلس التعاون الخليجي (٥٥٠ -٧٣٥) مليون دولار أميركي سنوياً. ومن المتوقع أن ترتفع هذه الأرقام بشكل مستمر، ولاسيما إذا علمنا أن دراسة مسحية أجرتها شركة (كاسبرسكي لاب الشرق الأوسط) على مدار ٥ أشهر بدءاً من يونيو ٢٠١٠م، تظهر تعرُّض مستخدمي الخدمات المصرفية عبر الإنترنت في السعودية لنحو خمسة آلاف إصابة من قِبل المحتالين الإلكترونيين،

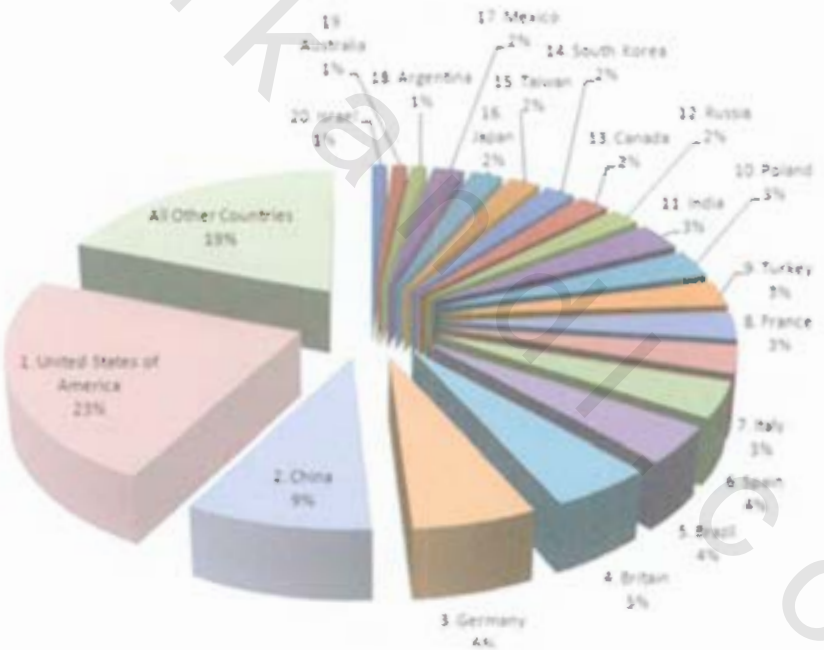
١ spam.gov.sa



obeikandl.com

وبذلك تكون السعودية في المرتبة الثالثة عالمياً، بعد مصر (٧٥٠٠) إصابة، والمكسيك (٥٠٠٠) إصابة، ضمن الدول الأكثر استهدافاً لخدماتها المصرفية. ومن ثم تأتي تركيا، والمغرب، وإيران والكويت بنحو ألفي إصابة من هجمة (ZeuS)، وهو برنامج حصان طروادة يتخصّص في الخدمات المصرفية المقدمة عبر الإنترنت.

ويقدم الشكل (٢) توضيحاً لمعدلات الجرائم الإلكترونية عالمياً، حيث تعد أمريكا من أكثر الدول ارتفاعا في هذا الباب.




الشكل (٢) معدلات الجرائم الإلكترونية عالمياً

# الفصل الأول :
# خصائص الجريمة في الإنترنت

obeikandl.com

**على الرغم من أن الجريمة في الإنترنت تعدّ مشابهة للجريمة في الحياة الواقعية بشكل أو بآخر، إلا أن هناك بعض الخصائص التي تميزها عن الجريمة في الحياة الواقعية. فبعض هذه الخصائص تسهم في التشجيع على الجريمة في الإنترنت وبعضها الآخر له دور كبير في جعل الجريمة في الإنترنت أخطر من تلك في الحياة الواقعية بشكل أكبر. وسيتحدث هذا الفصل عن بعض خصائص الجريمة في الإنترنت، وهي:**

١- كثرة المغريات والأهداف

٢- التفاعلية

٣- سهولة الحصول على المعلومة

٤- انعدام الحواجز الجغرافية

٥- انعدام التحكم المركزي

٦- انعدام الهوية

٧- قلة التكلفة

٨- قلة الإبلاغ عنها

فيما يأتي سيتم الحديث عن كل من هذه الخصائص بشيء من التفصيل.



obeikandl.com

## ١-١ كثرة المغريات والأهداف

عند بداية ظهور الإنترنت، كان دورها منحصراً في المجال الأكاديمي فحسب، ومن ثم أخذت الإنترنت بالتوسع بشكل متدرج لتقدم قدراً محدوداً من المعلومات عن الشركات والمؤسسات المختلفة. ولكن بعد ما يسمى بـ (انفجار الإنترنت) تسارعت أغلب الشركات والمؤسسات المختلفة لتقديم خدماتها عن طريق الإنترنت، حيث يندر أن تجد شركة دون أن يكون لها موقع أو خدمات على الإنترنت. ولم يقتصر الأمر على ذلك فحسب، بل ظهرت موجة التجارة الإلكترونية (E-Commerce) التي أدت إلى ظهور الكثير من مواقع التجارة الإلكترونية، لتمكين المستخدمين من شراء البضائع المتنوعة عن طريق الإنترنت. ناهيك عن استخدام معظم الشركات والقطاعات للإنترنت كوسيلة ربط للشبكات الموجودة في أماكن متباعدة جغرافياً. ووجود الكثير من المستخدمين العاديين المرتبطين بالإنترنت سواء أكانوا بشكل دائم أم مؤقت.

كل هذه العوامل ساعدت -بلا شك- في تفعيل الجريمة في الإنترنت، حيث إن وجود هذا الكم الهائل من المواقع والأشخاص، وارتباطهم بالإنترنت يجعلهم أهدافاً محتملة للمجرمين في الإنترنت، ولا شك بأن المعلومات الموجودة في المواقع التجارية كافية لأن يسيل لها لعاب المجرمين في الإنترنت. ولعل أبسط الأمثلة على ذلك هو قاعدة البيانات المحتوية على أرقام البطاقات الائتمانية الخاصة بزبائن المواقع التجارية في الإنترنت التي دائما ما يستهدفها المجرمون في الإنترنت، رغبةً في الحصول عليها، واستخدامها للقيام بعمليات شراء غير قانونية. وكذلك المعلومات التي تنتقل عبر الإنترنت، وقد تكون في بعض الأحيان شديدة الحساسية ولا تقدر بثمن سواء لاستخداماتها التجارية، أو السياسية، أو غيرها، وأبسط الأمثلة على ذلك هو الاختراقات

المتعددة التي حصلت لمواقع وزارة الدفاع الأمريكية وشبكاتها، والتي نتج عنها سرقة معلومات شديدة الحساسية. ولعل أشهر هذه الحوادث هي الوثائق السرية المسربة من وزارة الخارجية الأمريكية التي نشرها موقع (ويكيليكس) الإلكتروني، والتي تتضمن آلاف الرسائل والبرقيات الدبلوماسية المتبادلة بين الولايات المتحدة ودول العالم. ويذكر أن موقع ويكيليكس حصل على (٢٥٠) ألف وثيقة من الخارجية الأمريكية عن طريق الجندي الشاب (برادلي مانينج)، وقد ساعده أحد قراصنة الإنترنت، ويدعى (أدريان لامو) في تصنيف وتجهيز هذه المعلومات قبل إعطائها إلى مؤسس موقع ويكيليكس (جوليان أسانج).

## ١-٢ التفاعلية

من أهم خصائص الإنترنت هو حيويتها وتفاعليتها، فالتحديث يكون مباشراً بعكس ما هو في الحياة الواقعية، وهذه الخاصية للإنترنت تنطبق على جميع النواحي المتعلقة بها ومنها الجريمة. ففي الحياة الواقعية وعند حدوث سرقة في بنك من البنوك، فإنه لن يُعرف الخبر إلا بعد فترة قد تمتد أو تقصر، وذلك لأن وسائل الإعلام في الحياة الواقعية في الغالب تتطلب بعض الوقت لتحديثها. ولكن في عالم الإنترنت فإن تأثير الجريمة سيكون لحظياً، فبعد أن يتم اختراق الموقع بثوانٍ محدودةٍ، فإن من يطلب صفحة الموقع سيحصل على الصفحة المخترقة. ولعل من أشهر الأمثلة على ذلك قصة اختراق موقع جريدة نيويورك تايمز التي أصبح المخترقون وأصحاب الموقع يتبادلون الكر والفر فيها، فما أن يتم تعديل الصفحة، حتى يقوم المخترقون بتغييرها مرة أخرى، واستمر ذلك على مدى ساعات، حتى تمكن أصحاب الموقع أخيرا من استعادة السيطرة عليه وإعادة الصفحة الرئيسية. وهذه الخاصية للإنترنت تجعل التعامل مع الجريمة فيها يتطلب استعدادات وإجراءات مختلفة عن تلك في الحياة الواقعية، وسيأتي الحديث عن ذلك لاحقاً.



obeikandl.com

## ١-٣ سهولة الحصول على المعلومات

تعدّ سهولة الحصول على المعلومات من أهم خصائص الإنترنت، فهي محيط ضخم زاخر بشتى المعلومات في مختلف المجالات. وكل ما يلزم للحصول على المعلومة التي تريدها هو ضغطة زر، مما يضفي على نشاط المجرمين في الإنترنت خطورة أشد من أولئك في الحياة الواقعية. وهذا ملاحظ في معظم بلدان العالم مثل الولايات المتحدة الأمريكية، حيث أتاحت الشبكة نشر مثل هذه المعلومات على نطاق كوني، وجعلتها في متناول كل من يرغب في الحصول عليها، فانتشرت مواقع كثيرة لبيع المعلومات الشخصية، ومنها مثلا: موقع مسمى بموقع نبش الأوحال (Dig Dirt) الذي يقوم بتوفير معلومات عن الأشخاص الذين يتلقون أموال مساعدة اجتماعية بمقابل ضئيل لا يتعدى (١١٠) دولارات. ويتضمن هذا الموقع معلومات عن الفساد، فهو يوفر قوائم لمجموعة من الأطباء، والمحامين، والأساتذة، والصحافيين، والمسؤولين ذوي السمعة السيئة، من بينهم أطباء فاشلون، ومحامون يستغلون العملاء وصحفيون مرتشون مزيفون للحقائق ومزورون للمعلومات. وفي الشبكة أيضاً كثير من المواقع التي تجمع معلومات عن الأطفال والمراهقين وعن كيفية إنفاقهم لمصروفهم، ونوع مشترياتهم المفضلة، والمراكز التي يترددون عليها للشراء، وهي تشمل كل شيء عنهم حتى امتلاكهم لسندات أو أسهم، والوضع المالي لعائلاتهم. والغريب في الأمر أن الجميع يجيبون على الأسئلة التي تطرح عليهم من قبل هذه الشركات دون الإحساس بالخطر الذي قد يأتيهم من حصول آخرين على هذه المعلومات الخاصة جدا. ومن أطرف ما يأتي في هذا الباب هو موقع على الإنترنت يسمى (خداع الفيسبوك)، وقد أنشأه رجل سمى نفسه سافاج (المخدوع) عام ٢٠٠٩م، بعد وقت قصير على اكتشاف خيانة زوجته له، في محاولة منه لتعريف الآخرين بكيفية اكتشاف حالات الخيانة والخداع وتتبعها عبر

موقع (فيسبوك)، ومساعدتهم على التعامل مع الأوضاع الجديدة. وقد دفع هوس معرفة الحقيقة ببعض المخترعين حداً جعلهم يبتكرون برامج لتقفي آثر الخيانة الزوجية، أو تعقب الأشخاص من خلال مواقعهم أو اتصالاتهم، وهو أمر تبنته شركات الاتصالات والبرمجيات الإلكترونية.


شكل١-١: أحد المواقع المنتشرة في الإنترنت، وتمكن من الحصول على المعلومات عن الأفراد

ومما لاشك فيه أن سلعة البيانات الشخصية غدت رائجة، ومطلوبة من الكثير من القطاعات الاقتصادية، وربما اهتمت بعضها بشرائح معينة من الناس، ولذا تقوم بعض الشركات بجمع معلومات عن شخصيات كبيرة لا يحرصون هم أيضاً ولا يتخوفون من التطوع بتزويد المراكز والشركات بالمعلومات الشخصية التي تغص بها مواقع كبيرة على الشبكة. فالأسئلة تطرح في كل مجال، حتى عن الأمراض التي يصاب بها الأشخاص، وشركات التأمين المؤمن عليهم فيها، ووظائفهم، وأوضاعهم الاجتماعية والمالية، وأرقام بطاقاتهم المختلفة وغير ذلك. و(٩٠٪) من هذه الشركات والمواقع التجارية حسب إحصائية للجنة التجارة الفدرالية الأمريكية، تجمع

معلومات دون أن تنبه الأشخاص أو تعلن سياستها في جمع المعلومات أو مدى محافظتها على سرية تلك المعلومات. ولا يتعدى عدد المراكز أو الشركات التجارية التي تنبّه الزوار إلى ما تنوي عمله بالمعلومات المجموعة منهم وأنها تعد كل معلومة تقوم بجمعها غير سرية، وأن لها الحق في التصرف فيها بالشكل الذي تختاره إلا نسبة قليلة من الشركات العاملة في هذا المجال.

## ١-٤ انعدام الحواجز الجغرافية

لكي يقوم المجرم بارتكاب جريمة في الحياة الواقعية فلابد من وجوده في نفس موقع الجريمة، ولكن الجريمة في الإنترنت لا تعترف بالحواجز الجغرافية، فالمخترق يستطيع اختراق موقع خاص بشركة في إحدى قارات العالم بينما هو موجود في غرفة نومه الصغيرة أو في مقهى في الطرف الآخر من العالم. ويرجع الكثير من الباحثين سبب انتشار الجريمة في الإنترنت إلى هذه الخاصية.

ومن الأمثلة على ذلك ما حدث بين الصينيين والأمريكان بعد مشكلة طائرة التجسس الأمريكية، حيث قامت حرب إلكترونية بين البلدين، وأصبح الصينيون يقومون باختراق المواقع الأمريكية، والأمريكان يقومون باختراق المواقع الصينية. ولقد مكنتهم الإنترنت من القيام بذلك على الرغم من آلاف الأميال التي تفصل بينهم.

## ١-٥ انعدام التحكم المركزي

على الرغم من أن وزارة الدفاع الأمريكية هي التي أنشأت بذرة الشبكة في بادئ الأمر، إلا أنه لا أحد يملك الشبكة أو يتحكم بها حاليا. فكلُّ جهة تملك شبكتها، وهي التي تديرها وتتحكم بها دون أن تمتد صلاحياتها ونطاق تحكمها إلى شبكات الجهات الأخرى. ولا تستطيع دولة أياً كانت أن تفرض قيودها وأنظمتها على مستخدمي الإنترنت في العالم. ومع وجود الكثير من المنظمات التي تهدف لإيجاد ثوابت ومعايير للإنترنت غير أنها لا تمتلك سلطة مركزية على الشبكة المترامية الأطراف.

وهذه الخاصية تجعل التحكم بالإنترنت صعباً جداً، مما يساعد على انتشار الجريمة في الإنترنت. فالدول المختلفة تمتلك قوانين مختلفة لمستخدمي الإنترنت فيها. ومن أمثلة ذلك، وجود المواقع التي تقوم بمخالفة قوانين حماية الحقوق الفكرية، فالكثير من الدول التي تمنع وجود هذه المواقع في الشركات الموجودة في تلك الدولة، لا تملك أي سيطرة على المواقع الموجودة في دول أخرى لا يوجد لديها قوانين لاستخدام الإنترنت.

## ١-٦ انعدام الهوية

عندما ترتبط بالإنترنت فأنت في الأصل شخص مجهول الهوية، وهذا ما يعشقه المجرمون، حيث يستخدمون الوسائل المختلفة لإلغاء هويتهم عند اتصالهم بالإنترنت مما يجعل من تتبعهم أمراً صعباً، ومن ثم يقومون بارتكاب جرائمهم. ويرجع باحثو علم النفس ذلك لغياب عنصر الاجتماعية ووجود الاتصال وجهاً لوجه. ويذكر هذا بسلوك الإنسان بعد شيوع استخدام السيارات، حيث لوحظ أن شخصية المرء خلف عجلة القيادة تختلف عنها عندما يكون



obeikandi.com

أمام الآخرين وجهاً لوجه، فالكثير من الناس تتغير شخصيتهم لتصبح أكثر عدوانية عند قيادتهم للسيارة. وهو يماثل سلوك مشجعي كرة القدم، حيث إن وجودهم ضمن مجموعات كبيرة يخفي هويتهم مما يساعدهم على القيام بالشغب في الملاعب. وبنفس الطريقة فإن الشخص الذي يتصل بالإنترنت لا يرى منها سوى شاشة الحاسب أمامه، فاستخدامه للإنترنت يخفي هويته، ويحوله من كائن آدمي إلى مجموعة نبضات إلكترونية تنتقل عبر أسلاك الشبكات بسرعة الضوء من بلد إلى آخر. وهذا ما يجعل المجرمون في الإنترنت يتجرؤون على الجريمة، وكما قيل في الأمثال: «من أمن العقوبة أساء الأدب».

هذا لا يعني أن كل من يستخدم الإنترنت هو مجهول الهوية! فهناك وسائل لتتبع ومعرفة مستخدمي الإنترنت ولكن لكل قاعدة استثناء. والاستثناء لهذه القاعدة هم مجرمو الإنترنت والذين يمتلكون القدرة على التخفي في الإنترنت مما يجعل الوصول إليهم أمراً صعباً. ومن أمثلة هؤلاء أحد المتسللين الكنديين المشهورين الذي يذكر أنه قبل أن يقوم باستخدام مزودات المحادثة (chat servers) فإنه يقوم بالدخول عبر ستة أجهزة وسيطة لكي يجعل تتبعه مستحيلاً، ولاسيما إذا كان أحد هذه المزودات لا يسجل وقائع الاتصال والترابط بينه وبين المزودات الأخرى.

ويجب التفريق هنا بين انعدام الهوية وبين استخدام هوية زائفة. فالأولى تستخدم في الجرائم التي لا تتطلب إبراز هوية مثل جرائم الاختراق وغيرها. أما الأخرى فهي تستخدم عند ارتكاب جرائم تتطلب وجود هوية معينة، مثل فتح حساب في بنك. ولكنهما في النهاية يقومان بنفس الغرض، وهو إخفاء الهوية الرئيسة للمجرم.



obeikandl.com

## ١-٧ قلة التكلفة

من المعروف بأن ارتكاب جريمة في العالم الواقعي أمر مكلف ماديا. فهو يتطلب التحضير والتدريب وشراء المعدات وما إلى ذلك، مما قد يتعذر على الشخص العادي تحمل تكلفته أو الحصول عليه أساسا. أما ارتكاب الجريمة في الإنترنت فلا يكلف إلا شيئا قليلا، فكل ما يجب الحصول عليه هو جهاز حاسب آلي ذو قدرات معقولة بالإضافة إلى اتصال بالإنترنت، وبعدها يمكن لمستخدم الشبكة القيام بما يريد بافتراض أن لديه القدرات والخبرات اللازمة.

## ١-٨ قلة الإبلاغ عنها

لا يتم – في معظم الأحيان- الإبلاغ عن جرائم الانترنت خوفاً من التشهير أو لعدم اكتشاف ضحية هذه الجريمة لها. فمعظم جرائم الإنترنت تم اكتشافها بالمصادفة؛ بل وبعد وقت طويل من ارتكابها، زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها، فالفجوة بين العدد الحقيقي لهذه الجرائم ؛ وما تم اكتشافه هي فجوة كبيرة.



obeikandl.com

# الفصل الثاني :
# الأخطار المحتملة في الإنترنت

obeikandl.com

إن مصطلح (الجريمة في الإنترنت) لا ينحصر فقط في سرقة البطاقات الائتمانية أو اختراق المواقع، بل هو مصطلح عام يندرج تحت مظلته كل عمل مخالف للقانون ومخل بالآداب يتم عن طريق الإنترنت. وعلى الرغم من كثرة هذه الأخطار وتنوعها وصعوبة تصنيفها إلا أن الحديث سيدور حول خمسة أقسام رئيسة منها، وهي:

١- الأخطار المادية

٢- الأخطار النفسية

٣- الأخطار على الأطفال

٤- الأخطار على النساء

٥- الأخطار على الخصوصية



obeikandl.com

## ٢-١ الأخطار المادية

تعدّ الأخطار المادية من أهم الأخطار في الإنترنت، وهي أول ما يتبادر للذهن عند ذِكْر مصطلح الجريمة في الإنترنت. ففي تقرير أصدره مكتب التحقيقات الفيدرالي الأمريكي (FBI/CSI)، أوضح أن بطاقات الائتمان كانت تمثّل الغالبية من خسائر القرصنة والسرقات المالية التي حدثت في الولايات المتحدة عام ٢٠٠٥م، والتي بلغت ٣١٥ مليار دولار، وأفادت دراسة أوروبية ذكرت أن أكثر من ٢٢ مليون من الأشخاص البالغين قد وقعوا ضحايا خداع وسرقة بطاقاتهم الائتمانية في أوروبا عام ٢٠٠٦م، أما الإحصائيات الصادرة من البنك المركزي الفرنسي بنك فرنسا، فقد أظهرت أن خسائر سرقة بطاقات الائتمان بلغت ٢٣٦ مليون يورو (٣١٩ مليون دولار) عام ٢٠٠٦م.

وتقّدر إحصائيات أخرى معدل جهد الشخص المتضرر الذي يقوم بقضاء ما يقارب (١٧٥) ساعة ويصرف ما يصل إلى الألف دولار لكي يتمكن من استرجاع أمواله الضائعة نتيجة سرقة بطاقته الائتمانية. وتقدر الإحصائيات الخسائر المادية المتعلقة بالإنترنت ببلايين الدولارات سنوياً، وهذا شيء منطقي عند معرفة الخصائص والتسهيلات التي تقدمها الإنترنت للجريمة (كما ذكر سابقاً). وتستحوذ سرقة البطاقات الائتمانية على نصيب الأسد في هذه السرقات المادية في الإنترنت، لكونها الوسيلة الرئيسة لتبادل السيولة المادية في الإنترنت. ومن القصص المتعلقة بسرقة البطاقات الائتمانية في الإنترنت ما حدث في الأردن في الشهر السابع من عام ٢٠١١م، إذ حذر البنك المركزي الأردني البنوك المحلية من توسيع نطاق خدمة بطاقات فيزا الائتمانية بعد تعرض العديد منها إلى عمليات قرصنة وسرقة خارج البلاد، وقد ذكرت بعض المصادر في القطاع المصرفي أن حجم التزوير في البطاقات الائتمانية (فيزا) قد تصل في مجملها منذ بداية العمليات أي قبل ثلاثة أشهر إلى مليوني دينار أردني. وأما أكبر عملية في هذا الباب ما أعلنت عنه السلطات الأميركية في الشهر الثامن من ٢٠٠٩م، من ضبط ما قالت إنها



obeikandi.com

أكبر عملية قرصنة وسرقة هوية على الإطلاق. إذ شملت سرقة أكثر من (١٣٠) مليون بطاقة ائتمانية لأكثر من (٢٥٠) شركة للبيع بالتجزئة و منظمات مالية كبرى، ووجهت السلطات الاتهامات إلى ثلاثة أشخاص أحدهم أميركي يدعى (ألبرت غونزاليز) من مدينة ميامي والآخران روسيان. وإضافة إلى هاتين القصتين فهناك المئات من هذا النوع من الجرائم؛ إذ إن البطاقات الائتمانية ليست هي الطريقة الوحيدة، فهناك أيضا مواقع البنوك التي تمكن المعتدي من القيام بمختلف العمليات البنكية عن طريق الإنترنت، وعلى الرغم من أن هذه المواقع قد تكون آمنة من الاختراق من قبل المجرمين، إلا أن الثغرة الأمنية المتعلقة بها هي المستخدمون العاديون. فالمجرمون في الإنترنت يفكرون بطريقة مميزة وغير تقليدية-وسيأتي الحديث عن خصائصهم في الفصل الخامس- فإذا كان موقع البنك محصناً بشكل كبير- وهو بلا شك كذلك- فهذا لا ينفي الإمكانية العالية لاختراقه وسرقته، غير أن أسهل الطرق وأيسرها للمجرمين هي محاولة السرقة عن طريق انتحال شخصية المستخدم البسيط الذي لا يمتلك المعرفة والقدرة الكافيتين لتوفير مستوى جيد من الحماية. وأبسط مثال لذلك هو تعرض جهاز مستخدم عادي للاختراق عن طريق أحد برامج التجسس التي تمكن المخترق من معرفة كل ما يقوم به المستخدم أو يكتبه، ومن ضمن ذلك معرفة اسم المستخدم الخاص وكلمة السر التي يستخدمها ذلك الشخص للتحكم في حسابه البنكي؛ مما يمكن المجرم من استخدامها بشكل مضر لصاحبها. وهذا ينطبق أيضا على مواقع التعامل بالأسهم أو مواقع السوق الإلكتروني، أو مواقع الشراء في الإنترنت، أو غيرها من المواقع الأخرى.

وانتشار التجارة في الإنترنت هو سلاح ذو حدين، فهو يوفر السهولة والرفاهية للمستخدم، كي يتمكن من استخدام الإنترنت للتسوق والقيام بمختلف العمليات التجارية دون أن يخرج من بيته، ولكنه في الوقت نفسه يعد هذا الانتشار جذّاباً للمجرمين الطامعين في الإنترنت والذين يرغبون في استخدام خصائصها المختلفة للحصول على المكاسب بشكل غير قانوني.

## ٢-٢ الأخطار النفسية

ليست الإنترنت مستودعاً للمعلومات فحسب، بل يمكن النظر إليها على أنها مجتمع إلكتروني يتقابل فيه الناس ويتحادثون، ويبيعون ويشترون السلع المختلفة. وهذا المجتمع الافتراضي في حالة المستخدم الطبيعي المتزن هو مكمّل للمجتمع الحقيقي الذي نعيش فيه حياتنا الواقعية. وهناك معادلة يوجد في أحد طرفيها المجتمع الحقيقي، وفي الطرف الآخر المجتمع الافتراضي، وهذه المعادلة يجب أن يتم وزنها وإلا فإن هناك خللاً لابد من حدوثه. ولا يعدو الناس بالنسبة للمعادلة ثلاثة أقسام: فأما الأول؛ فهو قسم لا يعترف بالمجتمع الافتراضي ويرفض استخدامه، وهذا القسم يحرم نفسه من الفوائد التي تقدمها الإنترنت له، وأتوقع أن ينقرض هذا القسم عاجلاً أم آجلاً. وأما القسم الثاني؛ فهو قسم يوازن بين المجتمعين، ويستخدمهما كمكملين لبعضهما بعضا. وهذا هو القسم السليم والمطلوب. وأما القسم الثالث؛ وهو مدار الحوار في هذه النقطة، وهو القسم الذي انغمس في المجتمع الافتراضي بشكل كامل مما أدى إلى انعزاله عن المجتمع الحقيقي. وهذه هي المشكلة الكبيرة التي يطلق عليها في أوساط مجتمع الطب النفسي بإدمان الإنترنت، وهو مصطلح حديث برز مع ظهور الإنترنت. وتقضي هذه الفئة من الناس جلّ وقتها أمام شاشة الحاسب سواء في البحث عن المعلومات أو المحادثة أو غيرها. ويغلب على الأشخاص المنتمين لهذه الفئة المعاناة من مشاكل في التعامل مع الأشخاص الآخرين في الحياة الواقعية، بل إنك قد تجد بعضهم منبوذاً في الحياة الواقعية وينظر إليه على أنه غريب الأطوار، في حين يكون في مواقع الإنترنت ومنتدياتها من أشهر المشاركين وأكثرهم محبة من قبل الآخرين.

بالطبع فإن درجة الإدمان تتراوح بين عدة مستويات، ولكن أهونها سيِّئ. ولقد بينت إحدى الإحصائيات أن نسبة من يعانون من إدمان الإنترنت بشكل أو بآخر هو (١٠٪)، وهي نسبة ليست قليلة. والإدمان في الأعم الأغلب يكون إما على المواقع الإباحية، أو المحادثة أو المقامرة أو الألعاب. ولكل قسم من هذه الأقسام طريقة للعلاج.

ويعتقد علماء النفس بأن السبب الرئيس لإدمان الإنترنت هو وجود مشاكل اجتماعية لمدمني الإنترنت، حيث إن المدمن يهرب من المجتمع الحقيقي إلى مجتمعه (الافتراضي) الخاص حيث لا يعرفه ولا يعلم عن مشاكله أحد.

والطريف في الأمر أنه انتشر في الإنترنت حاليا مواقع تقدم المعالجة لإدمان الإنترنت، ومن دون حاجة المريض لزيارة العيادة في الحياة الواقعية.

## ٢-٣ الأخطار على الأطفال

تأتي مع الإنترنت فرصة يصعب تصديقها للأطفال. فهي تجعل كل شيء في متناولهم، ابتداءً بالتعليم وانتهاءً بالتسلية والترفيه. فالأطفال ( بنون وبنات) ممن هم في الصف الرابع أو الخامس، أو حتى قبل ذلك، يستطيعون زيارة مواقع كثيرة على الشبكة. فالطفلة، مثلا يمكنها أن تبحر في المواقع التي تشتمل على مواد خاصة بالبنات فحسب، مثل موقع الألعاب (بنات هاي)، وبقية المواقع المفيدة التي تستحق الإبحار فيها خصوصا للأطفال، مثل موقع بنين وبنات، أو كتاكيت وغيرهما.



obeikandl.com


شكل ٢-١: أحد المواقع العربية الخاصة بالأطفال(www.kids.islamweb.net)

فالشبكة تضع في متناول الأطفال الكثير، ولكن ينبغي للوالدين معرفة إلى أين سيبحرون، وكيف يبحرون، ووضع الاحتياطات اللازمة لحمايتهم من الانزلاق نحو المواقع غير المناسبة التي تشتمل على مواد تلحق بهم الأذى؛ مثل: المواقع الإباحية التي تعرض الصور الفاضحة أو الجنس، وتلك التي تدعو إلى تعاطي مختلف أنواع المخدرات وتبين آلية صناعتها، ومواقع لعب القمار، وبعض المواقع التي تحوي تعليمات صناعة القنابل والمتفجرات، أو تكون مؤطرة بالكره والتعصب والعنصرية، وتدعو للرذيلة أو تشجع على الانخراط في جمعيات سرية أو عصابات مافيا تمارس أعمالاً مخالفة للقانون. ومن المؤسف أن عدد هذه المواقع وما تعرضه من صفحات في تزايد مستمر. ولذلك، ينبغي الحذر وسدُّ الذرائع التي تفتح باب الشر هذا، والاكتفاء بالمواقع المفيدة التي ترتقي بمعارف الأطفال وتثري أخيلتهم، وتغرس فيهم قيماً لا تتناف مع المعتقدات الدينية، أو تتعارض مع الأخلاقية السائدة في مجتمعاتهم.

وهناك أمور مهمة تتعلق بالاتصال المباشر بالإنترنت يجب وضعها بالحسبان. فمع نمو الشبكة وازدياد عدد المواقع وتنوعها بين صالح وطالح، وبسبب عدم وجود رقابة عليها، أو قانون عام يحميها، يجب أخذ الاحتياطات اللازمة فيما يتعلق بتوفر الأمن والحماية للأطفال على الشبكة كي لا يخوضوا في أوحالها، أو يهبطوا إلى عالمها السفلي البغيض. فالأطفال دون هذه الحماية وبسبب عدم إدراكهم لما يدور في فضاء الإنترنت يمكن أن يصبحوا معرضين لخطر كبير. ولذلك، سيتم هنا اطلاع القارئ على ما يجب القيام به لحماية طفله وحفظه بعيداً عن هذه الأخطار.

إن الكثير من الأطفال يبحرون في الإنترنت هذه الأيام، ويشاركون الكبار في الاطلاع على أعقد المعلومات والملفات فضلاً عن أبسطها، فتجدهم يفتشون عن الأمطار الحمضية، والمسائل الاجتماعية الشائكة، ويقابلون الكبار والصغار ممن هم في سنهم ومستواهم الدراسي، ويتعرفون على معطيات حضارية وثقافية لأمم أخرى ومجتمعات لها معتقداتها ونهجها الحضاري المماثل أو المغاير. فشبكات الحاسب تَعِدُ بمزايا وفرص مذهلة، ولكنها في الوقت ذاته تطرح مشكلات في غاية الصعوبة والتعقيد، وتحتاج إلى نقاش صريح وواضح يمكن الوصول من خلاله إلى حلول واضحة لمشاكل معلقة يشار إليها دائما بالأخطار المحتملة. فإلى متى ستظل هكذا تهدد مستخدمي الشبكة بدرجة قد تؤدي إلى عزوف الكثيرين عنها.

ستُطرح هنا جملة من الأسئلة التي تشكِّل الإجابة عليها طريقاً آمناً - حماية الصغار والكبار والأسرة، بل ومستخدمي الشبكة جميعاً عند إبحارهم في عالمها الفسيح. هل يمكن منعُ الأطفال من الوصول إلى المواد المثيرة للجدل والمختلف عليها؟ وهل المنع أمر مرغوب فيه من قبل الجميع؟ وهل الرقابة هي الحل الأمثل لذلك؟ وما هي البدائل المطروحة؟ وما هي الحلول التي يمكن تقديمها؟ وكيف نتخاطب مع الأطفال حول هذه المسائل؟ وماذا نقول للآباء والأمهات ومديري المدارس الذين تقلقهم هذه المسائل؟ وإن من أعقد الأسئلة المطروحة ما يأتي: من الذي يقرر المناسبَ وغير المناسب من المواد؟ ومن هو الذي يضع المعايير الاجتماعية لما هو مناسب

وغير مناسب؟

إن الأسئلة كثيرة ومتشعبة، وإن المجازفة ستكون كبيرة جداً إذا لم يجد الجميع -بالتعاون مع بعضهم بعضا- سبلاً ووسائل لمعالجة هذه الأمور الصعبة والإجابة على هذه الأسئلة المحيرة لأن عدم إيجاد وسائل المعالجة سيدفع الآباء ومديري المدارس لمنع الأطفال من الإبحار في الشبكة كأفضل وسيلة لحمايتهم من الأخطار المحتملة التي تمثل أعقد تحديات هذا القرن وربما القرون القادمة.

إن أكثر الأخطار احتمالاً وفق الإحصائيات المتداولة، هو أن يقابل الأطفال في غرف النقاش، أو مجموعات الأخبار، أو في مواقع أخرى أشخاصاً بغيضين يتميزون بالوقاحة والخسة وسوء الخلق، ويمثلون خطراً داهماً عليهم. ومن المخاطر الأخرى هي أن يُضيَّعَ الأطفال وقتاً ثميناً من عمرهم في مجالات لا تعود عليهم بالنفع، **ويضاف إلى ذلك ما يأتي:**

- التعرض لمواد لا تناسبهم، وتشمل الجنس وإثارة نعرات الكراهية، أو التشجيع على العنف والدعوة للانخراط في جماعات أو جمعيات تمارس أنشطة خطيرة أو غير قانونية.
- الإيذاء الجسدي الذي قد يحدث من خلال قيام الأطفال - وهم مرتبطون بالشبكة- بتقديم معلومات، أو ترتيب لقاء مع أشخاص آخرين قد تعرض سلامة الطفل أو الطفلة أو سلامة الأسرة ككل للخطر. ففي العديد من الحالات استخدم أشخاص منحرفون من مستغلي الأطفال جنسياً، البريد الإلكتروني أو لوحات البيانات وغرف النقاش لكسب ثقة أحد الأطفال، ثم التنسيق معه لمقابلته فعلياً.
- التعرض للمضايقة والإزعاج المستمرين من خلال تلقي رسائل بالبريد الإلكتروني أو من خلال غرف النقاش أو لوحات المعلومات، فتسبب لهم مضايقة وإزعاجاً شديدين، كأن تكون هذه الرسائل قذرة المحتوى والأسلوب أو مثيرة للحنق. وهذا النوع من المخاطر لا يهدد بالطبع حياة الأطفال ولكنه يجرح مشاعرهم، وتترتب عليه ترسبات نفسية قد تكون



obeikandl.com

لها آثار ضارة وذكرى مؤلمة في مستقبل حياتهم، وهذا قد يحدث لأي طفل يمارس هواية الدخول إلى غرف النقاش، أو تبادل الرسائل على المنتديات.

- القيام بعمل مخالف للقانون أو تترتب عليه مسؤولية مالية. فمن الأخطار المرجحة أيضاً أن يقوم الطفل بعمل تكون له آثار سلبية من الناحية القانونية، أو المالية، مثل الكشف عن رقم بطاقة الائتمان الخاصة بوالده أو والدته، أو القيام بعمل يخلّ بحقوق الآخرين. وبغضّ النظر عن المسائل القانونية، فإن الطفل يجب أن يتعلم الطريقة الصحيحة للسلوك القويم على الشبكة، وتجنب البذاءة وسوء الخلق والسلوك غير المراعي لحقوق الآخرين ومشاعرهم. ويضاف إلى ذلك خطورة أن يقوم الأطفال بإعطاء كلمات السر الخاصة بأجهزتهم أو أجهزة ذويهم إلى أشخاص آخرين قد يستغلونها في أعمال قد تعرض الأسرة أو الطفل أو الممتلكات للخطر.
- من المخاطر المحتملة أيضاً سلب الخصوصية، فقد يتعرض الأطفال لمحاولة من جهات ذات أهداف مغرِضة لاستخلاص معلومات تتعلق بأسمائهم وأعمارهم والمدارس التي يدرسون فيها،والتعرف على أحوال بقية الأسرة وخصوصيتها.
- التعرض لخطر المخدرات والمسكرات والتدخين وما إلى ذلك، حيث إن هناك بعض المواقع على الشبكة ومجموعات الأخبار تتضمن معلومات تشجع على استخدام الكحول، والحشيش، والمخدرات وتدافع عن ذلك بكل عزيمة وإصرار، لأهداف مادية أو عدائية للمجتمع المحافظ.
- تعلُّمُ لعب القمار وأنواع السلوك الأخرى غير المقبولة عبر المواقع التي تسمح لمرتاديها بالمقامرة الحقيقية بالمال أو للتسلية فقط. وبعض هذه المواقع قد يقوم بهذا العمل في بعض الحالات بصورة مشروعة في بعض البلدان التي تسمح قوانينها بمثل هذه الممارسات للكبار، كما أشرنا سابقاً، ولكنها تكون غير قانونية للقُصَّرِ ممن هم دون سن الرشد، بغض النظر



obeikandl.com

عن مكان وجودهم. وتتطلب المقامرة على الشبكة أن يستخدم المقامر بطاقة ائتمان، أو أن يكتب شيكاً لتحويل الأموال. والحديث عن المقامرة يمكن أن يقود أيضاً إلى احتمال بيع وشراء الأسهم عبر الشبكة. لذا؛ فإذا كان للأطفال إمكانية الوصول إلى متصفح آبائهم، أو حساب مقدم الخدمة لهم، وكلمة السر الخاص بأعمال المضاربة لهم في الأسهم، فإنه سيصبح بإمكانه القيام بمثل هذه المعاملات عبر الشبكة. ولذلك ينبغي مراقبة ذلك بحذر شديد؛ إما بمنع الأطفال من القيام بذلك، أو تشديد الرقابة عليهم لمعرفة ما يقومون به من أعمال على الشبكة.

ولكن الأكثر إثارة ورعباً هو أن المرء قد يجد مواقع على شبكة الإنترنت تتيح له تعلُّم صناعة القنابل والمتفجرات، أو الحصول على الأسلحة بأنواعها المختلفة. ولكن لحسن الحظ لم ترد حتى الآن على الإنترنت روايات تفيد بقيام أي طفل بأعمال عنف أو استخدام لمواد صنع القنابل أو المتفجرات، أو المخدرات، من خلال تواصله مع الإنترنت والإبحار فيها. ومع ذلك، فإنه ينبغي في بيئة شديدة الخطورة لا سيطرة لأحد عليها، مثل شبكة الإنترنت التي تتوفر فيها جميع أصناف المعلومات المفيدة وغير المفيدة، اتخاذ كل ما يلزم من احتياطات لحماية أطفالنا من أي معلومة أو فعل يمكن أن يعرض حياتهم للخطر.

## ٢-٤ الأخطار على المرأة

كشفت إحصاءات أعلنت نتائجها شركة (جوجل الشرق الأوسط وشمال إفريقيا) في الشهر الثامن من عام ٢٠١١م، على موقعها (Insights MENA) وهو الموقع الذي أطلقته لخدمة المهتمين بمعرفة مؤشرات وسلوك استخدام الإنترنت؛ أنّ أكثر معدل لاستخدام النساء للإنترنت في الدول العربية التي تغطيها مؤشرات الموقع كان في دولة الإمارات حيث بلغت النسبة ٨١ ٪، فيما بلغت في السعودية ٦٥ ٪، وحلت المغرب في المرتبة الثالثة بنسبة ٤٢ ٪، ثم الأردن ٣٠ ٪، فمصر ٢٩٪.

وأظهرت الأرقام أن المعدل العام لاستخدام الإنترنت في الدول الخمس :مصر، الأردن، المغرب، السعودية والإمارات، يصل إلى ٥٧ ٪، حيث بلغت النسبة العامة للنساء المستخدمات للإنترنت في هذه الدول ٤٦ ٪، فيما بلغت نسبة الرجال المستخدمين للإنترنت ٦٥ ٪

وأظهرت الأرقام أن المعدل العام لاستخدام الإنترنت في الدول الخمس :مصر، الأردن، المغرب، السعودية والإمارات، يصل إلى ٥٧ ٪، حيث بلغت النسبة العامة النساء المستخدمات للإنترنت في هذه الدول ٤٦ ٪، فيما بلغت نسبة الرجال المستخدمين للإنترنت ٦٥ ٪

ومع أن الإحصائية السابقة تقدم أرقاماً معقولة لمشاركة النساء في الشبكة العنكبوتية إلا أن المتابع للمنتديات والمنابر العامة التي يتعرف فيها الأشخاص بعضهم على بعض، من خلال المقالات التي ترسل عن طريق البريد الإلكتروني، أو التحاور الإلكتروني، أو غرف المحادثة، أو غيرها من الوسائل التي تتيحها الشبكة؛ يلاحظ أن عدد الرجال الذين يشاركون فيها يفوق عدد النساء بشكل ملحوظ. لدرجة أن الرجال المشاركين يحاولون عبثاً الحصول على إجابة شافية للسؤال



obeikandl.com

عن سبب قلة النساء من حولهم في هذه المنتديات على الرغم مما يبدينه من ضجيج في الحياة العامة حول العدل والمساواة وتكافؤ الفرص.

والإجابة المرجحة على انعدام هذا التوازن لا تبدو واضحة بالقدر الكافي. فبعضهم يرى أن ذلك عائد إلى كثرة عدد الرجال الذين يستخدمون أجهزة الحاسب. ويرى آخرون أن الشبكة بدأت بغالبية من الرجال، وعند محاولة النساء الدخول إلى الشبكة والانتماء إليها يشعرن بمعاملة غير طيبة ومجحفة من عالم الرجال فيحجمن عن المشاركة الفاعلة فيها. ومع ذلك فهناك من يقول بأن عدد النساء على الشبكة كبير، ولكنهن يستخدمن أسماء مستعارة (رجالية) لصرف النظر عن جنسهن، والتركيز على كلماتهن وإنتاجهن الفكري والإبداعي. ولكنها في نهاية الأمر مسألة يصعب البت فيها والتيقن منها.

وأياً تكن الأسباب لقلة عدد النساء على شبكة الإنترنت، فالمعلوم أن المرأة غالباً في معظم دول العالم عندما تتحدث في مجموعة أخبار أو مجموعة نقاش يهيمن عليها الرجال، فإنها في الغالب تخشى أن تجد نفسها قد أصبحت محط الأنظار شاءت أم أبتْ. وهي ترجّح أن الرجال يستجيبون لها ليس فقط للتمعن في ما تطرحه من آراء وأفكار بل تطلعاً لمعرفة اسمها، وعمرها، وعنوانها، وشكلها أو حتى لمجرد الإحساس بالغبطة لمشاركة أنثى لهم في هذا المنتدى أو غيره، فتشعر بعدم الارتياح، ومن ثم تعزف عن المشاركة وربما ترحل عن الشبكة بكاملها.

ولذلك عندما تصبح الشبكة آمنة، ويعامل فيها كل فرد، رجلاً كان أم امرأة، بمساواة ويحظى بالاحترام دون النظر إلى نوعه، أو جنسه، أو جنسيته، أو دينه، أو لونه، أو نوعية جهاز حاسبه، و ما إلى ذلك، ويتم معاقبة أي محاولة للتحرش، فإن الشبكة ستصبح مكاناً نموذجياً لتبادل الآراء والأفكار والنقاش الجاد المثمر، وستحاول المرأة الانتماء إليها والانتفاع بما توفره من معلومات ومعارف دون اللجوء إلى ترتيبات ووسائل لإخفاء شخصيتها وانتحال اسم رجالي كثمن للإبحار في الشبكة دون التعرض للمضايقات والإيذاء النفسي، خصوصا وأن هناك الكثير

منه على الشبكة الفسيحة الأرجاء التي تحولت المرأة فيها إلى مجرد أنثى ورمز للمتعة الجسدية فقط.

ومن النصائح التي تبرع الكثيرون بتقديمها للمرأة إذا كانت تتعرض لمضايقات وتحرشات إلكترونية، هي أن تستخدم اسم مستخدم لا يدل على جنسها. فهناك الكثير من الذكور المنحرفين أو المراهقين الذين يجوبون سماء الإنترنت مستخدمين مختلف التقنيات بحثا عن النساء المرتبطات بشبكة الإنترنت طمعا في إرسال رسائل لهن أياً كان نوع هذه الرسائل بريئة أو غير بريئة. وهو أمر تعاني منه كثيرات من اللاتي يرتدن الشبكة، ويصبحن هدفاً للإزعاج والملاحقات التي لا تنقطع. ولحسن الحظ أن كثيراً من الأجهزة والبرامج تتيح لهن وقف مثل هذه الرسائل.

غير أن الشيء المؤسف هو أن الشبكة أصبحت أرضاً خصبة لإقامة أي نوع من العلاقات حتى دون التأكد من هوية الطرف الآخر، وجنسه، وهل هو رجل أو امرأة أو طفل. وهي علاقات قد أدت في كثير من الدول التي تنشأ فيها إلى ما لا تُحمد عقباه نتيجة للثقة السريعة التي يوليها بعضهم للذين يصادفونهم على الشبكة.

فهذه قصة فتاة مسلمة، كتبت لإحدى المجلات تطلب المشورة بشأن علاقة أقامتها عن طريق الشبكة أيضاً، إذ كتبت تقول: «إنها شابة مسلمة عمرها عشرون عاماً، متعلمة وتعيش مع أبيها وأمها وإخوتها العشرة، وتتمتع باحترام الجميع وحبهم. وإنها منذ خمسة أشهر تعرفت

على شاب في السادسة والعشرين من عمره عبر الإنترنت، وأدركت أنهما يدرسان في السنة الدراسية ذاتها. وبعد التعارف أيقنت أنه –كما تقول– إنسان رائع، وأنه يحبها حباً طاهراً، فهو لا يعرف الخداع أو الكذب. وقد كاشفها بكل شيء عن حياته وأخبرها بأنه مقعد على كرسي متحرك، ويعتمد على نفسه في كل شيء، ويعيش حياة طبيعية. وهي تقول إنها أحبته، وكانت تلتقي به على الإنترنت يومياً، أو تكتب له، أو يكتب لها عبر البريد الإلكتروني. وكانا يتحدثان على الهاتف أيضاً لأنه يسكن على بعد(١٥٠) مئة وخمسين كيلومتراً. وتبادلا صورهما، وأن إعجاب كل واحد منهما بالآخر قد ازداد ونما. ثم تذكر لقاءهما، وأنه عرَّفها على إخوته، وهم أسرة طيبة–كما تقول– إذ استقبلوها بترحاب وكرم كبيرين.

وتردف أيضاً بأنهما تعاهدا على الزواج وفكَّرا في المستقبل. وعندها –كما تقول– حان الوقت لإخبار أهلها، وعندما أخبرت أمها غضبت أولاً: لأن ابنتها قد تعرفت عليه على الإنترنت، وثانيا: لأنه مُقْعَدٌ، وطلبت منها قطع علاقتها به فوراً. وقد أدى ذلك إلى أن يسارع والداها بقبول خطيب لها وهو صديق لأبيها. وأنها حاولت أن تتكيف مع الأمر الجديد، ولكنها لم تستطعْ، وأخبرت من أحبت بالأمر فطلب منها الرضا بالنصيب، ولكنها حاولت ولم تفلح فرفضت الخطبة. وحاول والد حبيبها على الإنترنت الاتصال بوالدها ليحدد موعداً للزيارة، لكنه كان يعتذر ويتهرب، ونتيجة لإصرارها هددها والدها بالقتل إن فكرت في الزواج بحبيب الإنترنت، ثم خيَّرها بين الانصياع لأسرتها ونسيان الحب الفضائي، أو خسران أسرتها.

وواقع الحال يقول إن الذين يبحرون في الشبكة يرون العجب العجاب، لذلك تقوم الكثير من الدول بوضع مرشِّحات (فلاتر) تحجب ما يمكن أن يضر أفراد المجتمع، ورغم أن هذه الفلاتر قد لا تكون كافية إلا أنها تخفف من آثار المواقع السيئة التي تتوالد بمعدل كبير كل دقيقة أو دقيقتين، وتشكِّل بما تنشره وتبثه خطراً شديداً على الأسرة والمجتمع، وبالتحديد على المرأة والأطفال والمراهقين، وبخاصة في مجال الجنس والفاحشة والانحراف والإغواء والاستغلال الجنسي للنساء والأطفال. وقد حوَّلتْ كثيرٌ من المواقع المرأةَ إلى مجرد سلعة ورمز للجنس والبهيمية،

أو أداة –في أحسن الأحوال– لترويج السلع والبضائع ودغدغة الأحاسيس والمشاعر من خلال عرض مفاتنها الجسدية بهدف الإثارة الجنسية التي تتجاوز كل حدود الحشمة والحياء، دون مراعاة لأية قيم دينية أو إنسانية، وهو أمر تتيحه الشبكة لأنها مفتوحة أمام الجميع، ولا يوجد أي نوع من أنواع الرقابة عليها سواء أكان تقنياً أم قانونياً، بسبب اختلاف التوجهات والمفاهيم والمعتقدات والقوانين الخاصة بحرية النشر وقانون حماية الخصوصية على الشبكة.

والشبكة تعجُّ بالمواقع التي تتفنن في أساليب العرض والعبث بالمرأة، بل يوجد على الشبكة من يتبرع بإرسال الصور الفاضحة، والمشاهد الجنسية الصريحة إلى كل من يقع عنوان بريده الإلكتروني في أيديهم، أو كلمة السر الخاصة به في أيديهم. وهناك مواقع تتاجر في عري المرأة، وعرض المشاهد الجنسية، وتروج لها، أو تتخذها أداة لتهديد وابتزاز النساء اللواتي يقعن فريسة لمن يخدعهن تحت أي مسمى، ويقوم بتصويرهن وربما كانت بريئة ثم تتم عملية العبث بالصورة وإدخال تعديلات عليها تخدم أغراضهم الدنيئة، فتهدم كيان أسر، أو تؤدي إلى انتحار بعضهن، أو انهيارهن العصبي والنفسي. ولا يسلم من ذلك حتى الأطفال والحيوانات. وهناك مواقع تعمل على جذب الأطفال والنساء واستغلالهم جنسيا ويروج لها منحرفون على الشبكة، وهي بالجملة جرائم لا يقرها قانون أي بلد ولا يسمح بها.

ويستطيع القارئ الرجوع إلى كتابنا السابق (الشبكة وغزل الأشباح)[1] الذي يتناول بشيء من التفصيل المخاطر والمآسي التي قد تتعرض لها المرأة والطفل على الإنترنت.

---

١ صدر عن مدار الوطن للنشر ١٤٢٦هـ



obeikandl.com

## ٢-٥ الأخطار على الخصوصية

من سبق له أن اشترى بضاعة من موقع أمازون الشهير، سيلاحظ أنه بعد شرائه لبضاعة معينة، فإن الزيارة التالية ستجعله يجد أن الموقع قد اقترح له بضائع أخرى مشابهة لما اشتراه سابقاً. قد ينظر بعضهم للجانب الحسن في ذلك، وهو أن الموقع يساعد على شراء ما يحتاجه المتسوق الإلكتروني، ويوصله للبضائع التي تناسب اختياره. ولكن ما يغفله الكثير أن هذا يعني انتهاكاً كبيراً للخصوصية، حيث إن الموقع تم تصميمه لمراقبة المتسوق ومعرفة جميع اختياراته وحركاته. وهذا لا

يقتصر فقط على موقع أمازون، بل يندرج ليشمل الكثير من مواقع المبيعات التي ارتبطت فيما بعد بمواقع الإعلانات لتصبح حياة المرء الشخصية منشورة فيطلع عليها كل من يريد. ولعل بعضنا شاهد أحد الإعلانات التلفزيونية لشركة مقدمة لخدمة الإنترنت التي تبين فيها حرصها على حماية خصوصية المستخدم، ويظهر في ذلك الإعلان مجموعة من الناس يمشون في شارع كبير ويحمل كل منهم لوحة كبيرة، وتحتوي كل لوحة على معلومة شخصية خاصة لكل شخص، مثل (أنا أحب الأفلام المرعبة)، (أنا أعاني من مرض الكبد)، (أنا مطلقة ولدي طفلان) وغيرها من المعلومات التي من المحتمل أن يكون أي منا قد قام بإدخالها في الإنترنت بشكل أو بآخر. وفكرة ذلك الإعلان هو أن تلك الشركة تريد أن تبين لك كيف يتم انتهاك الخصوصية في الإنترنت إذا لم تستخدم منتجهم. وهذا مثال مبسط لتوضيح مدى انتهاك الخصوصية في

الإنترنت، التي تعد الطرف الآخر النقيض لخاصية (انعدام الهوية) في الإنترنت التي جرى الحديث عنها في الفصل السابق.

obeikandl.com

# الفصل الثالث:
# أنواع الجرائم في الإنترنت

obeikandl.com

**سيتطرق هذا الفصل لأنواع الجرائم في الإنترنت، ولقد تم تقسيمها إلى الأنواع الآتية:**

- جرائم ضد الحكومات
- جرائم سرقة المواقع التجارية
- جرائم الابتزاز
- جرائم الحقوق الفكرية
- جرائم الخصوصية
- جرائم الملاحقة والمضايقة
- جرائم المخدرات والعصابات وغسيل الأموال
- جرائم التمييز العنصري
- جرائم الإرهاب

obeikandl.com

## ٣-١ جرائم ضد الحكومات

يحفل التاريخ بالكثير من القصص عن أولئك الذين حاولوا خداع القطاعات الحكومية على مختلف مجالاتها. وعلى الرغم من تعدد الطرق والحيل التي يلجأ إليها المجرمون فإنها في الغالب تكون لتحقيق أحد هدفين؛ الأول: هو التهرب من دفع المستحقات، مثل: الضرائب والرسوم وغيرها. والثاني: هو الحصول على بعض المنافع التي لا يستحق المخالف الحصول عليها عادة.

والمتابع لتطور الإنترنت سيلاحظ أنه في الفترة الأخيرة قد كثر الحضور الإلكتروني للقطاعات الحكومية في الشبكة وظهور ما يسمى بـ (الحكومة الإلكترونية)، حيث يندر أن تجد مصلحة حكومية دون أن يكون لها موقع على الإنترنت تقدم خدماتها من خلاله.

وإن كان من المسلّم به أن ارتباط الجهات الحكومية المختلفة بالإنترنت له فوائد جمة، غير أن هذه الفوائد تجلب معها المخاطر أيضاً، حيث تعد الجهات الحكومية من أكثر الجهات تعرضا للهجمات. ويمكن تقسيم الهجمات على الجهات الحكومية إلى أربعة أقسام رئيسة، وهي كالآتي:

### ٣-١-١ سرقة المنافع

استغل المجرمون تطور الحكومات ودخول الحاسب الآلي في جميع المنافع والإدارات الحكومية، واستطاعوا مهاجمة الإدارات الحكومية المرتبطة بالإنترنت، ثم تعديل البيانات المتعلقة بهم لكي يحصلوا على منافع لا يستحقونها. ومثال ذلك قيام بعضهم بتعديل البيانات الخاصة بالضرائب، وذلك حتى يدفعوا كمية أقل، أو القيام بالدخول على بيانات التأمين الطبي وتعديل البيانات الخاصة بهم وإعطاء أنفسهم صلاحيات ومنافع أكثر مما هو مسموح لهم بها.



obeikandl.com

### ٣-١-٢ سرقة الأموال

ويشمل هذا النوع اختراق الأجهزة المتعلقة بالنواحي المالية، ثم العبث بها حتى يتم تحويل مبلغ من المال لحساب المستخدم أو لعنوانه. ومن الأمثلة على ذلك ما قام به أحد المجرمين من إدخال بيانات وهمية في نظام المحاسبة الخاص بأحد الإدارات الحكومية، بحيث يتم إرسال شيكات له، وأصبح يقوم بالحصول عليها وإدخالها في حسابه. واستطاع بذلك الحصول على مبلغ ٢,٧٥ مليون دولار.

### ٣-١-٣ سرقة المعلومات

لاشك بأن الحكومات تمتلك معلومات أكبر عن مواطنيها، وهذه المعلومات مخزنة في قواعد البيانات الخاصة بالجهات الحكومية المختلفة. وهذا ما يجعل المجرمين يستهدفون الشبكات الخاصة بالجهات الحكومية المختلفة، ويقومون باختراقها للحصول على المعلومات الموجودة في قواعد البيانات الخاصة بها.

ويندرج تحت هذه النقطة أيضا التجسس وسرقة المعلومات الحساسة الموجودة في بعض القطاعات الحكومية ذات الأهمية العالية، مثل القطاعات العسكرية أو قطاعات الاستخبارات، واستخدامها فيما بعد ضد هذه الحكومات. ولعل هذا ما يقوم به المجرمون الذين يقومون بالجرائم بدافع التجسس، وسنتحدث عن ذلك في الفصل الرابع.

### ٣-١-٤ إيقاف أو تعطيل الخدمات الإلكترونية عن العمل

ويعدّ هذا النوع من أخطر التهديدات التي تواجه الحكومات في الوقت الراهن. ومثال



obeikandi.com

هذا النوع من الجرائم ما حدث لجمهورية أستونيا، فقد تعرضت مواقع حكومية ومواقع خاصة بمصارف وشركات اتصالات ومؤسسات إخبارية، لهجمات إلكترونية عبر الإنترنت؛ تعرف بمصطلح الهجمات الموزعة لتعطيل الخدمة، وقد كانت هجمات هائلة ومنظمة وغير مسبوقة، استهدفت البنية التحتية الإلكترونية للدولة على المستويين العام والخاص عبر شبكة الإنترنت، فتسببت هذه الهجمات في تعطيل شبكات البريد الإلكتروني الحكومية، وأدت إلى وقف المؤسسات المالية لتعاملاتها المصرفية التي تجرى عادة عبر شبكة الإنترنت. فضلاً عن تعطيل موقع الرئيس الأستوني ورئيس الوزراء وموقع البرلمان على شبكة الإنترنت، وإغلاق مواقع خاصة بوزارات، نتيجة تعرضها لسيل عارم من الرسائل أدى في النهاية إلى إغلاقها. ويقول خبراء أستونيون كما جاء في جريدة الشرق الأوسط[1] «إن روسيا هي مصدر هذه المشكلة بسبب تغيير أستونيا موقع نصب تذكاري حربي لتمجيد الجيش الأحمر من وسط العاصمة الأستونية في نهاية أبريل ٢٠٠٧، مما أثار غضب الأقلية الناطقة بالروسية واحتجاجات حادة في روسيا التي ما زالت تجد صعوبة في تقبل استقلال هذه الجمهورية السوفيتية السابقة».

ويلاحظ أن جمهورية أستونيا تمتلك عدداً هائلاً من الأهداف التي يمكن مهاجمتها، ذلك أن النجاح الاقتصادي الذي حققته هذه الجمهورية السوفيتية السابقة الصغيرة الحجم قام أصلا على أساس وضعها كمجتمع إلكتروني، فالكثير من التعاملات الحكومية هي إلكترونية، حتى التصويت في الانتخابات يجري عبر شبكة الإنترنت، بل إن الكثير من التعاملات العامة في أستونيا، بما في ذلك التوقيع على الوثائق القانونية تجرى عبر الإنترنت. وقد بدأت الهجمات في ٢٧ أبريل ٢٠٠٧م، بعد مرور ساعات فقط على تغيير موقع النصب التذكاري الذي يعود إلى الحقبة السوفيتية. وكما جاء أيضا في صحيفة الشرق الأوسط أن مسؤولون في أستونيا قالوا: «إن تعليمات وإرشادات حول كيفية تعطيل المواقع الحكومية ظهرت في منابر إنترنت باللغة الروسية». ويعد هذا الهجوم من أنواع الحروب الإلكترونية بين الدول.

١ عدد رقم ١٠٤٠٠ الأحد ٠٣ جمادى الأولى ١٤٢٨ هـ، ٢٠ مايو ٢٠٠٧



obeikandl.com

وقد أدت هذه (هذه التجربة الملموسة) إلى تغيير مهم في طريقة تفكير حلف الأطلسي الذي رد بشكل مباشر بإنشاء مركز امتياز في الدفاع الإلكتروني في تالين عاصمة أستونيا، وتتلقى أستونيا دعما في المشروع من الولايات المتحدة، وألمانيا، ورومانيا، وإيطاليا، وأسبانيا، كما جاء في نفس الصحيفة.

## ٣-٢ جرائم سرقة المواقع التجارية

وهي الجرائم التي يقوم بها المجرمون الذين يلهثون خلف المال، وتعد من أكثر أنواع الجرائم انتشاراً، وتشمل هذه الجرائم اختراق المواقع التجارية التي تقدم خدمة المبيعات عن طريق الإنترنت، ثم الحصول على قواعد البيانات الخاصة بالزبائن المتعاملين مع هذه المواقع والحصول على معلومات بطاقاتهم الائتمانية، واستخدامها فيما بعد للقيام بعمليات شراء غير قانونية. ومن الأمثلة على ذلك ما قام به أحد المخترقين من سرقة قاعدة البيانات الخاصة بموقع (Geeks.com)، مما أدى بالشركة إلى إرسال رسالة إلى زبائنها تطلب منهم إلغاء بطاقاتهم الائتمانية، واستخراج بطاقات ائتمانية بأرقام جديدة. وهذا بالطبع أدى إلى خسارة الموقع لسمعته ولزبائنه. وكذلك أيضا ما يحدث في بعض المواقع التي تسمح للمستخدم بتخزين رقم بطاقته الائتمانية في الموقع بحيث يستطيع الشراء دون الحاجة لإدخال رقم البطاقة الائتمانية في كل مرة، ولقد لوحظ أن المجرمين يقومون باختراق جهاز المستخدم الساذج والحصول على كلمة السر للموقع التجاري، ومن ثَمَّ شراء ما يريدون دون الحاجة إلى معرفة رقم البطاقة الائتمانية. وهذا ما حدا بموقع أمازون (www.amazon.com) الشهير لتغيير إستراتيجيته ومطالبة المستخدمين بإدخال أرقام بطاقاتهم الائتمانية في كل مرة يقومون بعملية شراء.



obeikandl.com

## ٣-٣ جرائم الابتزاز

لا يقل الابتزاز جرماً عن السرقة، والفرق الوحيد بينهما هو أن السرقة غالباً ما تتم باستخدام عامل التغافل أو القوة، بينما الابتزاز يتم في الأعم الأغلب بالتهديد بالعواقب الوخيمة مستقبلا، ما لم ينصاع الضحية لمطالب المبتز.

**وتوفر الإنترنت مرتعاً خصباً لمن يريد الابتزاز، وتساعد المبتزين بأوجه عديدة، هي:**

**أولا:** توفر وسيلة اتصال آمنة بين المبتز والضحية (كما ذُكر في خاصية انعدام الهوية في فصل سابق).

**ثانيا:** يمكن استخدام الإنترنت كوسيلة لتحديد الهدف، وذلك لكون الإنترنت مليئة بالمعلومات التي تساعد على ذلك.

**ثالثا:** تعد الإنترنت وسيلة تهديد مرعبة للضحية، فيكفي المبتز أن يهدد بنشر ما لديه على شبكة الإنترنت ليدب الهلع في قلب الضحية، وذلك لأن وضع شيء على الإنترنت يعني اطلاع الملايين من البشر عليه.

**رابعا:** يمكن استخدام خدمات الشبكة لتحويل المبالغ المادية الناتجة عن الابتزاز مباشرة دون أن يعرف الضحية رقم حساب أو هوية المبتز.

ولعل من أشهر الأمثلة على ذلك، أحد المواقع الذي ذاع صيته في الولايات المتحدة الأمريكية منذ عدة سنوات، حيث قامت إحدى النساء بوضع موقع لتهديد شخص يدعى بيل (Bill)، وقامت بوضع صور له مع طمس وجهه حتى لا يتم التعرف عليه ، وقامت بتوجيه



obeikandl.com

رسالة له عن طريق الموقع بأنه إن لم ينصع لما تريده، فإنها ستقوم بنشر صوره على الإنترنت. وقد اشتهر هذا الموقع بشكل كبير، وتم عرضه في وسائل الإعلام بشكل كبير وأصبح من المواقع المشهورة. وكل يريد أن يعلم من باب الفضول من هو بيل؟ وماذا فعل؟ ليستحق ذلك. ولكن إلى الآن لا أحد سوى بيل يعلم ما تريد هذه المرأة. ويبدو أنه قد انصاع لما تريده منه.


شكل ٣-١: الموقع الذي يهدد المدعو بيل.

## ٣-٤ جرائم الحقوق الفكرية

تعد شبكة الإنترنت في الوقت الحاضر أكبر آلة نسخ في التاريخ، فما يقع في أيدي المستخدمين من مواد يمكن نسخه ونشره في ثوانٍ معدودة إلى ملايين المستخدمين الآخرين، ويندرج تحت هذه النقطة الكثير من النقاط الفرعية، فجرائم الحقوق الفكرية في الإنترنت تتباين درجاتها وأهميتها بشكل كبير، فهناك فرق بين سرقة الطالب لمقال في الإنترنت وتسليمه في المدرسة على أنه هو الكاتب الأصلي، وبين سرقة البرامج الأصلية ونسخها وتوزيعها بشكل غير قانوني في المواقع المختلفة. ولعل الناحية الأخيرة هي التي تتلقى جانباً أكبر من الاهتمام. فهناك العديد من الأسباب التي أدت إلى سهولة واتساع عمليات تبادل البرمجيات المقرصنة عبر الشبكة، ولعل من أهمها الزيادة في عدد مستخدمي الإنترنت بشكل مطرد سنوياً، والزيادة في معدل نقل البيانات لاسيما عند استخدام الإنترنت عن طريق التوصيلات السلكية (الكيبل)، أو خدمة الخطوط الرقمية (DSL) أو عن طريق شرائح الجوال أو الشبكات اللاسلكية، علاوة على انخفاض تكلفة الاتصال بالإنترنت في شتى أنحاء العالم ومجانيته في بعضها. وهو الأمر الذي جعل الشركات الكبرى تتخوف بشدة من نمو معدلات القرصنة عبر الشبكة العنكبوتية، وتحذر من الخسائر الضخمة التي مازالت تلحق بصناعة البرمجيات والشركات العاملة فيها.

وفي مؤتمر المنظمة العالمية للملكية الفكرية (WIPO)، حذر روبرت هوليمان الرئيس والمدير التنفيذي لاتحاد منتجي برامج الكمبيوتر التجاري (BSA)، في الكلمة التي ألقاها في المؤتمر من (أن سرقة المطبوعات والمنشورات مباشرة من شبكة الإنترنت تتصاعد إلى أبعاد خطيرة، الأمر الذي يهدد الصناعات الإبداعية إلى جانب عرقلة مسيرة تطوير التجارة الإلكترونية). وذكر أن الخسائر الناجمة عن قرصنة الإنترنت آخذة في الازدياد بحيث تسهم في النسبة المتعاظمة لإجمالي خسائر القرصنة العالمية التي تقدر بمبلغ ١١ مليار دولار أمريكي في السنة تقريباً، ومشيراً في

الوقت ذاته إلى أن: (وطأة التأثير الاقتصادي لهذا النشاط تتجاوز بكثير حدود صناعة البرمجيات مما يلحق الضرر باقتصاديات الدول في العالم قاطبة، وذلك بانخفاض عوائد الضرائب بشكل بالغ وفقدان أعداد هائلة من الوظائف). وتقدر الإحصائيات عدد الذين يفقدون وظائفهم نتيجة لعمليات القرصنة سنويًا في الولايات المتحدة وحدها بحوالي (١٣٠,٠٠٠) شخص، وأنها تحرم الخزانة الأمريكية من تحصيل ضرائب تصل إلى مليار دولار سنوياً.

فهناك أكثر من مليوني موقع على شبكة الإنترنت تقوم بعرض الحصول على نسخ برمجيات غير مشروعة أو التوصيل إليها أو الإشارة إلى مواقع ذات صلة بها، وهي المواقع التي اصطلح على تسميتها بين من يقومون بجرائم القرصنة في الإنترنت بمواقع(WAREZ). وهي تشتمل على برامج مقرصنة من كل الأنواع التي قد يزيد سعرها بعضها عن عشرات الآلاف من الدولارات في السوق، ويمكن لأي شخص جلب أي برنامج منها دون مقابل، أو بمقابل زهيد، وباستخدام زر الفأرة فقط. وتدرُّ هذه المواقع مبالغ طائلة من الإعلانات التي تتدفق عليها بلا حدود في الغالب من مواقع غير قانونية أو مروجة للرذيلة والإباحية. ويتّبع القراصنة طرق مختلفة للحصول على المزيد من الزوار، مما يؤدي إلى مزيد من الإعلانات مثل استخدام خاصية إعادة التنشيط، أو إعادة التوجيه لإجبار المستخدمين على تحميل صفحات متتالية وإظهار المزيد من الإعلانات. وكذلك طريقة (المصيدة) لإلغاء زر الرجوع إلى الخلف عند زيارة الصفحة، فيقع الزائر أسيراً في قبضة الموقع. وقد أشارت المراقبة غير الرسمية لهذه المواقع إلى أن أكثر من ٦٠٪ من البرمجيات المطروحة على مواقع المزاد في أمريكا وأوروبا هي نسخ مقلدة أو مزورة. ويستطيع مرتادو الإنترنت الاطلاع على تقارير كاملة عن القرصنة في العديد من مواقع الإنترنت.

وعلى الرغم من التحذيرات التي تطلق في هذا الصدد التي تركز على أهمية وجود قوانين صارمة لحقوق الطبع والنشر توفر الأسس الكفيلة لوقف قرصنة الإنترنت، وعلى ضرورة أن تكون الإجراءات الاحترازية والعقوبات المفروضة على الانتهاك المباشر لحقوق النشر والطبع كافية لتعويض صاحب الحق ولردع قراصنة الإنترنت، فقد أظهر المقلدون القدرة على التكيف

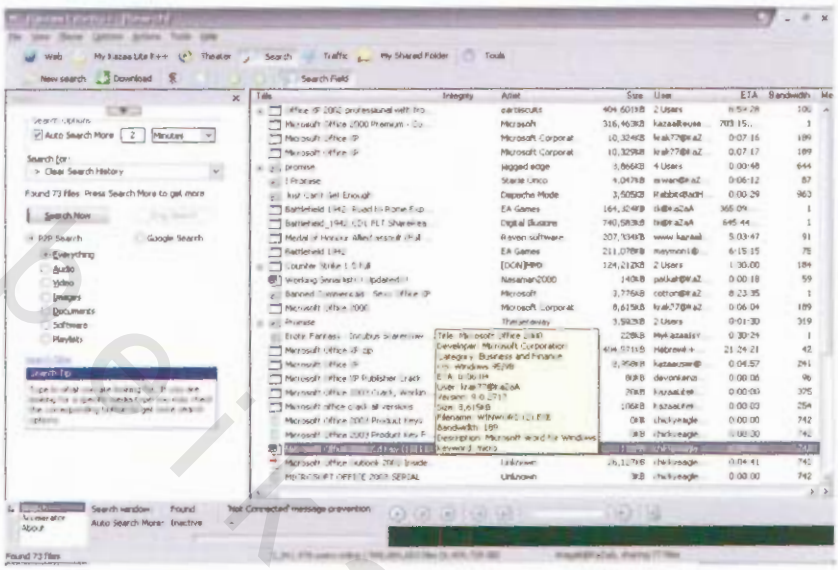


obeikandl.com

مع تطورات السوق المشروعة وتطورات التقنية وسعوا جاهدين لإيجاد طرق تمكنهم من استخدام أدوات التجارة الإلكترونية لإلحاق الضرر بأصحاب الملكية الفكرية. وقد برهن قراصنة الإنترنت- كمعظم المجرمين- على تميزهم بالدهاء وسرعة التكيف والعمل باستمرار على ابتداع طرق تتفق مع التقنية وتتيح لهم القيام بأعمالهم غير المشروعة.

والشيء العجيب أن لهؤلاء القراصنة مبررات لما يقومون به من أعمال القرصنة وسرقة أموال الآخرين دون وجه حق. فمثلاً يعلن العديد من أصحاب مواقع القرصنة بأنهم يقومون بذلك إسهاماً منهم في نشر المعلوماتية التي تحتكرها شركات البرمجيات الكبرى الشرهة التي تطالب بأسعار مُبَالَغٍ فيها لبرامجها، متناسين بأن بيع البرامج المقرصنة لا يختلف عن بيع أي بضائع مسروقة، إذ يجنون من خلال بيعها بأسعار زهيدة أموالاً طائلة، متجاهلين ما تبذله هذه الشركات من جهد ومال وساعات عمل طويلة في إنتاج هذه البرمجيات. والشيء الأكثر غرابة وإثارة أنهم يقدمون الكثير من هذه البرامج عبر شبكة الإنترنت مجاناً، تباهياً بقدراتهم على اختراق أنظمة حماية النسخ التي توضع على البرامج، أو بحجة غلاء البرامج الأصلية وعدم استطاعة معظم مستخدمي الحواسيب اقتناءها، وهي خدمة-على حد زعمهم- يقدمونها لطلاب المدارس والجامعات الذين يشكلون نسبة كبيرة من مستخدمي البرامج المقرصنة في جميع أنحاء العالم. ولعل بعض ما تم ذكره من أسباب صحيح وواقعي ولكن ذلك لا يجيز -ألبتة- سرقة الحقوق وإهدارها.

ومن الناحية الأخرى فلزائري مواقع القرصنة هم أيضاً مبرراتهم الغريبة، فهم كما يزعمون، يمارسون فلسفة (الاستخدام العادل) طالما أن شروط الاستخدام التي تضعها شركات البرمجيات الكبرى غير عادلة. ويقول بعضهم إنه في حالة إحساسهم بعدم إنصاف قوانين استخدام البرمجيات وإجحافها، فإنهم لن يتقيدوا بها وسيقومون بجلب البرامج من مواقع القرصنة في الإنترنت. ويقول آخرون مثلاً: إن أكثر من ٦٠٪ من برامج الحاسب رديئة، ولا تفي بمتطلباتهم، علاوة على غلاء ثمنها بصورة مبالغ فيها، مما يزين لهم الذهاب إلى مواقع (Warez).



شكل ٣-٢: لقطة لبرنامج كازا الخاص بتبادل الملفات في الإنترنت

وخلاصة القول؛ إن القرصنة مستمرة بخطوات قوية وجريئة وفي جميع مجالات البرمجيات والبيانات المتداولة على الشبكة، إذ لم ينجُ منها مجال من مجالات الإبداع أو الفن أو الأدب، ووصلت إلى مجالات لم تكن تخطر على البال، مثل ترويج محاكيات (Emulators) لأنظمة الحاسب المختلفة، وقرصنة برامجها، وقرصنة الدارات الإلكترونية لمحاكيات أنظمة شركات الألعاب وتحويل الألعاب إلى صيغة رقمية وغير ذلك كثير. ولا أحد يدري على وجه اليقين ما هي المجالات التالية للقراصنة؟ وما مدى استعداد الشركات المنتجة والمبدعين لمحاربة هذه الظاهرة الجُرْمية المستشرية؟

## ٣-٥ جرائم الخصوصية

بدا واضحاً أن المعلومات الشخصية أضحت تجارة رائجة ومربحة على الشبكة، بالرغم من التحذيرات التي تطلقها كثير من شركات الهاتف، وشركات تقديم الخدمات المختلفة، ومراكز جمع المعلومات وتصريحاتها العلنية، بأنها ستعد جميع المعلومات التي تحصل عليها معلومات غير سرية، وأنّ لها الحق في استخدامها بالطريقة التي تروق لها من نشر، أو نقل إلى جهات أخرى دون قيد أو شرط، أو أي نوع من الالتزام تجاه أصحابها أو المساءلة القانونية.

وبالطبع فإن هذه التحذيرات لم تأتِ من فراغ، لأن النشر والنقل لمعلومات شخصية دون موافقة أصحابها ومعرفتهم المسبقة لما سينشر عنهم، يشكّلُ تحدياً سافراً للخصوصية وحماية الحياة الشخصية على شبكة الإنترنت، وهو يفتح باباً واسعاً للابتزاز والتهديد والتشهير، خاصة في ظل عدم وجود القوانين والتشريعات التي تحمي الأفراد من مثل هذا التعدي للخصوصية، واستخدام المعلومات الشخصية دون تصريح من أصحابها.

ولقد راجت تجارة المعلومات الشخصية منذ زمن طويل، ولكنها وصلت عبر شبكة الإنترنت إلى أبعاد شديدة الخطر، لأنها أصبحت في متناول الجميع دون استثناء، علاوة على أن مهمة جمعها أصبحت سهلة للراغبين في ذلك من مراكز وشركات ومنظمات وأفراد، بغض النظر عن الغرض من جمعها واستخدامها.

ويشمل جمع المعلومات كل شيء بدءاً من التقارير الطبية، وشهادات الميلاد، والوفيات، ورخص قيادة السيارات، والوثائق المختلفة مثل: وثائق الملكية، والأحكام القضائية، وأرقام البطاقات المختلفة التي أصبحت سمة العصر مثل بطاقة الائتمان، وخدمات الهاتف، والتأمين الطبي، والعضوية، وانتهاء ببطاقات الدخول لمواقع العمل أو مراكز البحث.

والشيء المثير للمخاوف في كل هذا هو أن المراكز والشركات والمؤسسات التي تقوم بجمع



obeikandl.com

المعلومات التي تحمل جميع التفاصيل الخاصة، كما أسلفنا، من اسم الشخص وسنّه وجنسه، وعنوانه، واسم وظيفته ونوعها وعنوانها، والشهادات الدراسية التي حصل عليها، وخبراته العملية، واهتماماته وهواياته ومحلات التسوق المفضلة، بل وحتى نوع المأكولات التي يأكلها، والألبسة التي يلبسها، ونوعية مدارس أبنائه وبناته وعناوينها، ولا تكتفي بجمع المعلومات بمجرد الجمع والترويج للسلع وإنعاش المبيعات، بل تكوّن منها قواعد بيانات خاصة للتسويق والبيع لمن يرغب من أصحاب الشركات الذين يتحرون عن موظفيهم، أو المحامين الذين يريدون معرفة السجلات القضائية لموكليهم، أو لتوريط أشخاص لصالح آخرين أو إلى رجال أعمال الراغبين في معرفة المراكز المالية لشركاء حاليين أو محتملين، أو التحقق من حالة الإفلاس، أو الدخول في صفقات تجارية، أو لرجال عصابات، أو ربما لإرهابيين ينوون ارتكاب جرائم أو القيام بتفجيرات.

ويتمثل خطر المتاجرة بالمعلومات التي تمَّ جمعها وتحويلها إلى قاعدة معلومات أو بيانات توظف لمصالح خاصة لمن جمعها، في الأخطاء التي ترتكب عند إعطاء المعلومات عن الشخص المعني، وبذلك يقع كثيرون ضحايا لهذه الأخطاء. وهناك الكثير من الأمثلة في هذا الخصوص، فهناك مسؤول في مركز صحي مثلاً فُصِل من عمله بسبب خطأ مطبعي في عنوانه، إذ ورد في العنوان أنه يقيم في نادٍ للعراة، وكذلك تعرض موظف آخر إلى مصادرة راتبه، لأن خلطاً حصل بينه وبين أب محكوم عليه بدفع نفقة لابنه وهو يرفض دفعها، وغير ذلك كثير.



obeikandl.com

## ٣-٦ جرائم الملاحقة و المضايقة

تنتشر في بعض الدول مشكلة ما يسمى بالملاحقة، وهي ناتجة عن تعلق شخص بآخر (غالباً من الجنس النقيض) دون رغبة أو رضا الطرف الآخر، ومن ثم ملاحقته وتتبع خطواتهم مما يسبب لهم المضايقة وعدم الارتياح. وفي الغالب فإن الملاحقين كثيراً ما يكونون مسالمين ويفعلون ما يفعلونه من تتبع الضحية بدافع الحب والتعلق. ولكن في بعض الأحيان، يصاحبه بعض الأذى مما يحوّل هذا الفعل إلى مضايقة.

تعد شبكة الإنترنت مرتعاً خصباً لمن يريد أن يتتبع أو يلاحق شخصا آخر، فهي تحتوى على الكثير من المواقع التي تساعد على ذلك، منها ما هو غير قانوني كما ذُكر في قسم (جرائم الخصوصية)، ومنها ما هو قانوني، مثل توفير دليل الهاتف على الإنترنت الذي يمكّن من الحصول على رقم الهاتف والعنوان (أحياناً) للشخص الذي يُبحث عنه.

وتتراوح قدرات المواقع والمعلومات التي تزود بها، بين الحصول على معلومات اساسية، مثل: رقم الهاتف والعنوان، إلى معلومات مفصلة، مثل: مكان العمل والمعلومات المتعلقة بالتعاملات المادية. بالطبع فإن هذه المواقع تختلف من بلد لآخر، ففي بلد متطور مثل الولايات المتحدة الأمريكية، فإن معظم قواعد البيانات الكبيرة متوفرة على الإنترنت، ومثال ذلك موقع (www.555-1212.com) الذي يعطي معلومات متكاملة عن الشخص بمجرد إدخال رقم هاتفه. وكذلك موقع (www.usatrace.com) الذي يسمح بإدخال رقم الضمان الاجتماعي (Social Security) الخاص بالشخص (وهو رقم مشابه لرقم بطاقة الأحوال الشخصية) لكي يقوم الموقع بتحديد موقع الشخص المطلوب. ويضاف إلى ذلك الشبكات الاجتماعية مثل: فيسبوك، وتويتر، وجوجل+، وغيرها من مواقع التواصل الاجتماعية التي وصل مشتركو هذه المواقع إلى قرابة المليار شخص، وهذا ما أنشأ سوقاً رديفاً لمن يريد أن يتتبع أو

يستعلم عن أي شخص وماذا لديه من حسابات إنترنتية، وما هي توجهاته وطريقة تفكيره، وهي جزء من الهندسة الاجتماعية. و لا يغالي الإنسان إذا ما قال إن شبكات التواصل الاجتماعي جعلت المرء مكشوفا مثل من يدخل حماما من دون أبواب أو نوافذ!

أما بالنسبة للمضايقة، فيتم ذلك غالبا باستخدام مواقع المحادثة أو باستخدام البريد الإلكتروني. وتبين الإحصائيات أن أغلب من يقوم بالمضايقات هم من الرجال، وأن من يتعرضون للمضايقات هم من النساء والأطفال. وكما ذكر في قسم (الأخطار النفسية) فإن بعض مدمني استخدام الإنترنت لديهم مشاكل نفسية، مما يجعلهم يتعلقون بأشخاص آخرين في الإنترنت بشكل غير صحي، وهذا بدوره يؤدي لقيامهم بمضايقة الطرف الآخر. بل لاحظت الدراسات أن معظم من يقومون بالمضايقات تكون بداية علاقتهم بالطرف الآخر علاقة ود، ما تلبث أن تتحول إلى عداء مع تجاهل الطرف الآخر. ولو كان الخطر الوحيد من المضايقة هو الرسائل الإلكترونية لكان من الممكن تجاهلها، ولكن في أحيان أخرى فإن هذه المضايقة تصل أحياناً إلى مستوى غير محمود، عندما يمتلك من يقوم بالمضايقة معلومات عن الضحية، مثل رقم بطاقته الائتمانية حيث يقوم باستخدامها للانتقام من الضحية. أو الحصول على عنوانها بحيث يتمكن من الوصول إليها شخصياً!

ولقد انتشرت الكثير من المواقع التي تساعد المستخدمين، وخصوصا النساء، لكي لا يتعرضوا للمضايقات على الإنترنت ومن هذه المواقع (www.lovemenot.org) و(www.cyberguards.com/cyberstalking.html). وغيرها من المواقع الأخرى الكثيرة. انظر الشكل ٣-٣.



obeikandl.com


شكل ٣-٣: إحدى صفحات موقع www.lovemenot.org

وكمثال قريب على هذه المضايقات ما حدث في المملكة العربية السعودية مؤخرا في منطقة الإحساء شمال شرق السعودية، من قضاء محكمة سعودية بسجن شاب سعودي وجلده وتغريمه، بعد اتهامه بارتكاب جريمة إلكترونية عبر الإنترنت مثال حي لوجود مثل هذه الجرائم في مجتمعنا، فقد أمرت المحكمة بسجن مواطن وجلده وتغريمه، بعدما ثبت أنه قام باختراق البريد الإلكتروني الخاص بفتاة سعودية، وسحب صورها الشخصية منها، وابتزازها. وكما جاء في صحيفة الوطن السعودية على لسان رئيس المحكمة الجزئية في الإحساء، أن المحكمة عدت الشاب قد ارتكب (جريمة إلكترونية)، وتم معاقبته وفق نظام مكافحة الجرائم الإلكترونية السعودي. وأشار إلى أن الحكم الذي يعد أول حكم قضائي يعاقب فيه متهماً في جريمة إلكترونية كان تطبيقاً لنظام مكافحة الجرائم الإلكترونية.

## ٣-٧ جرائم المخدرات والعصابات وغسيل الأموال

تقول الإحصائيات إن أرباح تجارة المخدرات في الولايات المتحدة وحدها تتجاوز ثمانين مليار دولار أمريكي سنوياً، وهو رقم يفوق الدخل الكلي لأكبر خمس مئة شركة أمريكية. وقد سهلت الحاسبات المرتبطة بشبكات ثم بشبكة الإنترنت، كافة عمليات هذه التجارة وإجراءاتها، وبذلك قللت من الأخطار التي كان يتعرض لها المهربون والمروجون وخفضت تكاليفها. ويوجد على الشبكة الآن آلاف المواقع التي توفر حتى أدق المعلومات عن تحضير وصناعة أنواع مختلفة من المخدرات، والعقاقير المخدرة، والأقراص، والحقن، وفنون وطرق تعاطيها، وطرق إخفائها ونقلها وترويجها.

ونتيجة للعدد الهائل من الصفقات التجارية على المستوى الدولي التي تعقد يومياً، فقد أصبحت عملية مراقبة صفقات الإجرام ومتابعتها تُعَدُّ شبه مستحيلة، لصعوبة التمييز بين الصفقات المشبوهة وغير المشبوهة. وقد ساعد في هذا المجال أيضاً إمكانية ربط الحاسبات الآلية الصغيرة المحمولة أو الموجودة في المنازل بنظام الحاسب الآلي المركزي التابع لبنك معين، والذي يمكّن المستفيد من التصرف في حسابه المصرفي، وهو في منزله، أو متجره، أو سيارته، أو في الطائرة، أو الباخرة. وهو تطور سيمكن المجرمين من عقد الصفقات المالية المشبوهة، وتمويلها وتنفيذها بكل سهولة ويسر، بمجرد النقر على أزرار هذا الحاسب الصغير بعيداً عن أعين العدالة وقبضتها الصارمة.

وقد ورد في تقرير لبنك دبي الوطني أن عمليات غسيل الأموال في روسيا تشكل من

٢٥-٥٠٪ من الناتج المحلي، و١٠٪ من إجمالي الناتج المحلي لجمهورية التشيك، و٧-١٣٪ من إجمالي الناتج المحلي البريطاني. ومن إجمالي المبالغ المغسولة عالمياً البالغة ٣١ ألف مليار دولار كان نصيب سويسرا (٥٠٠) مليار دولار، والولايات المتحدة الأمريكية (٤٨) مليار دولار، والمكسيك (٣٠) مليار دولار، وكندا (١٧) مليار دولار.

وتمثل تجارة المخدرات المصدر الأول للأموال المغسولة يليها أموال الاحتيال المالي، عبر شركات التأمين وإعلان الإفلاس، علاوة على الرشاوى لموظفي الدول والحكومات وأموال العصابات المنظمة.

وقد عرَّف بعض المختصين مصطلح (غسيل الأموال) الذي هو ترجمة حرفية لعبارة (Money Laundring) بأنها: «العملية التي يلجأ إليها الذين يمارسون الاتجار غير المشروع في العقاقير المخدرة، أو الممنوعات بشكل عام، بهدف إخفاء مصادر دخلهم غير المشروعة، أو لاستخدام هذه الدخل في وجه غير مشروع، ومن ثمّ التمويه على الأجهزة النظامية، ليبدو وكأنه دخل مشروع ولا يثير الشبهات». ولذلك فهم يحتفظون بهذه الأموال بشكل نقدي حتى يسهل عليهم إيداعها في بنوك بلدان أخرى في حسابات سرية. ويطلق على عملية غسيل الأموال أيضاً عبارات، مثل: (تطهير الأموال)، و(تبييض الأموال)، و(تنظيف الأموال)، وهي مصطلحات غير معروفة على المستوى العام مما يسبب مشكلة كبيرة للحكومات في محاربتها، فضحاياها غير معروفين وتأتي متأخرة في قائمة تسلسل الجرائم بعد السطو والسرقة وغيرها من الجرائم.

وتشكل عملية غسيل الأموال هاجساً كبيراً للجهات الأمنية في شتى بقاع الدنيا، لأن بقاء السيولة الضخمة في أيدي المجرمين سيؤدي إلى تفاقم ظاهرة الإجرام وزيادة سطوته الاقتصادية، وتمكين المجرمين من الهيمنة على المشروعات الكبرى واحتكار الأسعار.

## ٣-٨ جرائم التمييز العنصري

إن شبكة الإنترنت كما سبق أن ذكرنا لا تختلف عن عالمنا الذي نعيش فيه، ويتعرض

مرتادوها لما نتعرض له. فالشبكة زاخرة بالمواقع المخصصة لمنظمات عرقية للبيض ولغيرهم، لها شعارات مختلفة ودعوات عنصرية بعضها يتخذ طابعا سياسيا أو دينيا كالصهيونية والنازية، أو منظمات التطرف الديني، أو التمييز العرقي، أو اللوني كما هو الحال في العديد من بلدان العالم التي تبرز فيها مظاهر العنصرية بين الملونين كأمريكا، والتمييز بين الهنود الحمر (السكان الأصليين)، والزنوج وغيرهم من ذوي الأصول الآسيوية. فالشبكة تعكس الواقع المعيشي في كثير من البلدان التي تمارس فيها مثل هذه التفرقة. ويلاحظ المتتبع لمثل هذه المواقع وجود نوعين من العنصرية؛ أولاهما ناجمة إلى حد كبير عن عقليات مضطربة ومشوشة، ونفسيات غير سوية، والنوع الآخر من قبل أشخاص نهجوا نهجاً عدائياً، ووضعوا خططاً تآمرية، فيلجؤون إلى إهانة الآخرين في المنتديات وغرف الحوار، ويعمدون إلى طمس الحقائق، ويدعون آخرين من الذين لديهم صلات بهم إلى ممارسة النهج ذاته مع الآخرين من مرتادي الشبكة الذين يقودهم حظهم إلى مواقعهم.

ومن أكثر مشاكل العنصرية بروزاً على الإنترنت، مشكلة الزنوج والهنود الحمر. فالزنوج لهم تاريخ طويل حافل بالصراع بينهم وبين الرق والاستعباد. وهناك العديد من المواقع على الإنترنت التي تدعو للتفرقة وتطرح مفاهيم في غاية الغرابة والسخف، تقول باستحالة العيش بانسجام بين البيض والسود في أمريكا. وهناك مواقع مثل (www.kkk.com) الخاص بمنظمة تسمي نفسها (The Ku Klux Klan) تنادي بمثل هذا التوجه بقوة وصلف.

وتكمن خطورة هذه المواقع في أنها تمثّل عدداً من الجماعات العنصرية التي لها جمعيات تحمل تسميات عرقية صريحة، مثل: جمعية (The White Race) ومجموعة (American First) و(The Constitution)، إذ إن المنتمين إليها يؤمنون إيماناً قاطعاً بما يقولونه وينشرونه في مواقعهم، ويدعون إليه، لدرجة أن كل مؤلف أو كاتب يوقع على صفحاتهم التي كتبوها، حتى أنهم يشيرون للتظاهرات التي شاركت وستشارك فيها جمعياتهم. وما الجريمة المروعة التي ارتكبها الطالبان (Eric Harris) و(Dylan Klebold) وهما عضوان في عصابة تضم طلابا عنصريين، يكنون كراهية شديدة للزنوج ولأسبان أمريكا اللاتينية والأقليات العرقية الأخرى، أطلقت على نفسها اسم مافيا ترنشكوت (Trenchcoat)، إلا مثالاً واضحاً على هذه العنصرية والحقد والكراهية. وهذان الطالبان مولعان بتقليد الأشرار في كل شيء، حتى في المظهر والحركات، ويطلقان شعارات هستيرية تحض على القتل وكراهية الملونين وخاصة الزنوج. والغريب أن هذين الطالبين ضليعان جداً في استخدام الحاسب، ومولعان بألعاب الحرب، ويملكان مسدسين يفاخران بهما، وبهذين المسدسين نفذا مجزرة مدرسة كولمباين (Columbine) الثانوية في مدينة ليتلتاون بولاية كولورادو الأمريكية، وقتلا خمسة عشر طالباً، وزرعا شحنات ناسفة في سيارة مجاورة للمدرسة. وقد انتهت حياتهما بانتحارهما في مكتبة المدرسة بعد ساعات من ارتكابهما لجريمتهما البشعة في شهر أبريل من عام ١٩٩٩. وبعد ذلك قامت شركة أميركا أونلاين بحجب موقع العصابة -التي أثارت الرعب في أمريكا- على الشبكة.

وأما الهنود الحمر، وهم المواطنون الأصليون في أمريكا، فإنهم يتعرضون للتفرقة من معظم الثقافات والأقليات العرقية الأخرى، وليس من البيض فحسب، وبعبارات واضحة وصريحة على شبكة الإنترنت التي تتيح للكثيرين عرض وجهة نظرهم عنصرية كانت أو غير عنصرية. وتؤثر وجهات النظر هذه بالطبع على كثير من الذين يفتقرون إلى الوعي من الأميين أو محدودي الثقافة والتعليم.

وأما الحملة العنصرية الأكثر شراسة ونجاحا، فهي التي تشنها المواقع الصهيونية ضد العرب على شبكة الإنترنت، وهي تستهدف العرب والنازية ومنتقدي الصهيونية. وتتضح ممارساتها العنصرية في تزييف التاريخ القديم والحديث، بالشكل الذي يخدم مصالح الصهيونية وتشويه صورة العرب وإطلاق تهمة معاداة السامية. والأدهى والأمر أن كمًّا هائلاً من مواقع الإنترنت المعادية للعنصرية تحبُّ جميعها للدفاع عن الصهيونية ومن ينتقدونها وتتهمهم بالعنصرية، خاصة وأن المواقع العربية ليس لها وجود واضح، ولا تملك منهجية واضحة للدفاع عن العرب وفضح ممارسات الصهيونية وجرائمها، بالإضافة إلى عدم عمق الرؤية وأخذ الأمر بالجدية المطلوبة من أشخاص مؤهلين للقيام بمثل هذا العمل.

وتقترن العنصرية في كثير من المواقع بإثارة البغض والكراهية، فقبل عدة سنوات كان عدد المواقع التي تحض على الكره قليلة العدد، ولكن الآن توجد على شبكة الإنترنت مواقع عدة بعضها مثير للاشمئزاز لدرجة الغثيان. فأحد هذه المواقع تديره ما تُعرف بكنيسة الخالق (Church of the Creator) وهي المجموعة التي كان (بنجامين سميث) البالغ من العمر ٢١ عاماً أحد أفرادها حتى تاريخ انتحاره. ومع أن الموقع في غاية السوء،إلا أن هناك مئات المواقع الأخرى تفوقه سوءاً. وقد تعّرف مركز سيمون ويسنثال (http://www.wiesenthal.org) الموجود في لوس أنجلوس، والذي يهتم بمتابعة المواقع المثيرة لنزعات الحقد والكراهية والعنصرية، على أكثر من (١٤٠٠) موقعاً نسيجياً من هذا النوع، وهي تتضاعف عاماً بعد عام، وهذا الرقم ذاته قد يكون أقل كثيراً من الرقم الحقيقي لهذه المواقع السيئة السمعة.

## ٣-٩ جرائم الإرهاب

إن من أخطر آثار الإنترنت في انتشار الجريمة، هو اشتمالها على مصادر للمعلومات عن صناعة القنابل والمتفجرات، وتعليم مختلف فنون القتال، بل والتدريب على القتل بأعصاب



obeikandl.com

باردة، مع شرح أساليب تعذيب الضحية قبل قتلها، ثم القتل باستخدام وسائل مختلفة بعد التوثيق بالقيود. وقد تم رصد ما يزيد عن (١٥٠٠) موقعاً تشتمل على معلومات لتعليم صناعة القنابل والمتفجرات على الشبكة.

وما دام عالم الشبكة الافتراضي يمثل انعكاساً لحقيقة ما يجري في العالم الواقعي، فإن عالم الشبكة تتوفر فيه دوافع الجريمة والقتل والعنف، كالتمييز العنصري، والتطرف السياسي والديني، والانحراف الفكري، والتطهير العرقي، والكراهية ومحاولات الإفساد وإثارة النعرات في المجتمعات، وكل الأمراض والانحرافات التي تصيب المجتمعات.

والأخطر من وجود العوامل والدوافع هو استثمارها من قبل مجموعة يمكن أن يطلق عليها (القيادة الخفية)، فهي شكل مختلف من أشكال التوجيه والتحكم، وتقوم به مجموعات مختلفة تنشط عبر الإنترنت، وتسعى إلى إخضاع قطاع عريض من الناس للرقابة والمتابعة بهدف دراسة اهتماماتهم وتطويعها، أو توجيه أفكارهم وتغذيتها بالعناصر العدائية تجاه الآخرين، ليكونوا أداة لينة لتحقيق الأهداف والغايات الخاصة بكل مجموعة.

وبلا شك فإن وجود الجريمة يبرر اللجوء إلى اقتناء السلاح، للدفاع عن النفس لعدم الإحساس بالأمان في مجتمع يقتني فيه آخرون السلاح، بهدف ارتكاب جرائم وتهديد أمن المجتمع، وهو أمر متاح تماماً من خلال المعلومات المتوفرة عن صناعة الأسلحة والمتفجرات، أو تسهيل عملية الحصول عليها. فمثلاً يقدم موقع جنة القنّاص على العنوان (www.snipersparadise.com) كما في الشكل ٣-٣، معلومات عن فن القنص وأدوات الترصد الليلي، والتنكر وغيرها من الأدوات اللازمة لقنص الحيوانات والبشر معاً. والقنص هو أحد أهم وسائل ارتكاب جرائم القتل في كثير من البلدان التي تنتشر فيها الجريمة المنظمة، مثل أمريكا وإيطاليا وروسيا. ويعد هذا الموقع واحداً من المواقع التي تروج لبيع الأسلحة عبر الشبكة وتتعاون مع متاجر حقيقية في عمليات البيع. وهناك مواقع تعرض أسلحة



obeikandl.com

لشركات محددة، وأخرى تقوم بعمليات بيع مباشر كاملة أسوة بالمتاجر الإلكترونية، وأخرى تدعو مرتاديها لتعبئة استمارات أو المراسلة بالبريد الإلكتروني لعقد صفقات الشراء.

أما التأثير الأخطر للإنترنت فهو ما توفره بعض المواقع من معلومات، حول صناعة الأسلحة والقنابل كصناعة قنبلة من الموز مثلاً. وهناك قصة تناقلتها وكالات الأنباء عام ١٩٩٦م، عن طالب جامعي ابتكر طريقة شديدة السهولة لصناعة قنبلة نووية، من خلال مجموعة من المعلومات التي جمعها من الصحف والمجلات ومجموعات النقاش وغرف الحوار. وتتوفر على الإنترنت كذلك معلومات تقود إلى صناعة المتفجرات والمواد السامة.

والمشكلة الحقيقية فيما يتعلق بتجارة الأسلحة عبر الشبكة، هي أن قوانين بعض البلدان تبيحها، وبعضها تحظرها وتعدّها غير شرعية. ولكن تخطي الشبكة للحدود الجغرافية لهذه البلدان وتلك، يجعل هذه التجارة تنطلق إلى بلدان أخرى تحظرها قوانينها. وتوجد على الشبكة آلاف المواقع التي تعمل في تجارة الأسلحة والترويج لها وتقديم الاستشارات لبيع الأسلحة وشرائها. وتقوم كثير من الدول بمتابعة المشاركين في المواقع التي تدعو إلى الإرهاب والإفساد، لتعرية خيوطها من جهة وللحد من انتشارها من جهة أخرى. ومثل هذه المتابعة تحتاج إلى قدرات فنية عالية للتعرف على من يقف خلف هذه الدعوات الإفسادية من جهات داخلية وخارجية.


شكل ٣-٣ صورة أحد المواقع المخصص لبيع الأسلحة

# الفصل الرابع :
# دوافع الجريمة

obeikandl.com

يذكر علماء النفس، أن الجريمة تتمحور حول ثلاثة عوامل: الدوافع، ووجود الأهداف المناسبة، وغياب الحماية عن هذه الأهداف. وبناء على ذلك فسيتحدث هذا الفصل عن دوافع الجريمة في الإنترنت، ويمكن تقسيمها للأقسام الآتية:

- الطمع وحب المال
- الحقد والانتقام
- التسلية والفضول والرغبة في التحدي
- السياسة وحروب المعلومات

obeikandl.com

## ٤-١ الطمع وحب المال

يعدّ المال من أكبر الدوافع وراء ارتكاب الجرائم بمختلف أنواعها، سواء كانت في الإنترنت أو في الحياة الواقعية. ولا شك أن الإنترنت تحتوي على الكثير من الأهداف التي يستطيع المجرم محاولة سرقتها. بل إن بعض المجرمين يقومون بتصميم موقع تجاري وهمي، يعرض نوعية من البضائع ويقوم بجمع أرقام البطاقات الائتمانية، ولكنه لا يقوم بتوصيل أي من البضائع للمشتري. ويقوم بإغلاق الموقع بعد جمع عدد كاف من البطاقات الائتمانية. ويحدث ذلك إما بوضع إعلان قوي وتخفيض مغرٍ جداً، وفتح الموقع لبضعة أيام ، ومن ثم إغلاقه، أو أن تقوم إحدى هذه الجهات المجرمة بالتمويه والعمل لمدة سنة وتوصيل المشتريات إلى طالبيها، حتى يحين موعد استغلال بطاقات الائتمان ويتم إغلاق الموقع بعدها.

## ٤-٢ الحقد والانتقام

من المعروف بأن من يوجد لديه الحقد أو الرغبة في الانتقام، فإنه لا يهدأ له بال ولا يغمض له طرف، حتى يقوم بتحقيق مبتغاه. وتصبح نار الحقد وقوداً وحافزاً كبيراً للقيام بكل ما هو لازم لتحقيق الغاية والهدف النهائي. والكثير من الجرائم في الإنترنت كان الحقد والانتقام هو الدافع الرئيس من ورائها، فهذا موظف مفصول من شركته قام باختراق شبكة شركته لكي ينتقم، وهذه مجموعة (HFG) المكونة من القراصنة أو المخترقين، تقوم باختراق موقع جريدة نيويورك تايمز وتغيير صفحتها الرئيسة، وذلك انتقاماً من أحد محرري المجلة الذي كان يكتب مقالات كثيرة مطالباً بإدانة الهاكر كيفن ميتنك.

ولعل أكثر الجرائم التي يكون دافعها الحقد والانتقام تبوء بالنجاح، وذلك لأن المجرم

في الغالب يكون له تاريخ مع الضحية يعطيه ميزة أفضل من غيره من المجرمين الذين لا يمتلكون أي معرفة بالضحية. فالشخص الذي يريد اختراق شبكة شركته التي فصل منها يعرف في الغالب تصميم الشبكة ونقاط الضعف فيها، وكذلك فإنه قد يحضر لنفسه باباً خلفياً يمكنه من تجاوز الإجراءات الأمنية. والشخص الذي يريد الانتقام من شخص يعرفه يكون في الغالب ملماً بمعلومات إضافية تساعده على ارتكاب جريمته، مثل الاسم الذي يستخدمه الشخص في المحادثة، أو المنتديات التي يزورها، وكذلك قد يعرف اسم جهازه أو البرامج والمنافذ المفتوحة في جهازه، وغيرها من المعلومات الأخرى.

ويندرج تحت هذا القسم أيضا من يكون دافعهم الحقد على شركة معينة أو نظام معين، وهذا القسم يطلق عليه بعض خبراء الشبكات اسم (المخترقون الغاضبون)، ولعل أكثر الشركات استهدافاً من قبل هؤلاء هي شركة مايكروسوفت التي تمتلك الكثير من الأعداء الذين ينتمون في جلتهم إلى فئة داعمي البرامج المفتوحة، وهمهم الأول إيجاد المشاكل في برامج مايكروسوفت عن طريق اختراقها، لإثبات أن اتباع مبدأ (البرامج المفتوحة) هو أكثر أمناً وفعالية.

## ٤-٣ التسلية والفضول والرغبة في التحدي

يوجد الكثير من المجرمين في الإنترنت الذين يقومون بالجرائم المختلفة، لا لشيء إلا للتسلية والرغبة في تحدي أنظمة الحماية المختلفة. وفي الغالب فإن هذه المجموعة من المخترقين يكونون صغاراً في السن، ولا يوجد لديهم أي من الدوافع الأخرى التي ذكرناها، ويكون الدافع الوحيد لديهم هو التسلّي برؤية نتاج أفعالهم، ورغبة منهم بالإحساس بالقوة والسيطرة بما يشبه

عملية استعراض للعضلات، باختراق وأنظمة الحماية المختلفة في الإنترنت وكسرها. ولعل من أشهر الأمثلة على ذلك الهجمات الفريدة النوع التي استهدفت المواقع الشهيرة، مثل: (CNN) و (Amazon) و (Yahoo!) ، وغيرها من المواقع الأخرى التي جعلت الوصول لهذه المواقع مستحيلاً، مما سبب الكثير من الخسائر لهذه الشركات. وبعد التحري والتدقيق اكتشف أن من قام بهذه العملية صبي كندي يبلغ من العمر ١٥ عاما، ويطلق على نفسه لقب (MafiaBoy) وكذلك ما حدث من قيام اثنين من المراهقين (الهاكرز الألمان) تنفيذ هجوم ناجح على مقدم خدمات الهاتف المباشر شركة تي – أونلاين T-Online، وهي الخدمة المباشرة التي تديرها شركة الهاتف الوطنية الألمانية، وتمكنا من سرقة معلومات حول مئات أرقام الحسابات البنكية. وكان هذان المراهقان المتسللان البالغان من العمر ١٦ عاماً قد تفاخرا بأعمالهما الجريئة ومآثرهما لمجلة تقنية الحاسب الألمانية، واصفين الأنظمة الأمنية للاتصالات الألمانية بالردئية والبدائية. والأمثلة على ذلك كثيرة جدًا.

وعندما يكون المجرم منطلقاً من هذا الدافع، فإنه من النادر أن يتراجع حتى تتم جريمته، فهو مصمم بشكل كامل على تنفيذ ما يريده. وعلى الرغم من أن هذا الدافع قد يبدو تافهاً لبعض المتابعين إلا أن الخسائر الناتجة عنه قد تكون وخيمة ومؤثرة على الضحية.

## ٤-٤ السياسة وحروب المعلومات

وهذه النوعية من الهجمات قد انتشرت بشكل كبير مؤخراً ولاسيما بعد أحداث ١١ سبتمبر. والمنفذين لهذه النوعية من الجرائم والهجمات يعملون في الغالب على شكل فرق من المجرمين يساعدون بعضهم بعضاً لتنفيذ ما يتغونه، ويشجعهم ويحفزهم فريق آخر من المستخدمين العاديين الذين يبثون مشاركاتهم في المنتديات التي تنتمي لهذه الفئة وتنطلق مشاركاتهم كأهازيج الفرح عند نجاح فريق المخترقين، باختراق أو إيقاع موقع أو خدمة من



obeikandl.com

الطرف الآخر. ولعل من أشهر الأمثلة على ذلك، الهجمات المتبادلة بين المخترقين في الولايات المتحدة وروسيا، وكذلك بين الولايات المتحدة والصين (خاصة بعد قضية طائرة التجسس الشهيرة)، وكذلك بين العرب وإسرائيل، وأيضاً بين الهند وباكستان. وقد بينت أحد الإحصائيات أن مجموعة USG(Unix Security Guards) ومجموعة WFD(World's Fantabulous Defacers) ، قد قامتا بشن (١١١) هجمة على مواقع تعليمية وتجارية في الهند. وقامت مجموعة USG وهي مضادة لإسرائيل بشن ما يقارب من (٨٧) هجمة على مواقع إسرائيلية خلال فترة شهرين فقط.

وفي أثناء حرب غزة الأخيرة كما ذكرت صحيفة (القدس) الفلسطينية أن العديد من صفحات الإنترنت تعرضت في نهاية شهر ديسمبر ٢٠٠٨م، إلى هجمات انتقامية من مجموعات، يعتقد أنها تعمل في لبنان والمغرب وإيران وتركيا. واستهدفت هذه المجموعات مواقع الشركات الإسرائيلية الصغيرة، ومواقع حكومية، وغيرها من المواقع الأخرى.

وكانت الهجمات متركزة بشكل أساسي على بعض مواقع الإنترنت المستضافة على النطاق الخاص بالكيان الصهيوني، وترك المهاجمون عبارات تندد بالكيان الصهيوني والولايات المتحدة الأمريكية كما خلف بعضهم صوراً تظهر وحشية العدو، والنتائج التي يخلفها القصف الإسرائيلي في الأرواح والممتلكات.

ويقول أحد (الهاكرز) المشاركين بالعمليات والمسمى بـ (T@ke Sn!per) إن مجموعته استهدفت مواقع حكومية واخترقت أكثر من ٣٠ جهازاً خادماً، كان من أبرزها حزبان من اليمين ومن اليسار، وبعض البنوك، ومواقع حكومية إسرائيلية. ويقدر عدد المواقع التي تعرضت لهجمات انتقامية حوالي ١٠ آلاف صفحة، وذلك بالتنسيق في أعضاء (الهاكرز) في المنتديات الخاصة.



obeikandl.com

Mirror saved on: 2009-01-08 04:05:07

Defacer: Agd_Storo | Domain: [redacted] | IP address: 155.207.155.243

System: Win 2003 | Web server: IIS/6.0 | Attacker stats

Nato Parliamentary Assembly Hacked by Agd_Storo | Peace Crew & Turuist-Crew

Members: JeXToXiC , rx5 , who , Kacak , 4R!F , Redrolix

Greetz : Kerem125 , Cr@zy_King , AmeN , Jum , TiKiAndre

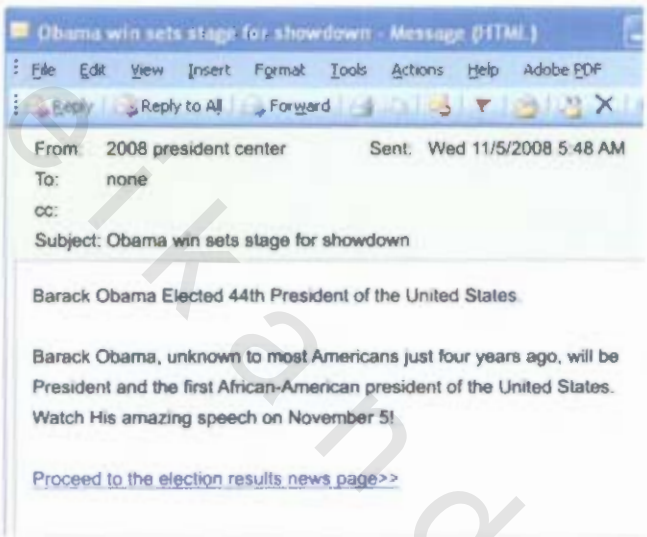
Free Palestine !

شكل ٤-١ : يوضح موقع الناتو بعد اختراقه ووضع صورة تندد بالعدوان الإسرائيلي على غزة



obeikandl.com

ومن الأمثلة الحديثة لبعض جرائم التصيد وعلاقتها بالسياسة، ما حدث في أثناء انتخابات الرئيس الأمريكي باراك أوباما، حينما تم إرسال رسائل تدعو لأوباما، وبها وصلة لموقع يدعي المرسل أنه موقع الحكومة الأمريكية، وأن به فيديو مهم لأوباما (انظر الشكل ٤-٢).




شكل ٤-٢ : رسالة البريد الإلكتروني المحتوية على الوصلة الخبيثة

وفي الحقيقة كانت الوصلة لموقع مزيف وملف الفيديو المزعوم لم يكن غير برنامج فيروس خطير، انتشر بسرعة كبيرة في الولايات المتحدة، وكان الهدف منه سرقة معلومات الضحية وإرسالها إلى خادم يقع في كييف بأوكرانيا ! والصور الآتية توضح ذلك المثال.



obeikandi.com


شكل ٤-٣ : الموقع المزيف


شكل ٤-٤ : الموقع الحقيقي.

وفي أحدث مثال على تداخل السياسة بالعالم الافتراضي، نجد أن الربيع العربي قد انتقلت بعض ساحاته إلى ميادين الإنترنت، فانتشرت الحروب الإلكترونية بين طائفة من الموالين للحكم القائم والثائرين عليه، وإن يكن الأمر في مصر وتونس لم يتعد فترة زمنية قصيرة جرت خلالها مناوشات كثيرة وهجوم على مواقع متفرقة للطرفين، غير أن الأمر في ثورة سورية اتخذ شكلاً أكثر احتداماً، وأكثر هذه الحروب تنشط على صفحات موقع التواصل الاجتماعي (فيسبوك)، حيث يخوض المعارضون حربهم بواسطة لقطات الفيديو التي تناقلتها وسائل الإعلام المختلفة، ثم تشكلت جيوش إلكترونية وكتائب قرصنة قامت بعمليات اختراق لكلا الطرفين، ومن اللافت في الأمر هو تدخل مجموعة أنونيموس (المجهول) وهي مجموعة ذاع صيتها خلال السنوات الماضية لصالح المعارضين وقامت باقتحام موقع وزارة الدفاع السورية ووضعت عليه صوراً وبيان تأييد للمطالبين بالحرية، انظر الشكل ٤-٥.

شكل ٤-٥ بيان مجموعة أنونيموس على موقع وزارة الدفاع السورية

وأما آخر هجوم فقد تم في مطلع فبراير ٢٠١٢، أعلنت جماعة القراصنة الشهيرة أنونيموس (Anonymous) عن تمكنها من اختراق البريد الإلكتروني الخاص بالرئيس السوري بشار الأسد، وذلك بعد نجاحهم في التسلل إلى مخدم البريد الخاص بوزارة شؤون رئاسة الجمهورية والوصول إلى ٧٨ صندوق بريد لموظفي ومعاوني الأسد، ومنهم وزير شؤون رئاسة الجمهورية، والمستشارة الإعلامية للرئيس.

وذكرت الصفحة الخاصة بهذه الجماعة (Anonymous) التي تقوم بالدفاع عن حقوق الإنسان والدفاع عن الحريات في العالم أن هذا الاختراق كان نتيجة للمجازر الدامية التي يقوم بها الرئيس السوري بشار الأسد في حق شعبه الأعزل .

## ٤-٥ المنافسة التجارية

قد تدفع المنافسة التجارية غير الشريفة ببعض الشركات الصغيرة أو الكبيرة إلى اللجوء إلى أعمال انتقامية بشن هجمات إلكترونية للإضرار بمصالح شركة أخرى، أو النيل من سمعتها لصرف أنظار المستهلكين عن منتجاتها، أو التقليل من أعدادهم. ومن ثم الاستئثار بأكبر قدر ممكن من الزبائن. وكثيراً ما يتم هذا الفعل بعيداً عن محيط الشركة المهاجمة، إذ تطلب هذه الشركة من أحد المحترفين في مهاجمة أنظمة المعلومات اختراق أو تعطيل الموقع الإلكتروني لشركة منافسة؛ حتى تكون بعيدة عن الشبهات، وتنجو من الملاحقة القضائية، بل يتعدى الأمر أحياناً إلى محاولة التلصيص على الوثائق والبريد الإلكتروني لدى الشركات المنافسة، للكشف عن الخطط المستقبلية والتسعيرات في العطارات التجارية، أو سرقة قوائم العملاء وبياناتهم التفصيلية.



obeikandl.com

obeikandl.com

# الفصل الخامس:
# أنواع المجرمين وخصائصهم

obeikandl.com

**يوجد الكثير من المجرمين في الإنترنت، ومن الخطأ الكبير التعامل معهم بنفس الطريقة، فهم ينتمون لأنواع مختلفة. وفي هذا الفصل يتم توصيف الأنواع المختلفة لهم، وتصنيفهم إلى أقسام مختلفة اعتماداً على الطرق الآتية:**

- أنواع المجرمين حسب النوايا
- أنواع المجرمين على حسب الدوافع
- أنواع المجرمين على حسب الخبرات

وبعد ذلك يتم ذكر بعض الخصائص المشتركة للمجرمين في الإنترنت بغض النظر عن أي صنف ينتمون إليه.

ومما ينبغي التنويه إليه أن الجريمة الإلكترونية متعددة الغايات والأهداف، ولذا تعددت أوصاف الفاعلين، فتجد أن مصطلحات: (الهاكر، والمخترق، والمتسلل، والمجرم، والمحتال، والمتطفل) هي مصطلحات مختلفة في اللفظ والمعنى ولكنها في الغالب تستخدم لتعبر عن معنى واحد.



obeikandl.com

# ٥-١ أنواع المجرمين على حسب النوايا

يختلف المجرمون في الإنترنت على حسب نواياهم، فبعضهم له نوايا سيئة والآخر له نوايا حسنة. ومن هذا المنطلق يمكن تصنيف المجرمين إلى قسمين:

## ٥-١-١ أصحاب القبعات البيضاء

يندرج تحت هذا القسم من يقوم بعملية الاختراق إيمانا بمبدأ (المعرفة هي القوة)، وهذه النوعية في الغالب لا تقوم بالتخريب أو تدمير المعلومات، وإنما تقوم بالاختراق للتعلم واكتساب الخبرة ومشاركة المعلومات، وبعضها الآخر يقوم بمحاولة الاختراق من أجل اكتشاف الثغرات، ومن ثم تبليغ المسؤولين عنها لكي يتمكنوا من سدها. ومن أكبر معتقداتهم أن ما يقومون به لا يمكن تصنيفه كجريمة، فهم لم يقوموا بسرقة أو تدمير أي معلومات، أو العبث بصفحات ومواقع الآخرين. ويقوم بعض المتابعين بمساندة هذه النوعية ويدعمون عدم تصنيفهم كمجرمين، بل إنهم أيضاً يقومون بتصنيف خبراء الحماية في الشبكات تحت هذه الصنف، مما يخلق نوعاً من اللبس. ولقد عُدَّت هذه النوعية من الأشخاص مجرمين لأن اختراق شبكة شركة والدخول إليها بغير إذن، يعد جريمة حتى لو كان هذا الفعل لم يحدث ضرراً في الشبكة. ومثال ذلك هو الدخول إلى منزل غريب، حيث إن هذا يعد جريمة حتى لو لم تتم سرقة أي شيء من المنزل.

## ٥-١-٢ أصحاب القبعات السوداء

كما أن اللون الأبيض المرتبط بالمجموعة الأولى يعكس عدم وجود نوايا سيئة، بحساب أن اللون الأبيض يرمز للطهر وصفاء النية، فإن اللون الأسود المرتبط بهذه المجموعة يعكس سوء النية والرغبة في التخريب والتدمير. وهذا هو ما يميز هذه المجموعة. فهدفهم الرئيس هو التخريب وإظهار وجودهم بأي شكل من الأشكال. فما أن يتم اختراق الصفحة، حتى يقوم بتغيير محتوياتها بمحتويات سيئة أو مخلة بالآداب. وكذلك هو الحال عندما يجدون بيانات، فهم يقومون بإتلافها مسببين الضرر الكبير لأصحاب تلك المواقع أو الشبكات. ولعل الغالبية من المجرمين في الإنترنت من هذه النوعية.

## ٥-١-٣ أصحاب القبعات الرمادية

وهم الذين تحتوي حياتهم العملية على مراحل مختلفة يتنقلون فيها بين القسمين الأول والثاني، فهم في الغالب ألطف من ذوي القبعات السوداء، وأقسى من ذوي القبعات البيضاء.

## ٥-٢ أنواع المجرمين على حسب الدوافع

تم الحديث في الفصل الرابع عن الدوافع وراء القيام بالجريمة في الإنترنت. ومن هذا المنطلق يمكن تقسيم المجرمين إلى الأقسام الآتية:

### ٥-٢-١ المرتزقة

وهم من يقومون بالاختراق لا لشيء إلا للحصول على المال؛ دون وجود أي حوافز أو دوافع أخرى. وهذه الفئة قد تقوم بمهاجمة مواقع تجارية لسرقة الأموال لصالحها الشخصي. أو قد تقوم باستلام مبلغ مادي مقابل تنفيذ عملية إلكترونية ضد شبكات معلومات، أو مواقع، أو بريد إلكتروني، أو أجهزة حاسب شخصية مرتبطة بالشبكة.

### ٥-٢-٢ المنتقمون

وهم من يكون الدافع الرئيس لارتكابهم للجريمة هو الانتقام، سواء لغرض شخصي، أو لمبدأ، أو لمجموعة أو لأي شيء آخر. وينتمي لهذه الفئة من يتم فصله من وظيفته، فيحاول الانتقام لنفسه. ويطلق على الجرائم من هذا النوع (الاختراق الانتقامي) . وأحد أول الأسئلة التي يطرحها المحققون في جريمة اختراق هي معرفة ما إذا كان هناك من يرغب في الانتقام من الشركة أو الجهة المخترَقة.

### ٥-٢-٣ المتحدّون

وهذا القسم من المجرمين هم من يقومون بالاختراق للتسلية والتحدي. ويجب عدم الاستهانة بهذه الفئة أو التقليل من حجمها، فهناك عدد لا بأس به من المجرمين ممن ينتمون لهذه الفئة. ونسبة كبيرة منهم يريدون تعلم الاختراق، ويقومون بذلك باختيار أهداف عشوائية، ومن



obeikandl.com

ثم محاولة اختراقها بدافع التحدي فقط، ولغرض التعلم.

### ٥-٢-٤ الجواسيس

وهم من يقومون بارتكاب الجرائم المختلفة للحصول على معلومات، بغرض التجسس أو المشاركة في حرب المعلومات. ومن ينتمون لهذه الفئة يتلقون تدريبا رسمياً، أو شبه رسمي من الجهات المتبنية لهم التي تكون منظمة وذات توجه سياسي أو تجاري محدد. ويسعى هذا النوع من المجرمين عند سرقة المعلومات على عدم ترك أي دلائل على عملية الدخول ومصدرها.

## ٥-٣ أنواع المجرمين على حسب الخبرات

يختلف المجرمون في الإنترنت على حسب خبراتهم في مجال شبكات الحاسب الآلي، التي تعد الأداة الأقوى للقيام بالجريمة في الإنترنت. ويمكن تقسيم المجرمين على حسب خبراتهم للأقسام الآتية:

### ٥-٣-١ الخبراء

ويمتلك من ينتمي لهذه المجموعة خبرة كبيرة جداً في مجال الحاسب الآلي بشكل عام والشبكات والاتصالات بشكل خاص. ويطلق أحياناً على هذه المجموعة اسم (صانعو الأدوات) حيث إن خبرتهم العالية ومعرفتهم بعلم أنظمة الشبكات وبرتوكولاتها، تسمح لهم



obeikandl.com

بكتابة البرامج المختلفة، وتكوين الأدوات المختلفة التي يتم استخدامها من الأقسام المتبقية من المجرمين. وقلّة من المجرمين في الإنترنت من ينتمي لهذه المجموعة.

### ٥-٣-٢ مستخدمو الأدوات

وهذا القسم من المجرمين يمتلك خبرة ومعرفة متوسطتين في مجال الحاسب الآلي والشبكات. وهذه الخبرة تمكنهم من استخدام الأدوات التي كوّنها القسم الأول، ولكنهم في نفس الوقت على معرفة بالمبادئ والأسس التي تقوم عليها هذه الأدوات. وتعد هذه المجموعة في المنتصف بين المجموعة السابقة ومجموعة لاحقة لا تملك أي خبرة في مجال الحاسب الآلي ولا تملك معرفة بالأدوات المستخدمة ومدى تأثيرها.

ويندرج تحت هذا قسم مستخدمي الأدوات أيضاً من المجرمين من يمتلكون أقل قدر من المعرفة في الحاسب الآلي، وتمكنهم من القيام بالجريمة يعود بشكل رئيس ويطلق عليهم فتيان البرمجيات، لتوفر الأدوات المختلفة التي قام القسم الأول بكتابتها. وهذا النوع يقوم باستخدام هذه البرامج والأدوات بشكل أعمى، دون أي معرفة بالمبدأ التي تقوم عليه هذه الأدوات أو بكيفية التعامل معها بشكل محترف ويسمى هؤلاء عند بعض المختصين بفتيان البرمجيات.

## ٥-٤ خصائص المجرمين

بغض النظر عن أي قسم ينتمي له المجرمين في الإنترنت، فإنهم يتشاركون في خصائص معينة. ولقد تخصص بعض الباحثين في مجال علم النفس في دراسة المجرمين في مجال الحاسب الآلي، وإيجاد الخصائص التي يتشاركون فيها. ومن هؤلاء الباحثين دون باركر، الذي قام بإجراء الدراسات على مدى ٢٠ سنة، وكانت نتائج دراسته أن المجرمين في الحاسب الآلي يتشاركون



obeikandi.com

في الخصائص الآتية:

- لديهم دوافع قوية، ومهارات عالية ومعرفة كبيرة في مجالات مختلفة.
- معظمهم يعتقدون أن الدخول على جهاز دون سرقة معلوماته أو تخريبه لا يعد جريمة.
- أغلبهم من الذكور بين ١٢ و ٢٤ سنة.
- معظم آباء المخترقين ليس لديهم أدنى فكرة عن قيام أبنائهم بالاختراق.
- معظمهم لا يلومون أنفسهم على الاختراق، بل يلومون أصحاب الأجهزة والشبكات على الأمن الضعيف لديهم.
- لا يتميزون بمستوى ذكاء أعلى من الأشخاص العاديين ولكنهم يمتلكون الكثير من الوقت.

وتعمد الشركات إلى الاستفادة منهم بتوظيفهم في أقسام أمن المعلومات، فمنهم من ينجح ويتطور، فينخرط في العمل المهني، ومنهم من لا يحقق أي نجاح لأنه يريد أن يستمر في العمل الحر غير المنضبط بأنظمة وسياسات.

obeikandl.com

# الفصل السادس:
# رواد قراصنة الإنترنت ومشاهيرها

obeikandl.com

كان لقب (هاكر) يطلق -سابقاً- على المبرمج الموهوب، ومن ثم أصبح كل من يقوم باستخدام نظم التشغيل والبرامج في الدخول على الأجهزة والشبكات بشكل غير مباشر أو غير مصرح، يحمل صفة هاكر (مخترق). وقد انطبعت الصورة الذهنية السيئة عن الهاكرز لدى الجميع، نتيجة أفعالهم واختراقاتهم، وبغية تعديل هذا المفهوم وتحسين الصورة الذهنية للهاكرز وإيضاح أن ليس جميعهم من الأشرار، بل هم أشخاص لديهم قدرات عقلية وتقنية عالية؛ اجتمع في نيويورك قراصنة الحاسب الآلي (الهاكرز) في قمة استمرت لمدة ثلاثة أيام. وشارك في هذا الاجتماع عدد من كبار الشخصيات في عدد من الشركات العالمية، مثل ستيف وزنياك أحد مؤسسي شركة (آبل) وكيفن ميتنيك الهاكر الذائع الصيت. ويعد هذا التجمع هو الخامس من نوعه منذ عام ١٩٩٤. ويقدم هذا الفصل تعريفاً بأشهر الهاكرز عبر الحقبة التقنية وروادها، ومنهم:



obeikandl.com

# ٦-١ جون درابر

يُرجع الكثير من المختصين عمليات الاختراق والاستخدام غير الشرعي للحواسيب إلى ما ظهر في سبعينات القرن المنصرم، وسمي بالفريكينج (Phreaking) كخطوة مهمة إلى ما نراه اليوم من جرائم على شبكة الإنترنت، بصورها المتنوعة من الاختلاس إلى التزوير والتحريض على الفسق والفجور، وإغواء الأحداث، بالإضافة إلى الجرائم التي تقع على الحاسب الآلي ذاته وبرامجه كما سنرى لاحقاً عبر الصفحات الآتية .

شكل ٦ - ١: جون درابر

يرجع ظهور الفريكينج إلى جون درابر الذي ولد عام ١٩٤٤، واستخدم طريقة بسيطة وذكية في الوقت نفسه في اختراق شبكة الهاتف، فقد كان يتصل برقم تليفون معين، وبينما يرن جرس الهاتف على الناحية الأخرى، يستخدم درابر صافرة عادية جداً كانت تسمى (كابتن كرانش)، وهي مخصصة للأطفال! لإصدار صوت على تردد ٢٦٠٠ هرتز. وكان هذا التردد هو المستخدم لتعريف حالة الخط، وبإطلاق هذا الصوت من الصافرة، يقنع درابر شبكة الهاتف أنه قد أغلق الخط، وكانت هذه العملية تنجح دائما بالرغم من أن الشبكة لم تتلق علامة حقيقية بأن الخط قد أغلق.

شكل ٦ - ٢: كابتن كرانش

وقد ألقي القبض عليه فيما بعد وظلت محاكمته حوالي أربع سنوات كاملة، لحداثة هذا النوع من الجرائم، فلم يكن هناك نص قانوني حينذاك، يجرم مثل تلك الأنواع من الجرائم، وفي النهاية صدر الحكم بحبسه لمدة شهرين!!!

وقد كانت فكرة درابر غير المشروعة هي السبب في ظهور مجموعات من الهاكرز، والفريكرز، وحركات جديدة هدفها في البداية هو التهرب من دفع الفواتير، والآن اقتحام مواقع الإنترنت وشبكات الحاسب وتخريبها، ومن أوائل تلك الحركات مجموعة سميت (مجموعة ٢٦٠٠)، كان هدفها إيجاد طرق جديدة للتهرب، أو التوقف عن دفع فواتير الهاتف.

ثم تطورت الفكرة فيما بعد على يد صديق درابر ( ستيف وزنياك ) الذي أكمل اكتشاف درابر وحسنه، ثم اسماه ( الصندوق الأزرق) الذي كان جهازًا يقوم بإخراج نغمات بترددات مختلفة ومطلوبة من أجل خداع شبكات الهاتف.

وقد كان الصندوق الأزرق أكثر احترافية وتعقيدًا من صافرة الأطفال التي استخدمها جون درابر. إذ كان قادراً على تقليد كل الأصوات على كل الترددات التي استخدمتها شبكات الهاتف، مما أدى إلى بيع الكثير من هذه الصناديق الزرقاء في السبعينات من القرن الماضي. ومن أشهر قصص الصندوق الأزرق هي المكالمات التي أجراها (وزنياك) للفاتيكان منتحلا فيها شخصية وزير الخارجية الأمريكي السابق هنري كسينجر. وجدير بالذكر أن الصندوق الأزرق سمي بهذا الاسم لأن أول جهاز تم مصادرته كان في إطار بلاستيكي أزرق.

شكل ٦ - ٣ : الصندوق الأزرق
معروض في متحف تاريخ الكمبيوتر

obeikandl.com

## ٦-٢ المخترق الأعظم كيفن ميتنك (Kevin Mitnick)

شكل ٦ - ٤ : كيفن ميتنك

لعل أبلغ تعبير يوجز صفات هذا الرجل، ما وصفته به فاطمة نعناع في مجلة إنترنت العالم العربي، حيث تقول: «الهاكر الأكبر،نسر ينقض على شبكات الكمبيوتر». إن كيفن يملك أصابع سحرية ما إن يضعها على لوحة مفاتيح الحاسب، حتى تنزاح أمامه أسوار الدفاعات المنيعة لمؤسسات وشركات ومنظمات، فيجد طريقه بسهولة ويسر إلى خزائن أسرارها، ونفائس مكنوناتها. فهو قد نجح ولمدة ثمانية عشر عاماً في اختراق شبكات العشرات من المؤسسات والشركات، بدءاً من شركة الهاتف المحلية للمدينة التي نشأ فيها، وانتهاء بوزارة الدفاع الأمريكية (البنتاجون). وبذلك أصبح أسطورة اختراق شبكات الحاسب الآلي في التاريخ الحديث.

حلّق كيفن مبكراً في هذا المجال على الرغم من أنه لم يكن من المتفوقين في الدراسة أو النابغين فيها، بل كان متوسط المستوى لا يلفت الانتباه، بدوافع تعويضية نجمت عن تفكك الأسرة وانفصال الوالدين، وعدم الاستقرار المعزز بسوء الوضع المالي ورقة الحال. ففي سن السابعة عشرة من العمر، انطلق كالبرق الصاعق (Three Days of the Condor) ملقبًا نفسه بالنسر تيمناً بفيلم أيام الكوندور الثلاثة، الذي تدور قصته حول باحث مطارد من قبل وكالة الاستخبارات الأمريكية، فيستخدم خبرته كضابط سابق في سلاح الإشارة في البحرية الأمريكية، للتحكم بشبكة الهاتف، وتضليل مطارديه.

وعندما شاع في أوائل الثمانينيات استخدام الحاسب الشخصي مع مودم للتحكم عن بُعْد بمقاسم شركات الهاتف، برع كيفن في الدخول إلى بدالات الهاتف المحلية، وتمكن من إجراء مكالمات هاتفية مجانية، وربما على حساب آخرين قد لا يعلمون بذلك أبداً. وتطور ذلك إلى الاقتحام والتنصت على محادثات الآخرين، فتكون لديه مخزون من الأسرار عن أشخاص من الأغنياء وذوي السلطة والنفوذ، فأشبع ذلك غروره، ومنحه إحساساً بالقوة والتفوق يعوضانه عما يحس به من الدونية والصَّغَار. وتعرَّف بعد ذلك على مجموعة من الشباب من ذوي الخبرة والمهارة في اختراق شبكات الهاتف باستخدام الحاسب، وشكلوا جماعة تستغل الهاتف، فيجرون محادثات مجانية على حساب الآخرين، أو على حساب شركات الهاتف. وكانوا يدخلون إلى شبكات الهاتف، ويهزؤون بالناس، وكل ذلك بحثاً عن المتعة والإثارة، ودفعاً للملل كما يقولون. وأصبحوا مصدر إزعاج ومضايقة سرعان ما تحول إلى أذى بارتكاب سلسلة من الجرائم. فقد قام أحد أعضاء المجموعة بإتلاف وتخريب ملفات إحدى شركات الهاتف في سان فرانسيسكو، ولم تتمكن الشرطة طوال عام كامل من معرفة الفاعل.

وفي يوم من عام ١٩٨١ تسلل كيفن واثنان من أصدقائه إلى المركز الرئيس لشركة الهاتف في مدينة لوس أنجلوس، ووصلوا إلى الغرفة التي تحتوي على الحاسب الذي يدير العمليات، وسرقوا كتب التشغيل، وقوائم سجلات شيفرة فتح الأبواب في تسعة مراكز أساسية تابعة لشركة الهاتف في تلك المدينة. ومرة أخرى لم تتمكن الشرطة من معرفة الفاعل. وبعد عام من ذلك التاريخ سارعت الشرطة إلى اعتقال كيفن ورفيقيه، بعد أن وشت بهم فتاة من أعضاء المجموعة. وحكم على كيفن بالسجن لمدة ثلاثة أشهر يقضيها في إصلاحية الأحداث بتهمة السرقة وإتلاف بيانات عبر شبكة حاسب آلي مع وضعه سنة تحت المراقبة في لوس أنجلوس. ولم يصلح حاله رغم محاولات مركز الخدمة الاجتماعية مساعدته على تطوير خبرته والاستفادة منها في عمل قانوني، بل أدت إلى نتيجة سلبية، لأنه سعى إلى تعلم أمور محددة وحِيَلٍ ماكرة تعينه على ممارسة هوايته غير البريئة بصورة أفضل. فكان نتيجة ذلك مزيداً من الأخطاء والجرائم المتتالية.

ومرة أخرى في عام ١٩٨٣ ضبط كيفن يحاول استخدام حاسب جامعة شمال كاليفورنيا لاختراق شبكة، ليصل من خلالها إلى وزارة الدفاع الأمريكية (البنتاجون)، وحكم عليه بقضاء ستة شهور تدريب في سجن للأحداث في كاليفورنيا. وبعد سنة اعتقل مرة أخرى متهماً بالعبث بالحاسب الخاص بحسابات إحدى الشركات، والشيء غير العادي هنا هو أنه بقي رهن الاعتقال دون محاكمة لمدة عام كامل، والغريب في الأمر أن ملفه اختفى من مركز الشرطة دون أن يعلم عنه أحد شيئاً.

وفي عام ١٩٨٧ أدين كيفن بسرقة برامج من إحدى شركات البرمجيات في كاليفورنيا، عن طريق الشبكة بعد أن اكتشفت الشرطة ذلك، من خلال تتبع خط الهاتف الذي تمت من خلاله العملية، وقادهم هذا إلى مسكن كيفن. وتعرض كيفن في هذه الحادثة للإهانة والضرب من قبل الشرطة، ووضع تحت المراقبة لمدة ثلاث سنوات زادته إصراراً وعزيمة على مواصلة ممارسة هوايته المؤذية له وللآخرين. وفي عام ١٩٨٨ تملكته (VMS Microcomputer) فكرة الحصول على نسخة من نظام تشغيل الحاسب الرقمي الصغير الخاص بشركة ديجيتال. فعكف لساعات طوال مع صديقه دييجو الذي يعمل في قسم دعم البرامج لإحدى شركات الحاسب في مقر عمله الذي كان يذهب إليه كل مساء، يحاولان الدخول إلى مختبرات شركة ديجيتال. وعند إحساس المسؤولين بالشركة بهذه المحاولات، وفشلهم في تتبع مصدرها أو تحديده ، طلبوا العون من الشرطة المحلية ومكتب التحقيقات الفدرالي (FBI) الذين عملوا بالتعاون مع خبراء شركة ديجيتال، ولم يتمكنوا لأيام عديدة من التوصل إلى نتيجة، لأن كيفن الماكر كان قد اتخذ احتياطات ذكية تحول دون اكتشافه، وذلك باستخدامه جهازي حاسب (VMS) يحاول من خلال الأول اختراق شبكة شركة ديجيتال، والحصول على نظام تشغيل ومن خلال الثاني مراقبة مركز مؤسسة الهاتف، وتتبع محاولات اكتشافه. وإمعاناً في التضليل قام باختراق شبكة الهاتف والعبث بمقاسمها الهاتفية. ونتيجة لذلك بذلت شركة ديجيتال الكثير من الجهد والوقت في مراقبة أجهزة الشركة وتطبيق إجراءات جديدة للحماية، فكلفها ذلك مبالغ

طائلة.

وأخيراً، تمكن رجال مكتب التحقيقات الفدرالي بفضل وشاية من ديجو صديق كيفن ورفيقه في المحاولات، وليس بفضل جهودهم، من القبض على كيفن الذي أثار حنق ديجو، وأغضبه بمزاحه الثقيل، حيث اتصل بمدير ديجو في العمل، وأخبره بأن ديجو يعاني من مشاكل كبيرة مع مصلحة الضرائب. وأحيل كيفن للمحكمة بتهمة سرقة برامج قيمتها ملايين الدولارات، والتسبب في خسائر لشركة ديجيتال تزيد عن ٢٠٠ ألف دولار، صرفتها لمنعه من الوصول إلى أجهزتها. وقد وُجد كيفن مذنباً في استخدامه الحاسب سنوات طويلة، للاحتيال وحصوله على كلمات العبور، للعديد من حاسبات الشركات بشكل مخالف للقانون. وهي المرة الخامسة التي يدان فيها كيفن في مثل هذه الجرائم، وحُكم عليه بالسجن لمدة سنة واحدة وستة شهور معالجة من إدمان اختراق الشبكات. وهو حكم أثار اهتمام الرأي العام لغرابته.

أمضى كيفن عقوبة السجن، لكنه لم يلتزم بالحكم الآخر، وهو الخضوع للمعالجة من إدمان اختراق الشبكات، وانتقل إلى لاس فيجاس وعمل مبرمجاً بسيطاً في إحدى الشركات المتخصصة في القوائم البريدية الإلكترونية.

ولكن كيفن لم يحتمل البعد عن سان فرانسيسكو، عاد إليها مرة أخرى بعد وفاة شقيقه وعمل مع والده في أعمال البناء، ثم انتقل للعمل مع صديق والده في وكالة تحقيق. وبعد مدة قليلة اكتُشِفتْ عمليةُ استخدام غير شرعية لقواعد البيانات التي تملك الوكالة حق الوصول إليها. ووجّه الاتهام إلى كيفن الذي قام مكتب التحقيقات الفدرالي بتفتيش منزله للبحث عن أدلة تدينه. وفي عام ١٩٩٢ أصدر القاضي أمراً باعتقاله بتهمتي الدخول غير الشرعي إلى حاسب إحدى شركات الهاتف، وعدم الالتزام بالبقاء في المدينة ومغادرتها قبل انتهاء فترة الستة شهور التي فرضتها المحكمة لعلاجه من الإدمان. ولم يتم اعتقاله لأنه اختفى فجأة دون أن يترك أثراً.

وفي عام ١٩٩٢ استطاع كيفن الهرب من الشرطة بعد أن شكَّتْ في طلب كان قد تلقاه قسم

الآليات بكاليفورنيا في اتصال عبر الحاسب، للحصول على نسخ من شهادات رخص السواقة للمتعاونين مع الشرطة، محاولاً إيهام المسؤولين بأنه مخول قانونياً بالاطلاع على الوثائق، وتم إرسال عناصر من الأمن إلى المحل المطلوب إرسال النسخ إليه، لمعرفة الشخص الذي طلب مثل هذه المعلومات المثيرة للريبة والشكوك وهدفه من طلبها.

وأفلت منهم كيفن، ولكن الأوراق سقطت منه في أثناء هربه. وجعلت هذه الحادثة والنجاح في الهرب من كيفن لصاً ذكياً، مثل أرسين لوبين تماماً، ومثيراً لإعجاب الكثيرين، لدرجة أن صحفياً يدعى ماركوف تخصص في تتبع أخبار كيفن، صغيرها وكبيرها، بالقدر الذي دفع مكتب التحقيقات الفدرالي إلى تعيينه مستشاراً لها في عمليات مطاردة كيفن.

وفي حادثة كانت قاصمة الظهر، وقع النسر الكاسر في شر أعماله. ففي إجازة أعياد الميلاد لعام ١٩٩٤، تمكن كيفن من سرقة مئات الملفات والبرامج من الحاسب المنزلي المتصل بشبكة العمل الواسعة لشيمومورا، أحد خبراء أمن الشبكات والبرمجة الذي يعمل مستشاراً، لمكتب التحقيقات الفدرالي، والقوى الجوية، ووكالة الأمن القومي الأمريكي، ومطور برامج لحماية نظم الحاسب من الاختراق. وكانت الملفات المسروقة مفيدة لكل من يريد تعلم أساليب اختراق شبكات الحاسب والهاتف النقّال.

لقد دخل كيفن إلى عرين الأسد، ولم ينتبه إلى أن شيمومورا قد ركّب نظام مراقبة ينذر عند الاشتباه بوقوع اختراق لشبكة الحاسب التي تتصل بها حواسبه المنزلية. فعندما بدأ الهجوم على حاسب شيمومورا المنزلي أرسل آليا مجموعة من السجلات، تتضمن كل ما دار من أحداث إلى حاسب آخر موجود في مركز الشبكة، مما جعل المشرفين يدركون وقوع اختراق لحاسب شيمومورا المنزلي، وتمكنوا من طرد المعتدي. وبعد دراسة الهجوم اكتشف شيمومورا أن المخترق قد خدع حاسبه، واتضح له أنه مخول بالدخول عليه. ولم يتمكن شيمومورا من تتبع مصدر الاتصال والوصول إلى نتيجة، وبدا له كأن الهجوم قادم من إحدى جامعات شيكاغو.

لقد أشعلت هذه الحادثة نيران غضب شيمومورا وحنقه، ودفعته إلى توجيه طاقاته وخبرته المتميزة للتعاون مع مكتب التحقيقات الفدرالي لإيقاع من تجرأ على دخول العرين.

ونجح شيمومورا بمساعدة المحققين، ومن خلال نظام المراقبة الذي بذل جهداً جباراً في تحسينه، من تتبُّع أثر المعتدي، وهو يبحر طليقاً في سماء الإنترنت، ورصده وهو يعبث دون هوادة بمقاسم شركة الهاتف، ويسرق ملفات من شركات موتورولا وأبل وغيرها، وينسخ عشرين (٢٠) ألف بطاقة ائتمان من إحدى شبكات الحاسب التجارية.

وقع النسر في الشبكة، وحامت الشكوك في كل هذه الجرائم حول كيفن ميتنك الهارب والمختبئ منذ عام ١٩٩٢، وكشفت عن أنه يقوم بعملياته الإجرامية، عبر شبكة هواتف نقّالة من مدينة رالي بشمال كاليفورنيا.

وفي مدينة رالي التي ذهب إليها شيمومورا في ١٣ فبراير ١٩٩٥، قام بمساعدة المحققين الفدراليين وخبراء شركة الهاتف المحلية، باستخدام جهاز مسح لترددات الهاتف النقّال، لتحديد مكان كيفن بمنتهى الدقة. وفي ١٥ فبراير ١٩٩٥، وصلوا إلى شقة في ضواحي مدينة رالي، وتم اعتقال النسر، ووضع في السجن دون محاكمة، حتى صدر عليه حكم بالسجن لمدة ٢٢ شهرا في ٢٧ يونيو عام ١٩٩٧، وكان حينها قد أمضى مدة الحكم وزاد عليها أربعة شهور أخرى، ومع ذلك لم يطلق سراحه على أساس أنه خطر جداً، ويمكن أن يهدد الأمن القومي للبلاد، بفضل قدرته على اقتحام أكثر المواقع خطراً وأهمية عبر شبكات الحاسب والهاتف.

ولقد تمَّ الإفراج عنه في أوائل عام ٢٠٠٠، ومنذ ذلك الحين عمد كيفن ميتنيك إلى تغيير سلوكه، وقام بتأسيس شركة استشارات متخصصة في أمن المعلومات أسماها (Mitnick Security Consulting)، تقدم مجموعة شاملة من الخدمات، لمساعدة الشركات على حماية أصولها.

والطريف في الأمر أن موقع شركة ميتنك (الهاكرز الأعظم) تم اختراقه أكثر من مرة!



obeikandl.com

فهل بات ميتنك هدفًا مثيرًا للمخترقين، أم أراد زملاء مهنة الأمس أن يجرعوه مرارة الكأس التي سقاها للكثيرين؟! أم هو أثبات بأنه لا يوجد موقع في العالم غير معرض للإختراق إذ من الممكن اكتشاف الثغرات واستغلالها، فيما تكمن الصعوبة في تأمين المواقع الالكترونية بشكل كامل.


شكل ٦-٥: موقع شركة متينك وبجوارها صورته معلنا (لست مخترقاً)

## ٦-٣ كيفين بولسون

شكل ٦-٦: كيفين بولسون

هو من أوائل المخترقين الذين أتعبوا المباحث الفدرالية في تتبع خطاهم حتى الإيقاع بهم، وقد ألقي القبض على كيفن للمرة الأولى في ١٩٨٩، عندما كان عمره أربعة وعشرين عاما.

واتهم بالعديد من الاختراقات لشبكات الهاتف والكمبيوتر، غير أنه تمكن من الهرب وظل طريدًا للمباحث الاتحادية لأكثر من ١٧ شهرًا، وفي هذه الفترة قام بولسون بأشهر الاختراقات التي عُرف بها. إذ قامت محطة راديو لوس أنجلوس بإطلاق مسابقة، يحصل فيها المتصل رقم (١٠٢) على سيارة بورش ٩٤٤، فبدأ بولسون باختراق شبكة الهاتف، وفرض سيطرة كاملة على الشبكة الموصلة إلى المسابقة، وحجب كل المكالمات الآتية، لكي يضمن أن

يكون هو المتحدث رقم ١٠٢. ودفع نجاح بولسون المباحث الاتحادية إلى تكثيف البحث، لتشديد الخناق حوله، إلى أن ألقي القبض عليه في أبريل ١٩٩١م، نتيجة وصول خبر قيامه بالتسوق في محل عادي في ضواحي لوس أنجلوس. ووجهت التهم لبولسون في ١٩٩٤، وحكم عليه بالسجن لأربع سنوات، وكان هذا الحكم أكبر عقوبة تصدر على هاكر في هذا الوقت.

## ٦-٤ جستن تانر بيترسون

يقول جون نيتيل ومايكل سوتو: «اشتهر في عام ١٩٩١ شخصٌ يدعى جستن تانر بيترسون، الذي عُرف وقد ألقي القبض عليه فيما بعد بلقب (وكيل السرقة) لسرقته سيارة، إلا أن التحقيقات التي أجريت معه لاحقاً بينت أن هناك أموراً أكثر من سرقة السيارة بكثير، قد ارتكبها هذا (اللص الظريف). فقد تبين أنه يخترق أجهزة الكمبيوتر المعقدة، ويتسلل إلى مختلف الأنظمة، وأدين بناء على هذه الأمور، إلى جانب حيازته مواد بريدية لا تخصه، وأرقام بطاقات ائتمان لأشخاص آخرين. والطريف في الأمر أن ملف هذا المجرم قد أقفل بناء على تدخل كل من مكتب التحقيقات الفيدرالي الأمريكي، ومكتب المحامي العام الأمريكي، نظراً للرغبة في استخدام مهاراته الفذة في الكشف عن المجرمين الآخرين من طرازه. وأفرج عنه من السجن، وبقي تحت إشراف مكتب التحقيقات الاتحادي الأمريكي من شهر سبتمبر ١٩٩١ وحتى أكتوبر ١٩٩٣، حيث ساعدهم في قضيتين لمخترقين كبيرين مشهورين، هما كيفن ميتنك وكيفن بولسن. إلا أنه لما أعيد فتح ملفه الإجرامي توقع الكثير أن يصدر الحكم عليه بالسجن لمدة (٤٠) أربعين عاماً، ودفع غرامة مالية قدرها (١,٥) مليون دولار. لأن بيترسون أقر في اجتماع ضمّه و محاميه مع محامي الدفاع الأمريكي بأنه لا يزال يقوم بالجرائم الإلكترونية. إذ اقتحم خلال فترة بسيطة عدداً من أجهزة الحاسب الخاصة بالحكومة الاتحادية الأمريكية ومكاتب بطاقات الائتمان. وتجاوزًا لغلطة الإقرار بالذنب، طلب بيترسون استراحة قصيرة، وفر

خلالها من المحكمة التي كان يحاكم فيها، وتوارى عن الأنظار، لأكثر من سنة، إلى أن اعتقل على مقربة من مكتب التحقيقات الفدرالي الأمريكي في مدينة لوس أنجلوس في عام ١٩٩٥، واعترف بأنه (مذنب) بتحويل مبلغ (١٥٠,٠٠٠) دولار برقياً في بنك (هيلر فاينانشال)، حيث صدر حكم عليه بالسجن لمدة ثلاث سنوات، وبالمراقبة لمدة ثلاث سنوات أخرى، ودفع غرامة مالية قدرها(٣٨,٠٠٠) دولار.

أُطلق سراح جستين بيترسن عام ١٩٩٧م، فأعلن عقب خروجه، أنه توقف نهائياً عن العمليات غير المشروعة التي كان يقوم بها، وركز على تطوير مهاراته في مجال الويب. فعمل مطورًا لصفحات ويب ضمن (ويندوز نت)، وافتتح موقعاً شخصياً له.

## ٦-٥ جيسون ميوهايني يُعتقل في وكالة الفضاء الأمريكية (ناسا)

ورد في خبر من أونتاريو بكندا بتاريخ ١٥ أبريل ١٩٩٨، أن شاباً كندياً يبلغ من العمر ٢٢ عاماً، يواجه عشرات التهم في قضايا هجوم واختراق لأنظمة حاسب، وسرقة شيفرات أمن حاسبات في مرافق جوية مهمة جداً في الولايات المتحدة الأمريكية.

وذكرت الشرطة الملكية الكندية التي أجرت تحقيقاً لمدة أربعة عشر شهراً، أن أحد المتطفلين الهاكرز، تمكن من الدخول إلى أنظمة حاسب كل من المركز الوطني لإدارة الطيران والفضاء، والجمعية الوطنية لعلوم الجو والمحيطات، وشركة هيوز إحدى أضخم الشركات العاملة في مجال الطيران والفضاء. وقد ذكر أن خسائر إتلاف ملفات في واحدة من هذه القضايا قد بلغ خمسين ألف دولار أمريكي، وأن اختراقاً قد تمَّ لعدة أنظمة حاسب خاصة، أو تابعة لجامعات بكندا، والولايات المتحدة الأمريكية.



obeikandl.com

وقد وجهت لهذا الشاب المدعو جيسون ميوهايني، تهم التسبُّب بالأذى لقيامه عن عمد بإعاقة الاستخدام القانوني للبيانات واعتراضه، والتدخل فيه، وقدم للمحاكمة في ١٣ مايو من عام ١٩٩٨.

## ٦-٦ روبرت تابان موريس

تسبب روبرت موريس في إتلاف أكثر من ٦٠٠٠ جهاز كومبيوتر في نوفمبر ١٩٨٨، وأدت إلى خسارة قدرت بعدة ملايين من الدولارات، وكان ذلك بسبب فيروس قام باختراعه وعرف باسم (دودة موريس)، وانتشر على تلك الأجهزة عن طريق الشبكة فتم إتلاف جميع تلك الأجهزة، ولم يستطع أحد جعلها تعمل كحالتها الأولى. وقد تم القبض عليه، وحاول تبرير فعلته بأنه كان يريد اختبار مدى تحمل الشبكة وأجهزة الكومبيوتر، ولكن ذلك لم يكن سبباً مقنعاً لذا حكم عليه بالسجن لمدة ٣ سنوات تحت المراقبة، و ٤٠٠٠ ساعة في خدمة المجتمع وغرامة مالية كبيرة .

وفى يومنا هذا يعرض في متحف بوسطن للعلوم قرص كومبيوتر يحتوي على الفيروس، وهذا القرص هو نفسه الذي استخدمه روبرت في هجماته .

## ٦-٧ المخترق السعودي ( sNiper_hEx)

ينظر كثيرون بعين الرضا والإعجاب لأحد المخترقين السعوديين، الملقب بـ(sNiper_hEx) واسمه الحقيقي خالد، لأن أعماله –كما يقولون– لم تنصب في الجانب المظلم من



obeikandl.com

الاختراقات، بل تكرّست في الهجوم –حسب رأيه– على الأعداء الصهاينة، ولعل شهرته زادت كثيراً حينما كتبت عنه بعض الصحف الأمريكية والإسرائيلية ونشر اسمه في المجلات والمواقع اليهودية للتحذير منه، ولأخذ الاحتياطات الأمنية اللازمة، إذ استطاع تدمير أكثر من (٤٠٠) موقع إسرائيلي ويهودي في فترة قصيرة. وذكر sNiper_hEx أنه عمل على تطوير برنامج (الدرة) بطريقة جديدة، لاستهداف المستخدمين الإسرائيليين بحيث تتم عمليات الهجوم على مزودات الويب الإسرائيلية بواسطة المستخدمين الإسرائيليين أنفسهم، وحتى لا يتمكنوا من صد الهجمات لاسيما بعد نجاح تجربته الأولى في إصابة أكثر من (٦٩) ألف جهاز في أربعة أيام.

والجدير بالذكر أن sNiper_hEx يأخذ على المخترقين العرب اختراقاتهم للعناوين البريدية والمواقع العربية، واستهداف المستخدمين ولاسيما المبتدئين منهم.

## ٦-٨ الهاكرز المراهقون

لم يكن الاختراق عملا خاصا بالبالغين أو المحترفين، بل غدا هواية للمراهقين الحالمين بتحقيق أمجاد شخصية، وقد برز عدد منهم، وقاموا بعمليات عديدة جلبت لهم كثيرا من الاهتمام.

### ٦-٨-١ ميشال سالس Michael Calce

مخترق مراهق عمره ١٥ سنة اكتسب سمعة سيئة منذ البداية بعد أن قام باختراق بعض المواقع التجارية العالمية، واستخدم اسماً مستعاراً (MafiaBoy) حيث اخترق (٧٥) جهاز كمبيوتر و (٥٢) شبكة، أثرت على شركة أمازون وإيباي وياهوو، وألقي القبض عليه فحكم عليه بالسجن لمدة ٨ أشهر وغرامة مالية صغيرة.



obeikandl.com

## ٦-٨-٢ مراهقان يتسللان إلى شبكة مقدم خدمة ألماني

استطاع اثنان من المراهقين الهاكرز الألمان تنفيذ هجوم ناجح، على مقدم خدمات الهاتف المباشر، وهي الخدمة المباشرة التي تديرها شركة الهاتف الوطنية الألمانية (T-Online)، وتمكنا من سرقة معلومات حول مئات أرقام الحسابات البنكية. وكان هذان المراهقان المتسللان البالغان من العمر ١٦ عاماً قد تفاخرا بأعمالهما الجريئة، ومآثرهما لمجلة تقنية الحاسب الألمانية، واصفين الأنظمة الأمنية للاتصالات الألمانية بالتخلف والبدائية المطلقة.

وقد حدث هذا الهجوم عقب قيام وزارة العدل الألمانية، باعتقال ثلاثة من المراهقين الإسرائيليين، لهم علاقة بسلسلة من الاختراقات، لشبكات حاسب مملوكة للحكومتين الأمريكية والإسرائيلية، بالإضافة إلى شبكات خاصة بشركات ومؤسسات تعليمية في الولايات المتحدة الأمريكية وخارجها.

ويمارس المتطفلون من المراهقين الألمان ألعاباً مجانية على الشبكة عند اختراقهم لأنظمة الحاسب والشبكات، وقد قام عدد منهم مؤخراً بسرقة بيانات مالية مهمة، ادَّعوا أنهم أتلفوها دون أن يستخدموها.

وعلَّق على ذلك أحد المسؤولين الألمان مشيراً إلى أن عمليات الاختراق والهجوم على الشبكات، أصبحت مشكلة دولية مع ازدياد حجم المعلومات التي توضع على الشبكة الدولية، وشبكات الحاسب الأخرى، وأن الاشتباه بقيام المراهقين بهذه الهجمات يزيد المخاوف من خطورة الأمر كثيراً، لأن في ذلك قابلية لوقوع معلومات حساسة في أيدي مراهقين باحثين عن الإثارة.

## ٦-٨-٣ مخترق مراهق يمنع من استخدام الحاسب

وجهت ولاية ماسيتشوتس تهماً بارتكاب جرائم اتحادية ضد مراهق، لقيامه بالهجوم



obeikandl.com

على حاسبات شركة اتصالات هاتفية بالولاية، تمكن خلاله من تعطيل برج المراقبة لإدارة طيران اتحادية، وقطع خدمات الهاتف الخاصة بالولاية، وهي أول قضية توجه فيها تهم اتحادية ضد حَدَثٍ لقيامه بجريمة حاسب آلي. وبناء على التماس قانوني خاص، أُخضع هذا المراهق للمراقبة مع تعليق العقوبة لمدة سنتين، لا يحق له خلالهما تملك أو استخدام جهاز مودم، أو أي وسائل اتصال عن بُعْد، مع أجهزة أو شبكات الحاسب بصورة مباشرة أو غير مباشرة، وأن يدفع تعويضاً لشركة الهاتف، وأن يكمل ٢٥٠ ساعة خدمة اجتماعية بالإضافة إلى مصادرة جميع أجهزة الحاسب التي استخدمت خلال فترة قيامه بنشاطه الإجرامي.

وقد علّق النائب العام الأمريكي دونالد ك. ستيرن على ذلك قائلاً: «إن شبكات الحاسب والهاتف هي قلب الخدمات الحيوية التي تقدمها الحكومة والقطاع الخاص، وهي البنية التحتية المهمة للدولة، وهي ليست لعبة لتسلية المراهقين لأن الهجوم على أي جهاز حاسب أو شبكة هاتف يمكن أن يشكل خطراً هائلاً على الجمهور، ولذا، فإن الحكومة ستحاكم المراهقين المتطفلين (الهاكرز) في القضايا المناسبة مثل هذه القضية».

## ٦-٩ عمليات اختراق متفرقة

هناك عدد من العمليات المميزة التي قام بها مخترقون (هاكرز)، وربما كان الباعث لتميزها هو الأثر النوعي الذي أحدثه، أو الطريقة التي تمت بها، ومن هذه العمليات:

### ٦-٩-١ هاكر نيوزيلندي يحذف ٥٠٠٠ موقعاً للإنترنت

في هجوم يعدُّ الأكبر من نوعه الذي تشهده نيوزيلندا على شبكة الإنترنت، قام أحد المتطفلين عام ١٩٩٨، بالدخول في خدمة مضيف في الولايات المتحدة الأمريكية تحمل مواقع



obeikandl.com

عنكبوتية مملوكة، لزبائن موفر خدمة إنترنت نيوزيلندي وقام بحذف ٥٠٠٠ موقع إلكتروني.

## ٦-٩-٢ هجوم على مواقع يابانية حكومية

أعلنت الحكومية اليابانية عن تعرض موقع وكالة العلوم والتقنية في اليابان على الإنترنت، لهجوم مزدوج تم فيه اختراق الصفحة الرئيسة، للموقع مرتين متتاليتين يومي الأربعاء والخميس ٢٦ و ٢٧ يناير ٢٠٠٠م، وقد سبقهما هجومين آخرين يوم الثلاثاء ٢٥ يناير ٢٠٠٠، على وكالة الإدارة والتنسيق ومكتب الإحصاء الياباني، وذكرت الحكومة اليابانية أنه الهجوم الأول من نوعه الذي تم على مواقع حكومية يابانية حتى التاريخ المذكور. وكان التركيز في هذا الهجوم على انتقاد الحكومة اليابانية، على محاولتها إنكار حدوث مجزرة "نانجينغ" التي راح ضحيتها ما يقرب من ثلاث مئة ألف من الصينيين عام ١٩٣٧، وهو أمر أثار حفيظة الصينيين الذين خرجت مجموعات منهم في مظاهرات احتجاجية على ذلك.

وقد قام المهاجمون باستبدال النصوص الموجودة على صفحات المواقع الرئيسة، بعبارات كتبت باللغتين الصينية والإنجليزية، تضمنت كلمات وشتائم بذيئة، فضلاً عن وصل أحد المواقع بموقع إنترنت إباحي، وكذلك شطب بيانات موقع الإحصاء بشكل كامل. ولكنه تمَّ استرجاع البيانات من نسخة احتياطية.

## ٦-٩-٣ عملية بعشرة ملايين دولار

حظي فلاديمير ليفين بشهرة واسعة بعد أن سرق عشرة ملايين دولار في عميلة مثيرة.

إذ اخترق ليفين شبكة (سيتي بنك) الأمريكي المشهور على مستوى العالم في عام ١٩٩٤م، وحصل على بعض الصلاحيات في الشبكة التي سهلت له الوصول إلى بعض الحسابات البنكية، وبمجرد الدخول إلى هذه الحسابات قام ليفين بتحويل (١٠,٧) مليون



Obeikandl.com

دولار إلى حسابات أخرى في الولايات المتحدة، وفنلندا، وألمانيا، والكيان الصهيوني، وهولندا. وقد قام ليفين بتحول هذه المبالغ بمعاونة ثلاثة من العاملين، داخل البنك الذين تم تخويلهم بجمع المال المسروق.


شكل ٦-٧: فلاديمير ليفين

وحين حاول المتعاونون معه الاختفاء بالمال المسروق، تم القبض عليهم. وتسبب التحقيق معهم في التوصل إلى ليفين، والبدء في ملاحقته بينما كان يعمل في شركة لتقنية الحاسب في سانت بطرسبرج في روسيا. وألقي القبض عليه في مطار هيثرو بلندن في مارس ١٩٩٥م، ولم تبدأ محاكمته حتى سبتمبر ١٩٩٧م، وانتهت المحاكمة بالحكم عليه بالسجن لمدة ثلاث سنوات في فبراير ١٩٩٨.

obeikandl.com

# ٦-١٠ أشهر مجموعات الاختراق على الإنترنت

يوضح الجدول الآتي أسماء أشهر مجموعات الاختراق على الإنترنت، ونلحظ المجموعة المسماة S4udi-S3curity-T3rror التي يبدو من اسمها أنها مجموعة سعودية.

| | | | | |
|---|---|---|---|---|
| Hmei7 | [elite top team#] | core-project | Prime Suspectz | S4udi-S3curity-T3rror |
| iskorpitx | Swan | 1923Turk | eMP3R0r TEAM | NobodyCoder |
| Fatal Error | D.O.M | linuXploit_crew | spook | Kernel_Attack |
| chinahacker | Triad | Poizonb0x | THE FREEDOM | Sovalye |
| Ashiyane Digital Security Team | 3n_byt3 | PowerDream | Silver Lords | DATA ir Security Group |
| Mafia Hacking Team | HEXB00T3R | KHG | Persian Boys Hacking Team | SPYKIDS |
| DeltahackingSecurityTEAM | LaTinHacKTeam | XTech Inc | ISCN | reDMin |
| Red Eye | sinaritx | Hi-Tech Hate | nf3rN.4lL! | OutLaw |
| uykusuz001 | ZoRRoKiN | S4t4n1c_S0uls | Vezir.04 | dark-underground |
| Iran Black Hats Team | By_aGReSiF | BeLa | batistuta | m0sted |

جدول ٦-١ أشهر مجموعات الاختراق

obeikandl.com

# ٦-١١ أشهر الجرائم الإلكترونية في العامين ٢٠١١/٢٠١٢

يعد العام المنصرم عاماً مفصلياً في تطور الجرائم الإلكترونية، وما تسببت به من خسائر مادية جسيمة على كافة الأصعدة وهنا سنستعرض أكبر عمليات الاختراق التي حدثت في عام ٢٠١١ ومطلع عام ٢٠١٢:

## ٦-١١-١ أكبر عملية تجسس

بهدف سرقة البيانات والتجسس، شُنَّت موجات عنيفة من الهجمات ضد الولايات المتحدة وبلدان أوروبية أخرى، ويرجح الكثيرون أن الصين هي مصدر هذه الهجمات، إذ تستخدم التجسس عبر الإنترنت للحاق بركب منافسيها الغربيين فضلا عن سعيها لتحقيق التوازن العسكري. وفي مقابلة نادرة على (SkyNews) صرّح رجل أعمال صيني بأنه يعمل مع الحكومة لاختراق الشركات المنافسة في الدول الغربية، وكشف عن صلات غامضة بين القراصنة والحكومة الصينية. وفي التقرير ذاته قال رجل شرطة: «نحن هنا لنرى ما إذا كان لديهم أي شيء يمكننا استغلاله، إذا كان هناك ما يدعو للاهتمام، فإننا سوف نحاول الحصول عليه، والقيام بالخطوات اللازمة». وقد ولدت الحصول على المعلومات واستغلال البيانات الحساسة «أعظم تحول للثروة في التاريخ»، بحسب وصف الجنرال كيث الكسندر.

فالحكومات ولاسيما الصين تسعى جاهدةً لتحقيق أهدافها المحددة في كتاب (الحرب غير المقيدة) انظر الشكل٦-٨. إذ إن واحدا من المكونات الرئيسة للكتاب هو (حرب الشبكة) والتي غالبا ما تكون ذات تكلفة هائلة وفق تقرير مكتب مكافحة الاستخبارات الذي يؤكد أن ما بين (٢ — ٤٠٠) مليار دولار هي مقدار الخسائر التي وقعت بسبب التجسس الإلكتروني.



obeikandl.com


شكل ٦-٨: صفحة الغلاف لكتاب (الحرب غير المقيدة)

## ٦-١١-٢ مواقع حكومية وعسكرية للبيع !!

ظهرت مؤخراً خدمات إلكترونية تقدم خدمة اختراق المواقع الحكومية والعسكرية باستغلال ثغرات حقن قواعد البيانات (SQL Injection) حيث إن المئات من المواقع مصابة بهذه الثغرة الخطيرة التي يمكن استغلالها والحصول على صلاحيات مدير النظام، ومن ثم يتم بيع هذه البيانات لمخترقين آخرين، وبإمكان من يملك ٥٠ دولاراً أن يستأجر هذه الخدمة ليتمكن من اختراق مواقع عسكرية كما تشير لائحة أسعار خدمات الاختراق الآتية:



obeikandl.com


**شكل ٦-٩:** لائحة أسعار خدمات الاختراق

لقد أثبتت ثغرة حقن قواعد البيانات (SQL Injection) بأنها الأغلى تكلفة، والثغرة الأكثر انتشارا في التاريخ. والموقع أعلاه يوضح كيف أن هذه الثغرة قد تستخدم من قبل المخترقين لجني الأرباح من خلال بيع ما يحصلون عليه من بيانات ومعلومات للمهتمين بها، إذ لم يعد اختراق الأنظمة لمجرد التحدي والمتعة وإنما لجني الأموال!

### ٦-١١-٣ سوني (SONY)

تم اختراق شبكة سوني الترفيهية والاستحواذ على بيانات أكثر من ١٠٠ مليون مشترك في شبكة سوني للموسيقا (Qriocity) وشبكة الألعاب (PSN) منها ١٢ مليون بيانات غير مشفرة والبيانات الائتمانية للمشتركين، وكان هذا الاختراق هو الأكبر نوعاً وكماً لعام ٢٠١١ مما كان له الأثر الأكبر على عدة أوجه.

قوائم الخسارة الكبيرة لأسهمها في سوق الأسهم كما يشير الرسم البياني الآتي:


شكل ٦-١٠: انخفاض سهم سوني في سوق الأسهم بعد عملية الاختراق

رفع هذا الاختراق من قيمة تأثير ثغرة حقن قواعد البيانات (SQL Injection) بحيث جعله الهدف الأول لمحاولي اختراق المواقع.

كان الهدف الأساس للهجوم ليس إحراج سوني وإنما إسقاطها تماماً، وهو ما تم بالفعل حيث بقيت شبكات الألعاب الاجتماعية معطلة قرابة الشهر.

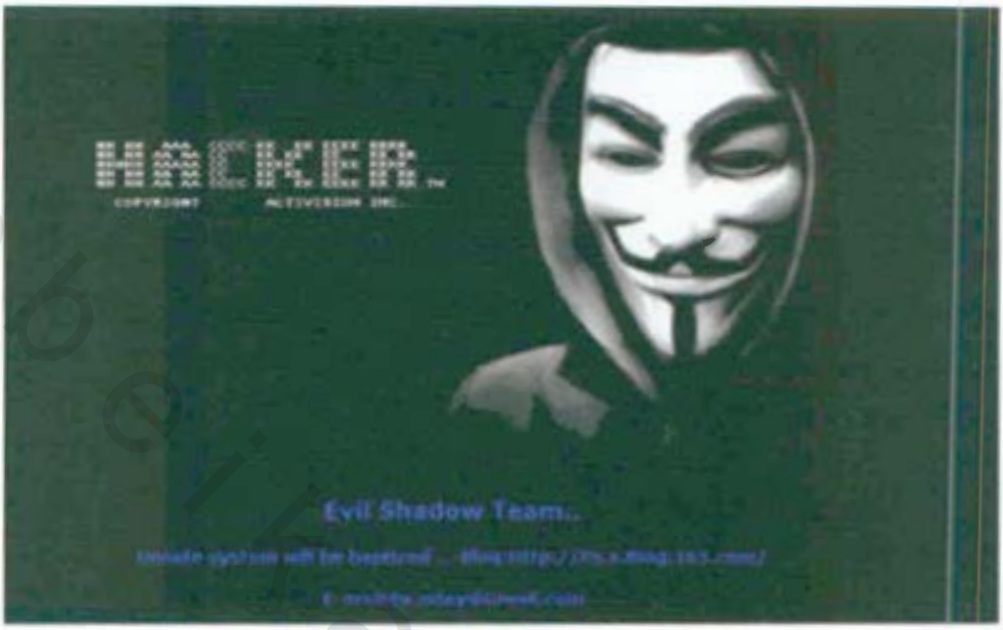
قدرت الخسائر المادية بقرابة ١٠٠ مليون فضلا عن خسارة السمعة وولاء الزبائن.

## ٦-١١-٤ اختراق متجر مايكروسوفت في الهند

قامت مجموعة من الهاكرز في منتصف فبراير ٢٠١٢، باختراق متجر مايكروسوفت لمستخدمي الهند، وقد تم وضع صورة للاختراق على الصفحة الرئيسة مما أدى إلى عدم قدرة المستخدمين الدخول إلى حساباتهم، انظر الشكل ٦-١١. ولم يقتصر الاختراق فقط على وضع الصورة، ومنع المستخدمين من دخول حساباتهم والتحميل، بل تمت عملية سرقة أسماء الحسابات مع كلمات المرور الخاصة بالمستخدمين.

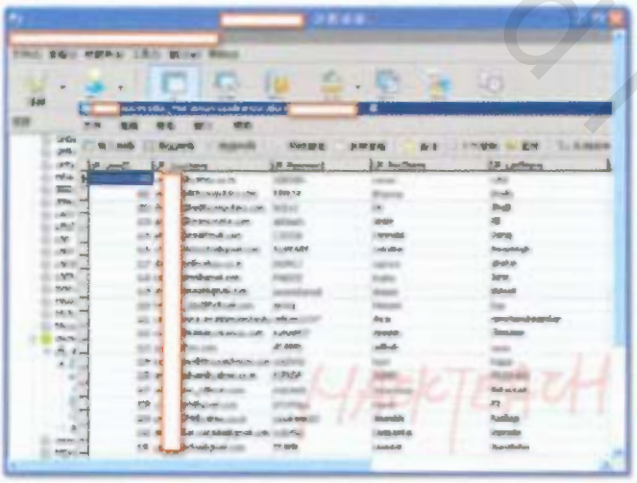


obeikandi.com




شكل ٦-١١ الصفحة الرئيسة لموقع متجر مايكروسوفت الهند.

وما يلفت النظر ويسترعي الانتباه أن المجموعة استطاعت الحصول على كلمات المرور لأنها كانت محفوظة في قواعد البيانات بشكل غير مشفر كما يوضح الشكل (٦-١٢).



شكل ٦-١٢ قواعد البيانات لموقع متجر مايكروسوفت الهند.

## ٦-١١-٥ موقع الاستخبارات المركزية الأمريكية

أدى تعرض موقع الاستخبارات المركزية الأمريكية (CAA) الإلكتروني للقرصنة على يد أشخاص استخدموا راية مجموعة القرصنة الشهيرة (أنونيموس) إلى توقفه ما يزيد عن ٩ ساعات.

وزعمت وسائل إعلام أمريكية أن مجموعة (أنونيموس) أعلنت مسؤوليتها عن الأمر قائلة أنها تمكنت من الحصول على المعلومات الشخصية لـ٤٦ ألف شخص في ألاباما. غير أنه بعد عدة ساعات نشرت المجموعة على صفحتها على موقع (تويتر) ملاحظة أوضحت فيها أن إعلانها عن تعرض موقع الـ(CAA) للقرصنة لا يعني أنها هي التي نفذت الهجوم الإلكتروني. ويشار إلى أن مجموعة (أنونيموس) تستهدف الوكالات الفدرالية الأمريكية وصعدت من هجماتها في الأشهر الأخيرة، فقرصنت مواقع تابعة لوزارة العدل الأميركية ومكتب التحقيق الفدرالي (FBI) ومواقع تابعة لشركات ترفيه.

## ٦-١١-٦ سرقة نحو ٤٠٠ ألف بطاقة ائتمانية إسرائيلية

مع بداية عام ٢٠١٢ تكاثرت الأخبار عن حدوث اختراق كبير طغى عليه البعد السياسي أكثر من جانبه التقني والمعلوماتي، فقد نشر مؤخرا أن مخترقاً يدعى (Ox Omar) قام باختراق حسابات مصرفية وعشرات الآلاف من بطاقات الائتمان العائدة لإسرائيليين إضافة شركة طيران العال والبورصة الإسرائيلية، وادعت إسرائيل أنه المخترق سعودي مقيم في المكسيك ويسمى عمر حبيب وهو ما نفته وزارة الخارجية السعودية، وفقاً لتقرير نشرته صحيفة (عكاظ)، فندت فيه المزاعم التي تداولتها وسائل إعلام إسرائيلية فذكرت أنه بمراجعة سجلات الرعايا في السفارة السعودية في المكسيك لم يعثر على أحد بهذا الاسم.



obeikandi.com

وأشارت تقارير إلى تمكن المخترق السعودي من نشر تفاصيل ٤٠٠ ألف بطاقة ائتمانية يملكها إسرائيليون إلا أن الشركات الائتمانية قالت أن نحو ١٤ ألف بطاقة فقط تضررت.

obeikandl.com

obeikandl.com

# الفصل السابع :
# أدوات الجريمة

obeikandl.com

لكي يتمكن المجرم في الإنترنت من تحقيق هدفه يجب أن يكون لديه بعض الأسلحة أو الأدوات التي تساعده على ذلك. وسيتطرق هذا الفصل إلى بعض الأدوات التي يستخدمها المجرمون في الإنترنت. فقد يحتاج المجرم لبعض الأدوات ويستغني عن بعضها الآخر اعتماداً على نوع الجريمة التي ينوي ارتكابها، وبناء على نوعية المجرم أيضا.

يكون الغرض من بعض هذه الأدوات هو الاستعداد لتنفيذ الجريمة، ويكون الهدف من بعضها الآخر هو القيام بتنفيذ الجريمة، أما القسم الأخير فيكون الغرض منه مسح آثار الجريمة. ونظراً لانتماء بعض الأدوات إلى أكثر من قسم، فلن يتم عرضها بناءً على هذا التقسيم، بل ستعرض واحداً تلو الآخر مع شرح الفائدة من كل سلاح.

وسيرد في هذا الفصل والفصول القادمة استخدام مصطلحي (المجرم) و(المخترق) بشكل متبادل، حيث إن المجرم في أغلب هذه الحالات يقوم بجريمته عن طريق الاختراق.



obeikandl.com

## ٧-١ تقنيات الشبكات

يعد هذا السلاح المعرفي من أهم الأدوات لمجرمي الإنترنت. ويمثل المعرفة بعلم شبكات الحاسب وكيفية عملها ومعرفة بروتوكولاتها. وهذا القسم مرتبط بشكل أو بآخر بجميع الأقسام الأخرى من أقسام أدوات المجرمين. قد لا يحتاج المجرم للإلمام بعلم الشبكات في بعض الأحيان. ولكن في أحيان أخرى كثيرة سيحتاج المجرم لمعرفة كيفية عمل الأداة لكي يتمكن من استخدامه، وهذا ينطبق غالباً على الجرائم الكبيرة التي تستهدف شركات كبيرة ذات شبكات محصنة. وكما أن الأداة تستخدم من قبل المجرمين، فإنها أيضاً تستخدم من قبل من يريد الدفاع عن نفسه أو شبكته.

## ٧-٢ فاحصات المنافذ

هذه النوعية من الأدوات هي برامج تقوم بفحص جهاز أو مجموعة من الأجهزة، وتقوم بتحديد المنافذ المفتوحة في تلك الأجهزة. ووجود منفذ مفتوح في الجهاز يعني أنه مستعد لقبول اتصال من جهاز آخر على ذلك المنفذ. ويتم تعريف المنفذ بتحديد رقم معين، وهذا الرقم في الغالب يمكن ربطه بتطبيق من تطبيقات الحاسب، فمثلا؛ مزودات الويب في الغالب تكون على المنفذ رقم ٨٠، ومزودات نقل الملفات (FTP) تكون على المنفذ ٢١، ويوضح الجدول ٧-١ بعض المنافذ والتطبيقات المقابلة لها. وفائدة هذه البرامج بالنسبة للمستخدم هي أنها تقوم بإعطائه معلومات مبدئية عن الجهاز الذي يرغب في اختراقه، أو أنها تساعده على تحديد الجهاز الذي يريد اختراقه. فمثلاً، ما الفائدة من تجربة البرامج التي تقوم باختراق مزودات الويب على جهاز، ما لم يكن ذلك الجهاز محتوياً على خادم ويب في الأصل. وكذلك أيضاً فإن المجرم قد يرغب في تحديد الأجهزة التي تحتوي على مزود نقل ملفات لكي يحاول اختراقها، ففي هذه الحالة يمكنه



obeikandl.com

استخدام برامج فاحصات المنافذ لكي تقوم بفحص عدد من الأجهزة وإعطائه قائمة بالأجهزة والمنافذ المفتوحة في كل جهاز.

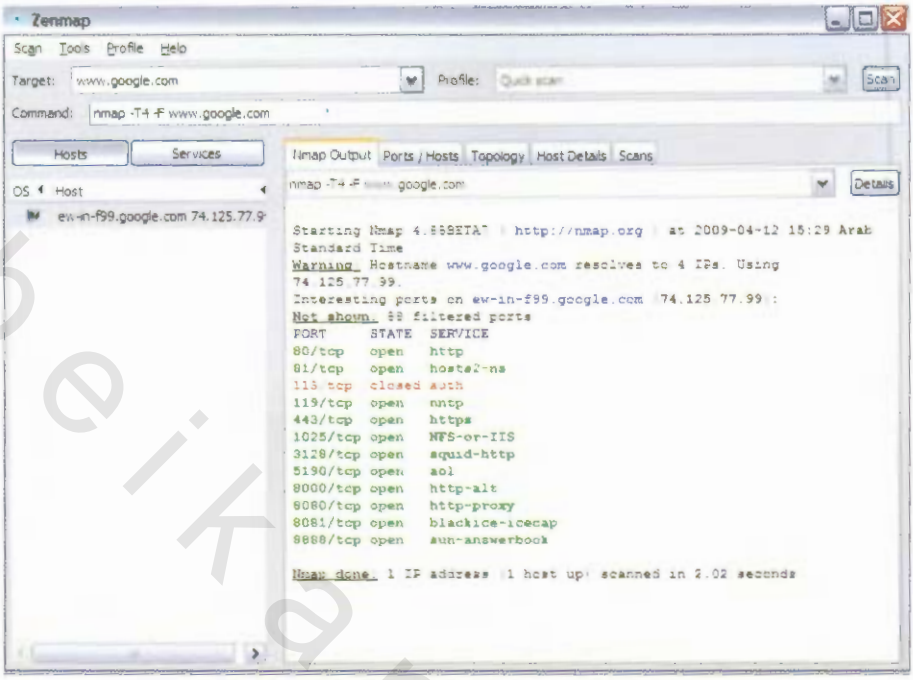
| المنفذ | التطبيق المستخدم |
|---|---|
| ٨٠ | مزودات الويب Web Servers |
| ٢١ | مزودات نقل الملفات FTP |
| ٢٥ | مزودات نقل البريد SMTP Servers |
| ١١٠ | مزودات استقبال البريد POP3 Server |
| ١٣٩ | تطبيق مشاركة الملفات في ويندوز Windows File Sharing |
| ٥٣ | مزود الأسماء DNS Servers |

جدول ٧-١: بعض المنافذ والتطبيقات المقابلة لها.

والقيام بعملية فحص المنافذ يتطلب عادةً محاولة إنشاء اتصال بين الجهاز الفاحص والمفحوص، مما يعني أن الجهاز المفحوص سيلاحظ محاولة الاتصال، وفي بعض الشبكات المحصنة، فإن هذا سيقرع ناقوس الخطر للمشرف على الشبكة مبيناً وجود من يقوم بجمع المعلومات عن الشبكة. لهذا فإن بعض برامج فحص المنافذ المتقدمة تقوم بالقيام بفحص الجهاز الضحية بطريقة خفية ومن أشهر هذه البرامج برنامج (www.nmap.com)



obeikandl.com




شكل٧-١: لقطة من برنامج nmap لفحص المنافذ من (www.insecure.org)

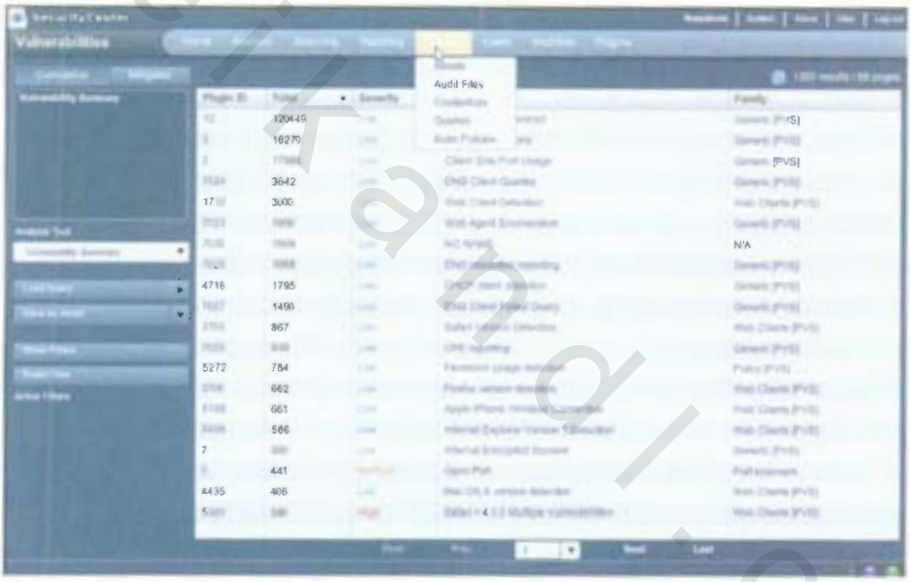
## ٧-٣ برامج تحديد الثغرات

إن برامج تحديد الثغرات هي مشابهة في الهدف لبرامج فاحصات المنافذ، ولكنها أعقد وأكثر تقدماً منها. فهي مزودة ببعض الثغرات الموجودة في بعض التطبيقات، التي تستخدمها لكي تقوم بفحص جهاز أو مجموعة من الأجهزة لتحديد الثغرات الأمنية الموجودة بها، ومعرفة بعض المعلومات المفصلة عنها. وطريقة عمل هذه البرامج تقوم أولاً على فحص المنافذ وعند وجود منفذ مفتوح في الجهاز الضحية، فإن البرنامج يقوم بتجربة الثغرات المشهورة المرتبطة بهذا المنفذ، ومن ثم إعطاء المخترق تقريراً كاملاً عن الجهاز أو (الأجهزة) الضحية، ويحتوي التقرير على المنافذ المفتوحة والتطبيقات المرتبطة بها، وعدد الثغرات الموجودة في هذه الأجهزة.

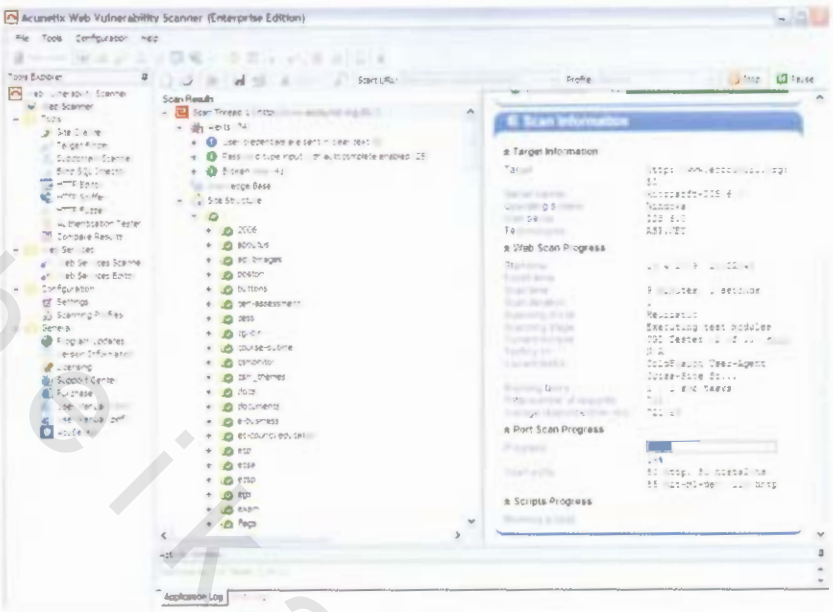


obeikandl.com

وهذا بالتأكيد يعطي معلومات أكثر من تلك التي تعطيها برامج فاحصات المنافذ. فمثلاً؛ برامج فاحصات المنافذ تقوم بإخبار المخترق بأن الجهاز يحتوي على منفذ مفتوح على الرقم ٨٠. بينما برامج تحديد الثغرات تخبر المخترق بأن الجهاز يحتوي على منفذ ٨٠ مفتوح، وأن الجهاز من نوع ويندوز٧ وهو محتوٍ على الإصدار ٧،٥ من برنامج Internet Information Services (IIS) وأنه تمت تجربة ثغرة (Buffer overflow) بنجاح، بينما فشلت تجربة الوصول للقرص الصلب.




شكل ٧-٢ صورة لأحد برامج مسح الثغرات




شكل ٧-٢ صورة لأحد برامج فحص الثغرات لتطبيقات الويب.

وتساعد مثل هذه البرامج على حفظ وقت المتطفل، وذلك بتجربة كل الثغرات المعروفة آليًا ودون الحاجة لتدخله. وهي أيضا تساعده على جمع المعلومات عن الجهاز الضحية، وهي المرحلة الأولى من مراحل الاختراق (سيتم الحديث عن ذلك في الفصل التالي)

على الرغم من أن هذه البرامج تساعد المجرم بشكل كبير، إلا أنها لا تغنيه بشكل كامل، حيث يتم اكتشاف الثغرات بشكل دائم ومستمر، وقد لا تحتوي هذه البرامج على آخر ما تم اكتشافه من الثغرات، التي تعد من أخطر الثغرات حيث يغفل المشرفون على الشبكات أو يتأخرون عن تحديثها. لذا فقد يحتاج المخترق للقيام بذلك بشكل يدوي أو باستخدام برامج أخرى مستقلة.

وعلى الرغم من أن هذه البرامج تستخدم في الغالب من المتطفلين والمجرمين. إلا أنه يمكن استخدامها من قبل المشرفين على الشبكات لتحديد الثغرات الموجودة في شبكاتهم قبل أن



obeikandl.com

يحددها المجرمون، وهذا أحد التطبيقات المقترحة لتلك النوعية من البرامج.

## ٧-٤ البرامج المتنصتة

وهذه النوعية من البرامج هي اسم على مسمّى، حيث يستخدمها المخترق عند ارتباطه بشبكة معينة لكي تقوم بالتقاط كل البيانات التي يتم تبادلها في تلك الشبكة. وهذه البيانات قد تكون بيانات غير مهمة، مثل صفحة الأخبار التي قام أحد المستخدمين بزيارتها، ولكنها في أحيان أخرى كثيرة قد تكون مهمة جداً، مثل كلمة السر الخاصة بالبريد الإلكتروني، أو رقم البطاقة الائتمانية.

وتعمل هذه البرامج ضمن بعض أنظمة الشبكات، إذ إن البيانات المرسلة من جهاز إلى جهاز آخر يتم إرسالها لجميع الأجهزة في تلك الشبكة، وتقوم جميع الأجهزة بتجاهلها، ما عدا الجهاز الذي أرسلت له تلك البيانات حيث يقوم باستقبالها. وهذه البرامج تقوم بوضع كرت الشبكة في وضع التنصت الذي يمكّن الكرت من استقبال جميع البيانات، سواء كانت موجهة له أو لغيره.

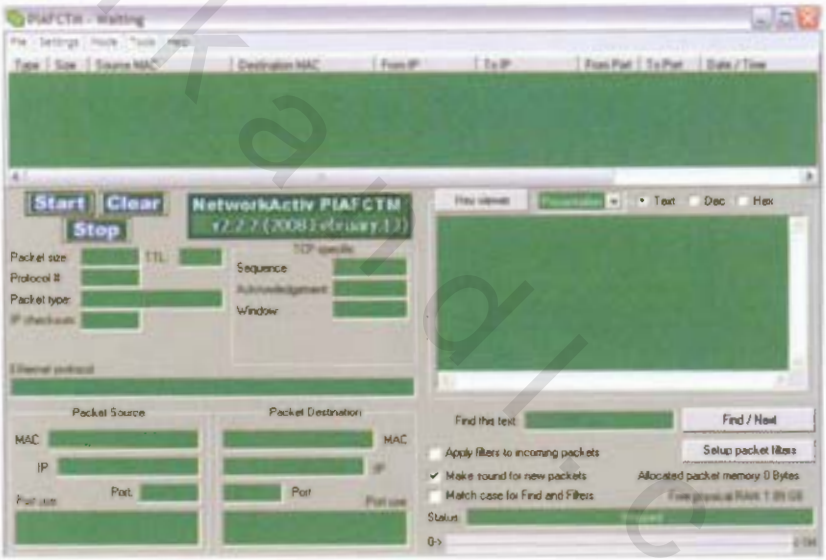
ولكن لكي يتمكن المخترق من استخدام هذه البرامج، فلابد له أن يكون مرتبطاً بالشبكة التي يريد اختراقها، ليتمكن من التنصت على البيانات المارة خلال تلك الشبكة. مع العلم بأن معظم الشبكات الحديثة تقوم بوضع ما يسمى بالمقسم، وهو جهاز يسمح بنقل البيانات مباشرة من الجهاز المرسل إلى الجهاز المستقبل دون أن تراها الأجهزة الأخرى، بعكس الموزع الذي يقوم بوضع البيانات على وسيط مشترك بين كل الأجهزة المرتبطة به بحيث تستقبلها جميع الأجهزة المرتبطة بهذا الوسيط المشترك. وإذ يظن بعضهم أن المقسم يبطل عمل البرامج المتنصتة إلا أن هناك العديد من الوسائل التي تمكّن مثل هذه البرامج من العمل على المقسم، مثل ما يسمى بـ (ARP Cache Poisoning) ، وكذلك (Switch Port Stealing)



obeikandl.com

وأيضا (CAM Table Flooding).

ولعل ظهور تقنية الشبكات اللاسلكية زادت من خطورة هذه النوعية من البرامج، حيث إنه في السابق كان لابد للشخص من الارتباط بالشبكة بشكل سلكي، أي إنه لابد له من الوجود في مقر الشبكة وربط جهازه بالموزع. أما مع ظهور الشبكات اللاسلكية فإنه يكفي المتطفل أو المجرم أن يكون ضمن نطاق بث جهاز نقطة الاتصال التي تعمل كوسيط مشترك بين الأجهزة في الشبكة لكي يتمكن من التقاط البيانات المارة في الشبكة. وهذا يعني أنه بإمكانه أن يكون داخل سيارته في مواقف المبنى لكي يتمكن من الارتباط بالشبكة.



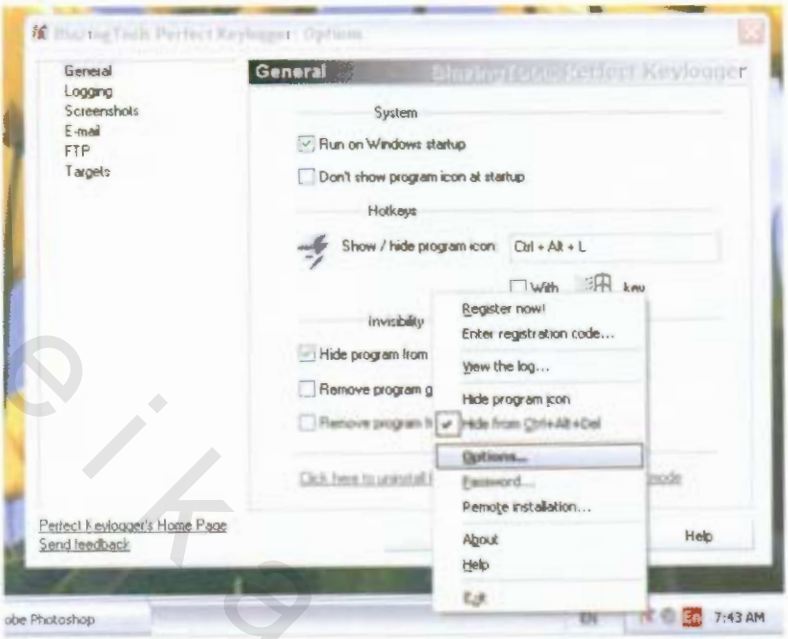

شكل ٧-٣ : لقطة لبرنامج (NetworkActiv) الذي يقوم بالتنصت

## ٧-٥ تسجيل لوحة المفاتيح

هذه النوعية من الأدوات تقوم بتسجيل كل ما يقوم المستخدم بكتابته على لوحة المفاتيح، وحفظه لكي يقوم المخترق بالاطلاع عليه فيما بعد. وتوجد هذه النوعية من الأدوات على نوعين، أحدهما برامج يتم تركيبها في الجهاز، والآخر هو عتاد يتم وصله في الجهاز بين سلك لوحة المفاتيح والمنفذ الخاص بها في الجهاز. والفرق بينهما هو أن البرامج تعمل عندما يعمل نظام التشغيل، وهي بذلك لا تستطيع تخزين ما يكتبه المستخدم قبل الدخول لنظام التشغيل، مثل كلمة السر الخاصة بـ(BIOS) ولكنها في نفس الوقت تتميز بسعة عالية، حيث تقوم بتخزين كل ما يكتبه المستخدم حتى تنفذ المساحة في قرصه الصلب. أما بالنسبة لنوعية العتاد، فميزتها أنها تعمل بمجرد تشغيل الجهاز، فهي لا تعتمد على نظام التشغيل، بل هي قطعة مستقلة بذاتها، ولكنها في الوقت نفسه ذات مساحة محدودة، ويتطلب المخترق من الوصول الفيزيائي للجهاز لكي يقوم بفكها أو تركيبها، بعكس البرامج التي يمكن تركيبها عن بعد. وغالب البرامج من هذه النوعية تعمل بحيث لا يستطيع المستخدم رؤيتها ضمن قائمة البرامج العاملة في النظام عندما يضغط على Alt+Ctrl+Del . انظر الشكل ٧-٤.



obeikandi.com




شكل ٧-٤: برنامج Perfect Key logger

(ويظهر فيها خيار إخفاء البرنامج من الظهور في قائمة البرامج العاملة)

## ٧-٦ برامج التروجان (حصان طروادة)

أغلبنا يعرف قصة حصان طروادة الشهير، الذي كان يبدو في ظاهره كالهدية، ولكنه كان يحتوي على جنود الجيش، الذين ما أن دخل الحصان إلى وسط المدينة حتى قاموا بالخروج من الحصان واحتلوا المدينة.

برامج أحصنة طروادة، التي درج الناس على تسميتها بـ (التروجان) نسبة إلى كلمة Trojan الإنجليزية التي تعني طروادة، تعمل بنفس الطريقة، فهي برامج ترسل للمستخدم على أنها برنامج

مفيد أو لعبة أو غيرها من البرامج التي يرغب المستخدم بها، وما أن يقوم المستخدم بتشغيلها حتى تقوم تلك البرامج بفتح منفذ في جهاز المستخدم، وانتظار المخترق لكي يقوم بإرسال الأوامر لها. وإكمالا لخداع المستخدم الضحية، فإن البرامج الحاملة للتروجان تعمل في الغالب، وذلك حتى لا يشك المستخدم في الحيلة.

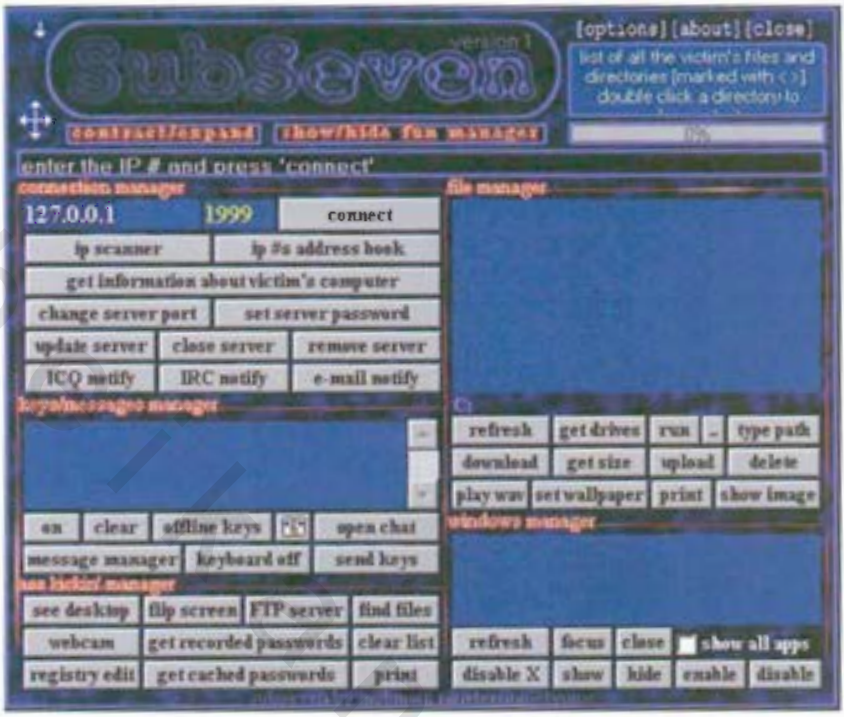
وبرامج أحصنة طروادة الشهيرة تنقسم لأربعة أقسام:

**أولاً**: البرنامج الحامل، وهو البرنامج الذي يقوم بخداع المستخدم حتى لا يشك في الأمر. وهذا البرنامج قد يكون أي نوع من البرامج بدءًا من الألعاب وحتى برامج معالجة الكلمات أو تحميل الأفلام، وغيرها.

**ثانيًا**: البرنامج الخادم، وهذا البرنامج يكون ملحقاً في البرنامج الحامل بشكل خفي، بحيث ما إن يقوم المستخدم بتشغيل البرنامج الحامل حتى يقوم البرنامج الخادم بتركيب نفسه بحيث يعمل بشكل دائم، وكذلك أيضاً فإنه يقوم بفتح منفذ قام المخترق بتحديده مسبقاً، ويبدأ في الاستماع انتظاراً لأوامر المخترق.

**ثالثاً**: البرنامج العميل، وهو برنامج موجود لدى المخترق، ويسمح له بالاتصال بأي جهاز ضحية، وإصدار الأوامر التي تتراوح من فتح باب مشغل القرص المدمج CD إلى عرض الملفات في جهاز الضحية وسحبها، أو رؤية ما هو خلف الكاميرا في حالة وجود كاميرا. وبعض البرامج أيضا تسمح بوضع رسالة على شاشة الضحية.

**رابعاً**: برامج الدمج، وهذه البرامج وظيفتها هي دمج برنامج الخادم بالبرنامج الحامل ليصبحا برنامجاً واحداً، وذلك لخداع المستخدم.




شكل ٧-٥: لقطة لبرنامج SubSeven Client

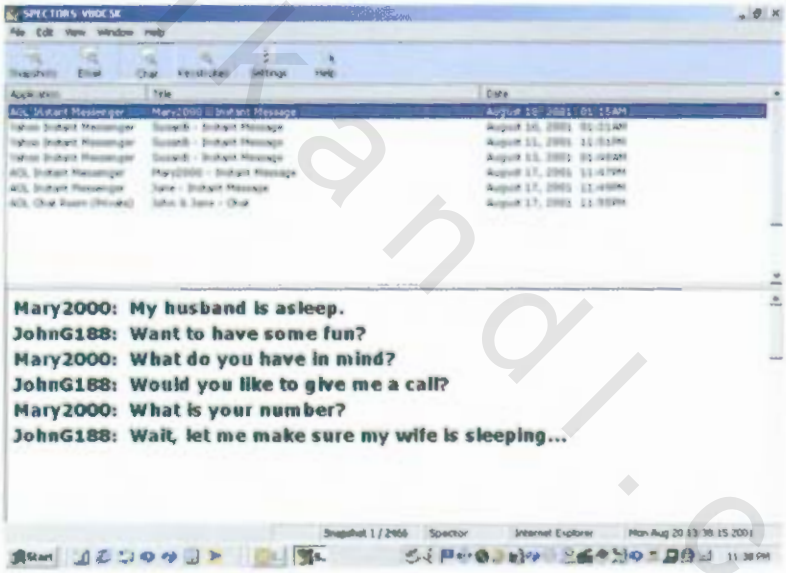
## ٧-٧ برامج التجسس

هذه البرامج، كما هو مسماها، تقوم بالتجسس على جهاز المستخدم، وذلك بتسجيل كل ما يقوم به، سواء أكان نص محادثة أو عنوان موقع أو بريداً إلكترونياً. وهي تختلف عن برامج تسجيل لوحة المفاتيح في كونها تقوم بتفصيل كل شيء على حدة، فهي تعطي المخترق تقريراً كاملاً ومبوباً بكل ما قام المستخدم الضحية بعمله، مفصلاً على قائمة من الرسائل التي استقبلها، والمواقع التي زارها ونصوص المحادثة التي قام بها. وهذه البرامج أيضاً تقوم بعمل لقطة

لمحتوى الشاشة بشكل متكرر وإلحاق ذلك بالتقرير الذي يستلمه المخترق.

وتعمل هذه البرامج أيضا بالنظام الخفي، حيث لا يتمكن المستخدم من معرفة عملها. ويحتوي أغلبها على الخيار الذي يسمح لها بإرسال هذا التقرير بالبريد الإلكتروني إلى من قام بتركيبها لكي يطلع عليه أينما كان.

والتطبيق الشائع لهذه البرامج هو ما يقوم به الأزواج من مراقبة زوجاتهم أو العكس لكشف خيانتهم. ولقد وجدت الكثير من قضايا الطلاق التي استندت على تقارير هذه البرامج كدليل أساسي فيها.




شكل ٧-٦: لقطة لخاصية تسجيل نصوص المحادثة في برنامج Spector



obeikandl.com

## ٧-٨ برامج تعطيل الخدمة

الغرض الرئيس من هذه البرامج هو تعطيل الجهاز الخادم (المزود) والمغار عليه عن تقديم خدماته للمستخدمين والأجهزة الأخرى المستحقة للخدمة. وفكرة عمل هذه البرامج هي إرسال العديد من الطلبات للخادم الضحية، بحيث يعتقد الجهاز الخادم بأن هذه الطلبات هي طلبات حقيقية ويحاول القيام بخدمتها، مما يجعله مشغولاً عن خدمة الطلبات التي يقدمها المستخدمون العاديون والمستحقون للخدمة. ويطلق على هذه النوعية من الهجمات، هجمات تعطيل الخدمة (DoS) ، وهناك نوعية أخرى يتم تنفيذها بشكل موزع، حيث تقوم مجموعة كبيرة من الأجهزة بالقيام بهذه النوعية من الهجوم في وقت واحد وهذه النوعية يطلق عليها الهجمات الموزعة لتعطيل الخدمة (DDoS) ولعل آخر هجمة شهيرة هذا القبيل هو ما حدث لموقع ويكيليكس المتخصص في نشر الوثائق السرية، فحين ملأ هذا الموقع الدنيا وشغل الناس بأخباره وتسريباته، انشغلت جهة ما بتجهيز جيش كبير وإعداد العدة لغزو الموقع وتدميره، ففتحت عليه سيلا جارفًا من الرسائل الإلكترونية مما أدى إلى تضعضع الموقع وتوقفه عدة مرات، والطريف في الأمر أن جنود هذا الجيش العظيم أصغر من أن تُرى، وأخفى من تلمس أو تحس، وتعرف بين المختصين بـ(البوت)، وهي برامج يتم تنزيلها وتركيبها بصور مختلفة على الأجهزة المصابة كأشباح رقمية، وتدار عن بعد بواسطة خادم التحكم والسيطرة (C2S). وتصبح أجهزة المستخدمين أداة للآخرين بغير علم أصحابها، وتشكل مجاميعها شبكة تقوم بهجمات تسمى الهجوم الموزع لتعطيل الخدمة، ويصنف هجوم (البوت نت) على موقع ويكيليكس على أنه من أعلى الهجمات خطورة نظرًا لحجم البيانات الكبير التي تعدت ١٠ غيغا في الثانية (١٠ Gbps). وقد حدث إغلاق الموقع في نهاية ٢٠١٠م، وتكررت الهجمات عليه ثانية، وكان آخرها ٢٠١١/٨/٣٠م، عند أعلن موقع ويكيليكس تعرضه لهجوم إلكتروني بعد انتقادات وجهت إليه لنشره آلاف الوثائق الدبلوماسية الأميركية الجديدة. ومن أشهر برامج الهجمات الموزعة لتعطيل الخدمة أيضاً،

برنامج (Trinoo)، وبرنامج TFN (Tribal Flood Network).

## ٧-٩ إخفاء الهوية

عند اكتشاف أي هجمة على موقع من المواقع، فإن المشرفين عليه سيقومون بتتبع مصدر الهجمة لمقاضاته. ولهذا فإن المخترقين في الغالب يلجؤون لإخفاء هوياتهم، وذلك بطريقتين:

الأولى: اختراق أجهزة وسيطة والسيطرة عليها ومسح آثارهم من تلك الأجهزة، ومن ثم استخدام هذه الأجهزة للقيام بالاختراق. ففي هذه الحالة وعند تتبع مصدر الهجمة، فإن الأثر سينتهي عند تلك الأجهزة ولن تصل للمخترق.

الثانية: استخدام بعض البرامج التي تقوم بإخفاء الهوية، وهي تعمل ذلك بكونها أجهزة وسيطة بين المستخدم وبين ما يطلبه، ويكون هناك غالبا نوع من التشفير والعشوائية لضمان عدم إمكانية تتبع المستخدم. ولكن هذه البرامج أصلاً وضعت لمن يخشون على خصوصيتهم في الإنترنت ولم توضع للمخترقين. لذا فإنه نادراً ما تستخدم للقيام بعمليات الاختراق، بل يلجأ المخترقون للقيام بذلك باستخدام النوع الأول. ولعل أشهر البرامج من هذه النوعية هو برنامج (Freedom) من شركة (Zero-Knowledge) التي قامت بإغلاق خدمتها بعد فترة وجيزة. وكذلك برنامج (JAP) الذي يمكن الحصول عليه من الموقع الألماني http://www.anon-online.de



obeikandi.com

## ٧-١٠ برامج التشفير وفك التشفير

هذه النوعية من البرامج يكون هدفها فك تشفير البيانات الخاصة بالمستخدم، سواء كانت هذه البيانات عبارة عن ملفات مشفرة، أو أنها كانت بيانات مشفرة تمر بالشبكة بين جهاز المستخدم وجهاز آخر.

تقنيات التشفير الموجودة حالياً لا تضمن عدم إمكانية كسر الشفرة، ولكنها تضمن أن ذلك سيستغرق وقتاً طويلاً تصبح البيانات بعده عديمة الفائدة. فبعض تقنيات التشفير المعتمدة على المفتاح العام والمفتاح الخاص قد تتطلب مئات السنين لفكها.

ولكن الجهات الاستخباراتية المنتمية للدول تمتلك من القدرة الحاسوبية ما يمكنها من القيام بذلك في فترات قصيرة جداً. ويوجد في الإنترنت العديد من المشاريع التي تستخدم القدرة الحاسوبية لأجهزة ملايين المستخدمين، لكي تقوم بفك تشفير بيانات معينة. ولقد قامت شركة (RSA) الشهيرة بوضع مسابقات ذات جوائز تقدر بعشرات الآلاف من الدولارات، لمن يقوم بكسر بيانات قامت بتشفيرها ووضعها على موقعها. ولقد تم فعلاً كسر بعض هذه البيانات، ومازال بعضها الآخر سليماً لم يتم فك تشفيره إلى الآن.

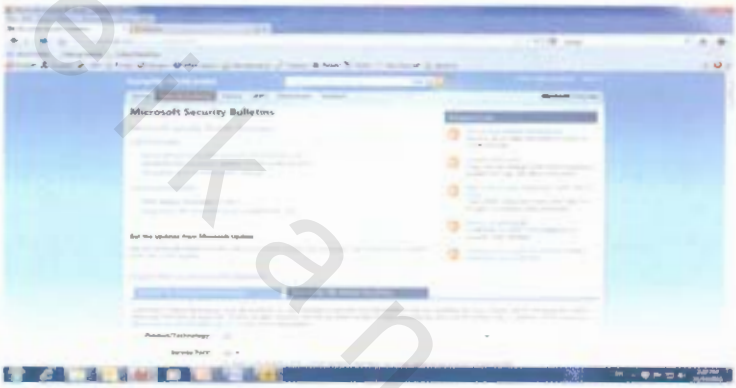
## ٧-١١ نشرات الثغرات الجديدة

يتوفر في الإنترنت الكثير من المواقع والقوائم البريدية التي تقوم بنشر أحدث الثغرات التي تم اكتشافها سواء كان ذلك على مستوى الأجهزة أو أنظمة التشغيل أو التطبيقات المختلفة. وتوفر هذه المعلومات على المجرم عناء البحث ومحاولة فتح ثغرة في النظام الذي يحاول اختراقه. كما أن حصول المجرم على هذه المعلومات قبل أن يحصل عليها المشرف على الشبكة، يمكنه من استخدام هذه الثغرات للقيام بجريمته سواء كانت حصوله على معلومات محمية أو قيامه بتخريبها.



obeikandi.com

للحد من فعاليه هذا السلاح فإن معظم البرامج وأنظمة التشغيل تقوم دورياً بالاتصال بموقع الشركة المنتجة للبرنامج، والحصول على التحديثات التي تقوم بإصلاح هذه الثغرات. ولكنها تبقى مسؤولية المشرف على الجهاز أو الشبكة أن يتأكد من حدوث ذلك. انظر الشكل المرفق.




شكل ٧-٧: لقطة لموقع الأمن من شركة مايكروسوفت الذي يعرض آخر الثغرات التي تم اكتشافها ويوفر البرامج اللازمة لإصلاحها.



obeikandi.com

# الفصل الثامن :
# مراحل الاختراق

obeikandl.com

سيركز هذا الفصل على جرائم الإنترنت التي تتطلب اختراقاً لجهاز أو مجموعة من الأجهزة، وبذلك تستثنى الجرائم التي لا علاقة لها بالاختراق، مثل جرائم الابتزاز أو جرائم الحقوق الفكرية. وسيقتصر هذا الفصل على الحديث عن المراحل التي تمر بها عملية الاختراق، ولكن قبل القيام بتفصيل هذه المراحل، ينبغي إلقاء الضوء على حجم هذا الجرم ومدى انتشاره، من خلال بعض الحقائق التي يقدمها موقع (zone-h) وهو من أهم المواقع المهتمة برصد جرائم الانترنت وخصوصا المتعلقة باختراق المواقع الإلكترونية وتغيير محتواها والتحكم بها.

فقد تلقى الموقع عام انطلاقه في ٢٠٠٢م، ما متوسطه ٢٥٠٠ حالة تشويه للمواقع المختلفة والمتباينة فيما بينها شهرياً، ثم ارتفعت هذه الحالات إلى حوالي ٦٠٠٠٠ حالة تشويه واختراق في ٢٠٠٩م، وارتفع العدد إلى ٩٥٠٠٠ حالة حتى شهر أبريل ٢٠١٠م.

ويبين الجدول ٨-١ والجدول ٨-٢ إحصاءات تشير إلى الزيادة المطّردة في حجم الاختراقات. وإحصاءات أخرى للاستفادة ومعرفة أسباب الاختراق وطرقه، ومقارنة نظم التشغيل المختلفة طبقا لمعدل اختراقها.

obeikandl.com

| الاختراقات خلال الشهور | عام ٢٠٠٨ | عام ٢٠٠٩ | ٢٠١٠ عام |
|---|---|---|---|
| يناير | ١٨,٥٦٢ | ٣٧,٩٦٨ | ٥٣,٩٢١ |
| فبراير | ٥١,٩٢٥ | ٢,٩١٩ | ٥٧,٨٦٩ |
| مارس | ٤٨,١٣٨ | ٧ | ٧٣,٧١٥ |
| إبريل | ٤١,٤٩٢ | ٦٠,٤٧١ | ٩٥,٠٩٠ |
| مايو | ٢٩,٠١٧ | ٤٨,٠٨٧ | |
| يونية | ٣٨,٤٤٥ | ٤٣,٥٦٩ | |
| يولية | ٣٩,٥٤٩ | ٤٥,٤٨٠ | |
| اغسطس | ٧٤,١٢١ | ٨٣,٨٥٠ | |
| سبتمبر | ٤٢,٣٧٩ | ٧٤,٣٨٤ | |
| أكتوبر | ٥٤,٩٧١ | ٥٤,٤٦٢ | |
| نوفمبر | ٤٤,٤٨٦ | ٤٣,١٧٧ | |
| ديسمبر | ٣٤,٣٧٤ | ٥٠,٠٣٥ | |

جدول ٨-١ توزع الاختراقات حسب الأشهر

openkandil.com

| Operational System | Year 2008 | Year 2009 | Year 2010 |
|---|---|---|---|
| Linux | 352.468 | 378.744 | 256.648 |
| Windows 2003 | 117.978 | 127.128 | 81.785 |
| Windows 2000 | 21.929 | 12.529 | 2.805 |
| FreeBSD | 13.418 | 10.050 | 5.503 |
| Unknown | 4.642 | 3.933 | 1.815 |
| Solaris $^{9}/_{10}$ | 3.002 | 7.699 | 364 |
| SolarisSunOS | 1.629 | 16 | 10 |
| MacOSX | 893 | 510 | 384 |
| Win NT9x | 440 | 225 | 132 |
| Win 2008 | 364 | 2.977 | 3.165 |
| Win XP | 329 | 270 | 72 |
| HP-UX | 216 | 85 | 32 |
| NetBSDOpenBSD | 69 | 99 | 39 |
| Solaris 8 | 35 | 41 | 5 |
| BSDOS | 10 | 14 | 2 |
| AS/400 | 6 | 1 | 1 |
| Com paq Tru64 | 6 | 16 | 2 |
| NovellNetware | 5 | 5 | 0 |
| Unix | 3 | 29 | 43 |
| IRIX | 3 | 12 | 5 |
| OpenVMS | 3 | 1 | 0 |
| AIX | 3 | 1 | 0 |
| MacOS | 3 | 0 | 2 |
| OpenBSD | 1 | 0 | 0 |
| Win Vista | 1 | 1 | 0 |
| OpenServer | 1 | 0 | 0 |
| Win .NET | 1 | 1 | 0 |
| OS2 | 1 | 0 | 5 |
| Dig i tal Unix | 0 | 3 | 0 |
| SCO Unix | 0 | 19 | 2 |

جدول ٨-٢ توزع الاختراقات حسب نظم التشغيل

obeikandl.com

وإذا تبيّن مقدار انتشار هذا النوع من الجرائم الإلكترونية وخطورتها، فإن آلية عمليات الاختراق ومراحلها لا تتطابق في كل الحالات، حيث إن نوع العملية ومعطياتها يختلفان من مجرم إلى آخر، وبناءً على ذلك تختلف المراحل التي تمر بها تلك الجريمة. ومعرفة هذه المراحل ضرورية لمن يريد حماية نفسه منها. فدراسة الخصم ومعرفة خططه وطريقة عمله تساعد بشكل كبير على اتقاء شرّه.

**ويمكن تقسيم المراحل التي تمر بها الجريمة في الإنترنت إلى ثلاثة مراحل رئيسة:**

**أولا:** مرحلة جمع المعلومات

**ثانيا:** القيام بالاختراق

**ثالثا:** مسح الآثار

وقد يندرج تحت كل مرحلة بعض المراحل الفرعية التي سيأتي الحديث عنها بالتفصيل.

## ٨-١ مرحلة جمع المعلومات

ويشبه خبراء الحماية هذه المرحلة باللص الذي يقوم بالدوران حول المنزل، ويحاول بخفة أن يرى ما إذا كان أحد أبواب المنزل أو نوافذه مفتوحة ليستخدمه للدخول للمنزل وسرقته. وهذا فعلاً ما يقوم به المجرم في هذه المرحلة، حيث يقوم باستخدام بعض الأدوات التي ذكرناها في الفصل السابع لجمع أكبر قدر من المعلومات عن الشبكة، أو الجهاز أو الشخص المستهدف. وهذه المعلومات في الغالب تكون:

- قائمة بالأجهزة الموجودة في الشبكة، ومع كل جهاز يوجد أكبر قدر من المعلومات عنه، مثل نوعية نظام التشغيل، والمنافذ المفتوحة، والثغرات الموجودة في التطبيقات التي تعمل في الجهاز.



obeikandl.com

- محاولة معرفة تصميم الشبكة، وهناك برامج وتقنيات تساعد على ذلك. ونقصد بتصميم الشبكة هو معرفة مواقع جدران الحماية ومعرفة عدد الشبكات الفرعية (Subnets) وأرقام (IP) الخاصة بكل شبكة، ومعرفة أرقام (IP) الخاصة بالمحولات (Routers) الموجودة في كل قسم.
- معرفة عناوين التطبيقات التي يستخدمها الموظفون.
- معرفة ما اذا كانت المعلومات موجودة في مقر الشركة أو في مكان آخر.
- محاولة الحصول على أسماء المستخدمين وكلمات المرور واستخدامها للدخول للشبكة.
- معرفة البريد الإلكتروني للموظفين والمجموعات الإخبارية والمنتديات التي يشاركون فيها ومواقع التواصل الاجتماعي الخاص بهم.
- معرفة أرقام هاتف الشركة وأقسامها، وهذه مهمة في حالة استخدام المخترق لحيل الهندسة الاجتماعية للحصول على بعض المعلومات التي تساعده على الاختراق.

ولا يوجد حد للمعلومات التي يريد المخترق الحصول عليها، ولا يوجد حد لكيفية الحصول عليها. ومن الطريف ذكره أن بعضاً من أنجح عمليات الاختراق تم الحصول على معلومات مهمة، ساعدت على تنفيذها عن طريق التنقيب في (النفايات) الخاصة بالشركة لتي ترمي فيها بعض الشركات بمعلومات حساسة دون أن تعلم.

ويمكن تقسيم عملية جمع المعلومات إلى قسمين:

١. جمع المعلومات دون الاتصال المباشر بالجهة الضحية، وهذه المعلومات يمكن أن يحصل عليها المخترق بواسطة البحث في محركات البحث عن الجهة التي يريد اختراقها. فمثلا، خبر منشور عن شراء تلك الشركة لترخيص من شركة مايكروسوفت، يعني أنها ستقوم باستخدام مزود الويب (IIS)، وأنه ستوجد بعض المزودات التي تستخدم نظام التشغيل ويندوز.



obeikandl.com

٢. جمع المعلومات بالاتصال المباشر بالجهة الضحية. ويتم ذلك عن طريق استخدام البرامج المذكورة سابقاً التي تسمح بتحديد الأجهزة والمنافذ المفتوحة فيها، والبرامج والثغرات الموجودة في تلك الأجهزة.

وهذه المرحلة هي أهم مرحلة في عملية الاختراق، وهي تحدد ما إذا كانت العملية ستتم أم لا. فمن دون جمع معلومات كافية، لن يستطيع المجرم تنفيذ فعلته. وبعد الانتهاء من هذه المرحلة، ينتقل المجرم إلى المرحلة التالية، وهي مرحلة الاختراق الفعلي.

## ٨-٢ مرحلة الاختراق الفعلي

وفي هذه المرحلة، يقوم المخترق باستخدام المعلومات التي حصل عليها في المرحلة الأولى للقيام بعملية الاختراق. حيث يوجد لديه كل ما يريد لتنفيذ الهجمة، فهو يعرف الأجهزة التي يريد مهاجمتها، ويعرف كذلك الثغرات الموجودة فيها وكيفية استغلالها.

وعلى العكس من مرحلة عملية جمع المعلومات التي يستطيع المخترق فيها أن يأخذ كل الوقت الذي يريده، فإن مرحلة الاختراق الفعلي، لابد أن تتم مباشرة بعد عملية جمع المعلومات والتخطيط للهجمة، وذلك لضمان فعالية المعلومات وضمان عدم قيام المشرفين على الشبكة بإصلاح أو سد الثغرات الموجودة فيها.

وبناءً على نوعية الهجمة فإن عملية الاختراق قد تمر دون ملاحظة. فمثلا عند قيام المخترق بهجمة على شبكة لسرقة معلومات مهمة منها، فإنه في الغالب يرغب أن لا يلاحظ أصحاب تلك الجهة هجمته، لأن ذلك في بعض الأحيان قد يلغي فائدة المعلومات التي تمت سرقتها. فمثلاً، عندما يعلم أحد البنوك بأن أرقام البطاقات الائتمانية قد سرقت فإنه سيقوم بإيقاف هذه الأرقام، بحيث تصبح تلك الأرقام التي حصل عليها المخترق عديمة الفائدة.

ولكن هناك هجمات أخرى يقصد منها أن تلاحظ الضحية تأثيرها، مثل هجمات تعطيل الخدمة (DoS) وهجمات تغيير محتوى الموقع، فالمخترق في هذه الحالة يرغب أن يلاحظ أصحاب الشبكة، وغيرهم تأثير هجمته. وغالبا ما يكون هناك دافع سياسي أو عقائدي لتلك الاختراقات. ويوفر موقع (http://www.zone-h.org) معلومات غزيرة عن المواقع التي يتم اختراقها والعبث بمحتواها.


شكل ٨-١ يوضح اختراق إحدى مجموعات الهاكر لشركة أسترالية متخصصة في أمن المعلومات !!

يتضح من الشكل ٨-١ اسم المخترق، واسم الدومين الذي تم عليه الاختراق، ووقت وتاريخ الاختراق. وعنوان الـ (IP) الخاص بالضحية.

في أحيان كثيرة، فإن هذه المرحلة قد تحتوي على مرحلة فرعية، وهي مرحلة توفير وصول دائم للجهاز المخترق. حيث إن بعض المخترقين بعد اختراق جهاز أو شبكة معينة، فإنه قد يرغب في البقاء في الظل أكبر وقت ممكن من دون أن تتم ملاحظته، وهو بذلك يجني الفوائد الآتية:

عدم معرفة أصحاب الأجهزة بوجود الاختراق يجعلهم يحسون بالأمان، وهذا يعني حصول الشخص على قدر أكبر من المعلومات.

المعلومات التي يحصل عليها الشخص من الجهاز المُخترَق هي أكثر حساسية من المعلومات التي حصل عليها في أثناء المرحلة الأولى. حيث إن الجهاز المُخترَق ينتمي للشبكة الخاصة بالشركة مما يعني أنه داخل نطاق المنطقة الموثوقة التابعة للجهة، وهذا يسمح له بالحصول على قدر أكبر من المعلومات.

يمكن للمخترق استخدام هذا الجهاز لبدء هجمات أخرى على أجهزة وشبكات مختلفة، وهو بذلك يلغي هويته. حيث إن أي محاولة لتتبع أثر الهجمة سيقود إلى هذا الجهاز الوسيط الذي سيعمل المخترق على إزالة آثاره منه.

ومن الطريف أن بعض المخترقين عندما يتمكنون من الدخول إلى جهاز معين واختراقه، فإنهم يقومون بتحصين ذلك الجهاز بحيث لا يستطيع المخترقون الآخرون الدخول عليه. ويوجد العديد من الطرق والبرامج التي تسمح للمخترقين بعمل ذلك، ومن ضمنها ما يسمى بـ (Rootkit) التي تسمح للمخترق بالسيطرة على الجهاز على مستوى نظام التشغيل نفسه، وليس على مستوى التطبيقات فحسب.

## ٨-٣ مرحلة مسح الآثار

وفي هذه المرحلة فإن المخترق يقوم بمسح جميع الآثار التي تدل على عملية الاختراق، وذلك لخدمة أهداف عديدة، أهمها:

حماية نفسه، بحيث لا يستطيع أحد الوصول له، وهو بذلك يقطع الخط على من يريد تتبعه.



openkanal.com

إشعار المشرفين على الجهاز المخترق بالأمان. حيث إنهم حتى لو قاموا بفحص الجهاز المخترق فلن يجدوا ما يثير المخاوف أو ما يشير إلى حدوث عملية الاختراق.

ويتمكن المخترق من مسح أثار الجريمة بطرق عديدة، أشهرها هو الآتي:

تعديل محتويات ملفات سجل العمليات الخاصة بالتطبيقات المختلفة، ومسح كل ما يتعلق به. حيث إن هذه الملفات في الغالب تعطي معلومات كافية للتعرف على المخترق.

تبديل بعض ملفات النظام بحيث لا تعرض أي معلومات خاصة بالمخترق، مثل برنامج (netstat) الذي يعرض أرقام الآيبي (IP) للأجهزة المتصلة بالجهاز حالياً. حيث يقوم المخترق بتبديل هذا البرنامج ببرنامج آخر يعرض جميع الاتصالات ماعدا جهاز المخترق.

وينبغي التوضيح بأن هذه المرحلة غير مطلوبة دائما. حيث يحتاجها المخترق عندما يقوم بالوصول المباشر للجهاز. فهي لا تنطبق على هجمات منع الخدمة مثلاً.

وينصح في نهاية هذا الفصل بعدم الانجراف خلف أي دعوات لتنظيم هجمات عدائية على مواقع المخالفين، وألا نكون صيداً رخيصا لأطراف تجهل ماهيتهم ونعلم أهدافهم. فقد ظهرت في فترة سابقة ما تسمى بحملات الجهاد الإلكتروني، وكان بعض الناس بنية طيبة يشارك في هذه الحملات بإنزال برامج على جهازه لشن الهجمات، وهذه البرامج تتجسس عليه ولا تحقق مراده. بل إن بعض البرامج التي انتشرت تلك الفترة كانت تشن هجمات (تعطيل) لمواقع عربية وإسلامية. لذا فالحماس والنية الطيبة لا تؤدي دائماً إلى خير، بل يجب التحقق من الأمور والوقائع وزيادة الوعي والتعامل مع القضايا والنوازل بحكمة وعقلانية.



obeikandi.com

# الفصل التاسع :
# الشبكات الاجتماعية والسرية المفقودة

obeikandl.com

انتشرت ظاهرة الشبكات الاجتماعية هذه الأيام بكثرة حتى غدت أهم المواقع على الإطلاق، وأكثرها مشتركين ومهتمين، والمعلوم أن هذه المواقع تسمح لأعضائها بإنشاء ملف شخصي، ومن ثم مشاركته مع أعضاء آخرين داخل الموقع، مما يشكل شبكة كبيرة من المعارف والأعضاء، ويوفر كمية هائلة من المعلومات المجانية على شبكة الإنترنت المفتوحة أمام الجميع.

وقد بدأت مواقع الشبكات الاجتماعية تقريبا عام ١٩٧٧م، من خلال موقع (SixDegrees.com)، تلا ذلك موقع (Friendster) عام٢٠٠٢ م، ثم موقع (My Space) الشهير عام ٢٠٠٣م، وجاء أشهر مواقع الشبكات الاجتماعية وأهمها (Facebook) عام ٢٠٠٤م، ثم تلاه موقع (Twitter) عام ٢٠٠٦م.

وسيتم الحديث هنا بشيء من التحليل لأشهر هذه الشبكات الاجتماعية وأكثرها انتشاراً، وهي شبكتي (Facebook) و (Twitter).



openkanal.com


## ٩-١ شبكة (Facebook)

تظهر الأرقام التي يرصدها موقع الشبكة مبلغ الإقبال العظيم عليها؛ إذ يوجد فيها أكثر من ٨٠٠ مليون مستخدم نشط، وأكثر من ٥٠٪ من المستخدمين النشطين يقوم بتسجيل الدخول إلى (فيس بوك) على الأقل مرة واحدة كل يوم. وأما نشاطات المشتركين وصداقاتهم عبر الشبكة، فتظهر في المتوسط أن كل مستخدم لديه ١٣٠ صديقاً على الموقع، فيما يقضي مرتادو الموقع أكثر من ٨ مليارات دقيقة على الموقع كل يوم (على مستوى العالم)، وتظهر البيانات أن هناك أكثر من ٤٥ مليون مستخدم يقوم بتحديث بيانات على الأقل مرة واحدة كل يوم.

وأما التطبيقات، فهناك أكثر من ملياري صورة يتم تحميلها إلى الموقع شهرياً، وأكثر من ١٤ مليون ملف فيديو يتم رفعها كل شهر، كما يتم إدراج ملياري جزء من المحتوى (وصلات على شبكة الإنترنت، وأخبار، وإعلان وظائف...إلخ) كل أسبوع، فضلاً عن أنه يتم إنشاء أكثر من ٣ ملايين حدث كل شهر.

ويبلغ مدى انتشار الشبكة عالمياً أرجاء المعمورة، فأكثر من ٧٠ ٪ من مستخدمي الفيس بوك هم خارج الولايات المتحدة، ويزود الموقع رواده العالميين بأكثر من ٧٠ ترجمة متاحة عليه.

## ٩-٢ المخاطر الأمنية في شبكة (Facebook)

أول المشاكل الأمنية في فيس بوك ظهرت في بداية ٢٠٠٧م، وتعاطف معها الكثير ، وبدأ الشك ينشأ بين المستخدمين. إذ وقعت هذه الحالة في ولاية أيلينوي (الولايات المتحدة) ، عندما تنكر رجل على أنه طفل في سن المراهقة لجذب الأطفال وتبادل الصور معهم ومحاولة استدراجهم. واعتقل الرجل ومن بعدها بدأت ووسائل الإعلام والجمعيات في انتقاد سجل الفيس بوك فى حماية الأطفال.

وظهرت الدعوات المطالبة بحماية الأطفال من الاستغلال الجنسي، مما دعا شركات التقنية إلى تقديم حلول إلى أولياء الأمور مثل نظام سوشيل شيلد (SocialShield)، وهو يقدم وظائف أمنية متقدمة وخاصة جداً بالمخاطر على الشبكات الاجتماعية مثل (CyberBullying Promise) الذي يعرّفهم بمفهوم استغلال الأطفال ومضايقتهم على الويب، وطرق حدوثه وتحديداً على الشبكات الاجتماعية. ويعدّ هذا التطبيق -حالياً- من أفضل الخيارات الأمنية المتوافرة أمامهم. لأنه يقدم خصائص حماية متقدمة تمنحهم رؤية شاملة عما يقوم به الأطفال من أنشطة وزيارات على شبكة الإنترنت كما يعطي أولياء الأمور فكرة جيدة عن ماهية أصدقائهم على الشبكة العنكبوتية. ويوجد أيضا تطبيق آخر يسمى (Friend verification technology) ويتحرى عن أصدقاء الطفل على شبكتي Facebook وMySpace ، ويقوم بالاستقصاء عنهم من خلال أكثر من ٥٠ قاعدة بيانات على الإنترنت حتى يؤكد لأولياء الأمور إذا ما كان عليهم القلق من أصدقاء أولادهم على الشبكات الاجتماعية، كما يتم إعلام أولياء الأمور بالسلوكيات



obeikandl.com

الخطيرة التي قد تسبب ضرراً دائماً لأولادهم على غرار وضع صور أو محتوى خاص غير لائق.

وكذلك يوجد نظام (Alerts Engine) الذي يقوم بالبحث عن جميع الحسابات التي يمتلكها أي طفل، بما فيها تلك الحسابات التي يجهل أمرها أولياء الأمور ويقوم بالتحري عن جميع المعلومات وحتى المشاركات. وظهرت أيضا مشكلة أمنية ترجع إلى عيوب في برمجة الموقع، كانت نتيجتها أنه عندما يقوم المستخدم بإدخال كلمة المرور الخاصة به، يتم إعادة توجيه إلى علبة بريد مستخدم آخر، وكثير من المشتركين تعرضت معلوماتهم السرية للانتهاك من للآخرين.


وخلاصة القول أن الفيس بوك قد تعرض للكثير من الانتقادات في مناسبات عدة بسبب المشاكل الأمنية، لاسيما تلك المتعلقة بتسهيل إتاحة أعداد ضخمة من الفضائح الجنسية، وكثير ما يتبين أن هذه الفضائح تكون مزورة، فضلاً عن عدم التمكن من معرفة مصدر نشر هذه الفضائح . وزد على ذلك المشاكل المتعلقة بإدارة البيانات الحساسة والشخصية لمرتادي الموقع، فالكثير من الحوادث تؤكد حصول أنظمة استخباراتية على معلومات أشخاص

من على الموقع دون رغبتهم أو علمهم بذلك، وهو ما تنفيه بشدة إدارة الموقع بالطبع! ووفقا لإحصائية قامت بها شركة سوفوس (Sophos) المتخصصة فى أمن المعلومات فى ديسمبر ٢٠٠٩م، تقول الإحصائية إن ٦٠ ٪ من المشاركين في المسح الذي أجرته الشركة يعتقدون أن الفيس بوك هو أكبر مواقع الشبكات الاجتماعية تعرضا لثغرات أمنية، متقدما بشكل كبير على (Twitter، MySpace، LinkedIn).

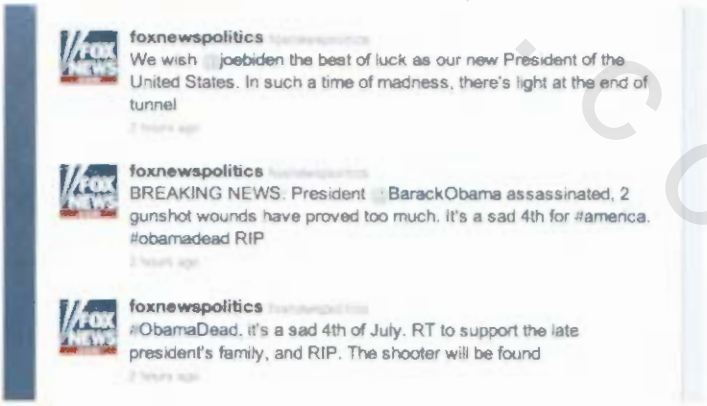
## ٩-٣ المخاطر الأمنية في شبكة (Twitter)


نبّه كثير من الخبراء أن فضاء الإنترنت رغم اتساعه، إلا أنه يسهل تتبع نشاطات أي شخص، ولاسيما إذا كانت هناك رغبة في اقتفاء أثر فرد بعينه! وجاء في جريدة الرياض في عددها ١٢/١/ ٢٠١٢ :من ظهور تقرير (مراجعة الالتزام بالخصوصية) الذي أصدرته وزارة الأمن الداخلي الأمريكية في نوفمبر عام ٢٠١١ ، والذي يوضح أنه منذ يونيو ٢٠١٠ على الأقل ومركز العمليات التابع للوزارة يقوم بعمليات متابعة لمواقع التواصل الاجتماعي ومواقع

الإنترنت التي تتضمن الاطلاع المنتظم على (منتديات الإنترنت المتاحة للعامة، والمدونات، ومواقع الانترنت العامة). وكذلك أظهرت وثيقة حكومية أمريكية أن مركز القيادة في وزارة الأمن الداخلي يتابع بشكل منتظم عشرات مواقع الإنترنت التي تلقى رواجا، مثل: فيسبوك، وتويتر، وويكيليكس، ومدونات ومنتديات على الإنترنت.

وكما هو معروف يعد موقع تويتر عملاق منصات التدوين المصغر على الإنترنت، والذي يسمح لمستخدميه بإرسال تغريدات (Tweets) عن حالتهم بحد أقصى ١٤٠ حرف للرسالة الواحدة. وذلك مباشرة عن طريق موقع تويتر، أو عن طريق إرسال رسالة نصية قصيرة SMS أو برامج المحادثة الفورية أو التطبيقات التي يقدمها المطورون، مثل: (TwitBird، twitterfox ، Twhirl ، Twitterrific).

ولم يسلم الموقع بين آونة وأخرى من حادثة تثير الاهتمام بموضوع الخصوصية والأمان لهذا الموقع العملاق. ومنها على سبيل المثال، تمكن هاكرز مجهولي الهوية من قرصنة حساب شركة باي بال (paypal) للدفع الإلكتروني على موقع توتير (Twitter)، ونشروا رسائل تنتقد شركة باي بال (paypal)،وكذلك اختراقهم موقع شبكة فوكس نيوز الإخبارية، ونشرهم خبراً عن مقتل الرئيس الأمريكي باراك أوباما، كما يظهر في الشكل الآتي.




الشكل ٩-١ : الخبر المزور على موقع شبكة فوكس نيوز الإخبارية على توتير



obeikandi.com

**ويقول الخبراء:** إن موقع تويتر يفتقد إلى بعض المعايير الأمنية المهمة، أهمها عدم وجود معيار ثنائي للتوثيق مقارنة بفيسبوك أو جوجل، وهو ما ينصح بأتباعه على موقع تويتر.

وحرصاً من شركة تويتر على الانتشار الآمن، فقد نشرت وكالة (أنباء الشرق الأوسط) مطلع شهر يناير ٢٠١٢ ، أن شركة (تويتر) قد أطلقت برنامج أمني على منصة (أندرويد) يسمى (تيكست سيكيور)، الذي استحوذت عليه في شهر ديسمبر ٢٠١١، وفق رخصة المصادر المفتوحة، لتتيحه مجاناً للمستخدمين للاستخدام والمشاركة والتطوير. ويقوم هذا البرنامج بتشفير الرسائل النصية قبل إرسالها للمنصة الاجتماعية، من خلال إضافة طبقة أمنية عليها. وتشير تلك الخطوة إلى توجه (تويتر) الجديد نحو التوسع كصانع للبرمجيات يتمتع بنفوذ في العديد من الأسواق الرقمية.

obeikandl.com

الفصل العاشر :

# متطلبات الحماية للأجهزة الشخصية

obeikandi.com

لما تزل الإحصاءات تظهر الخطر الكبير الذي يتهدد المستخدمين لشبكة الإنترنت، سواء على صعيد الأفراد أو المؤسسات، أو الجهات الحكومية وغيرها، ففي إحدى الإحصائيات التي أجرتها وكالة التحقيقات الفيدرالية الأمريكية (FBI) فإن ٥٧٪ من المشاركين في تلك الإحصائية أوضحوا تعرضهم لمحاولة اختراق في أثناء اتصالهم بالإنترنت. وفي إحصائية أخرى أجرتها الوكالة أيضاً بالتعاون مع معهد أمن الحاسبات (CSI) فإن ٩٠٪ من المشاركين في هذه الإحصائية أثبتوا تعرضهم للاختراق.

فيما كشفت أحدث التقارير الذي طرحتها شركة مكافي في مطلع عام ٢٠٠٩م، أن مجرمي الإنترنت غالبًا سيستغلون الأزمة المالية العالمية المتفاقمة بنظام وبراعة أكبر في عام ٢٠٠٩، مما يشكل تهديدًا على جميع المستخدمين. فقد شكلت سنة ٢٠٠٨م، فترة لم يسبق لها مثيل للتهديدات والمخاطر، وتوقعت الشركة المزيد من تلك البرامج في ٢٠٠٩م، أكثر بكثير من السنة الماضية. إذ شهد العام المنصرم المزيد من البرامج الضارة أكثر من أي وقت مضى. فخلال فترة ١٥ عاما الماضية حتى نهاية عام ٢٠٠٧م، تلقت مختبرات مكافي حوالي (٣٥٨٠٠٠) من البرمجيات الخبيثة، في حين أن أكثر من (١٣٥٠٠٠) من تلك البرمجيات الخبيثة المحددة كانت في العام ٢٠٠٧ وحده. وبحلول مارس ٢٠٠٨ زادت البرامج الضارة التي تم تحديدها عن كل ما ظهر عام ٢٠٠٧. وفي عام ٢٠٠٨ ، تلقت مختبرات مكافي تقريبا (١,٥) مليون من البرمجيات الخبيثة ، أي بمعدل (٣٥٠٠) كل يوم.

ومن المفيد معرفة بعض الإحصاءات حول أفكار مستخدمي الإنترنت وطبيعة تصرفهم حيال الأخطار المحتملة، ففي تقرير لمجلة أمن المعلومات ٢٠٠٧م، ذُكر أن حوالي ٦٠ ٪ من الناسِ الذي طُلِبَ منهم كلمة السر الخاصة بالدخول على شركاتهم بشكل مهذب! قاموا بإعطائها لمن طلبها منهم.

ولعل حادثة السيدة السعودية التي وقعت في الشهر العاشر من عام ٢٠١١م، تدلل على سهولة الحصول على كلمة السر بهم، إذ اتصل بها أحد الأشخاص مدعياً أنه موظف المصرف المودع حسابها لديه، وطالباً منها تحديث بياناتها، بعد أن تصل إليها رسالة جوال تظهر بعض المعلومات الخاصة بها، وبعد أن رأت تلك المعلومات وفي أعلى الرسالة النصية اسم المصرف، قامت بإعطاء كلمة السر للمتصل، وما هي إلا ساعات قليلة حتى سحب المحتال رصيدها البالغ (١٠٠) ألف ريال على دفعتين، وأودعه في حساب شركة وهمية في نفس المصرف.

ولهذا أيضاً تبين الأرقام عدم ثقة الكثيرين بالتعاملات المالية عبر الإنترنت، إذ يعتقد ٥٨٪ من المستخدمين أن التعاملات المالية على الإنترنت غير آمنة. ولعل اقتناع العديد من المستخدمين بأن بياناتهم الخاصة عرضة للبيع والشراء يجعلهم يترددون في استخدم الشبكة، وقد أظهرت دراسة نسبة فقدان سرية المعلومات للجمهور، حيث ظهر أن ٣٥٪ من المواقع التجارية تقوم بتقديم معلومات الزبائن الخاصة لشركات الإعلان لكي تقوم بعرض الإعلانات المناسبة لهم.

فيما بينت إحصائية أخرى أجريت على الأطفال المتصلين بالإنترنت أن عددهم سيصل إلى (٧٧) مليون طفل في الولايات المتحدة الأمريكية، وأن ١٨٪ منهم قرروا مقابلة أشخاص في الحياة الواقعية، بعد أن تعرفوا عليهم مبدئيا عن طريق الإنترنت.

ومن تلك البيانات والإحصائيات يمكن الحديث عن البرامج والاحتياطات اللازمة للمستخدم الفردي لحماية نفسه عند ارتباطه بالإنترنت. وهذه المتطلبات تتباين من حيث أهميتها وضرورة وجودها. فبعضها مهم جداً، ومن المفترض إن لم يكن من الضرورة استعمالها. أما بعضها الآخر، فهو من باب الاحتياط الزائد ويحبّذ استخدامها لمن لديه معلومات حساسة في جهازه، مما يجعل من الضروري توفير أقصى قدر من الحماية.

## ١٠-١ برامج الحماية من الفيروسات (Anti-Virus)

وتعدّ هذه البرامج من أهم برامج الحماية، فلا يستغني عنها أي شخص مهما كانت خبرته في مجال الحاسب ، وذلك لأنه لا يوجد طريقة لأي شخص لتمييز الملفات التي تحتوي على الفيروسات ما لم يكن لديه برنامج فاحص الفيروسات (هناك بعض الاستثناءات ولكن لن يجري ذكرها هنا).

وقد تطورت برامج الحماية من الفيروسات في الآونة الأخيرة لتقوم بالتعرف على أنواع الفيروسات المختلفة، سواء كانت:

- فيروسات مدمجة في ملفات تنفيذية.
- فيروسات من نوعية الماكرو (Macro) التي تدمج في برامج الأوفيس غالباً.
- برامج التروجان (حصان طروادة)، وإن كانت برامج التروجان لا تُصنّف كفيروسات، إلا إن برامج الحماية من الفيروسات تقوم باكتشافها أيضاً.

ونظرا لكثرة طرق انتشار الفيروسات في الآونة الأخيرة، فإن برامج الحماية من الفيروسات كان لابد أن تتطور بشكل كبير لكي تقوم بحماية المستخدم. ومن ذلك التطور أن برامج الحماية من الفيروسات تأتي بخيار يسمح لها بالعمل بشكل خفي في الخلفية، بحيث تقوم بفحص أي ملف يتم وضعه على القرص الصلب أو ذاكرة الفلاش مباشرة من دون الحاجة لتدخل المستخدم. وهذه الخاصية تحمي جهاز المستخدم من أن يصاب بالفيروس في حالة نسيان المستخدم أن يقوم بفحص الملف الذي سحبه من الإنترنت قبل تشغيله.

كما أن هذه البرامج تقوم بفحص الملفات الملحقة بالبريد الإلكتروني في أثناء سحب الرسالة، وبذلك يحمي المستخدم من الإصابة بالفيروسات التي تنتقل في البريد الإلكتروني التي في



obeikandl.com

الغالب تأتي، وكأنها مرسلة من أحد الأصدقاء مما يجعل المستخدم يثق بها ويقوم بفتحها.

ويمتد مستوى الحماية في هذه البرامج لتقوم بحماية المستخدم من الفيروسات التي تنتقل عبر برامج المراسلة اللحظية مثل: (Instant Messaging)، و(MSN Messenger)، و(Yahoo Messenger)، و(AOL Messenger).

ولعل أهم ميزة في برامج الحماية من الفيروسات هو قيامها بالتحديث الذاتي، بحيث تقوم بحماية جهاز المستخدم من أحدث الفيروسات ظهوراً. وغني عن الذكر بأن برنامج الحماية من الفيروسات إذا لم يتم تحديثه فإنها لن تكون ذات فعالية وموثوقية.

ومن أشهر برامج الحماية من الفيروسات ما تقدمه شركتي سيمانتك (www.symantec.com)، وشركة مكافي (www.mcafee.com) ، وشركة كاسبر سكاي...إلخ، ويمكن للمستخدم الحصول على نسخة تجريبية من هذين الموقعين وتجربتها ومن ثم شراؤها منهم. كما أن أغلب الأجهزة الحديثة تأتي مدعمة بهذه البرامج عند شراء الجهاز.


شكل ١٠-١: قسم التحكم في برنامج Norton AntiVirus ويظهر فيه خاصية مسح الملفات السريع في أثناء عمله.

## ١٠-٢ برامج جدر الحماية الشخصية

هذه النوعية من البرامج تقوم بتركيب نفسها كطبقة وسيطة بين الشبكة وبين نظام التشغيل، بحيث تكون على علم بأي اتصال شبكي يكون صادراً أو وارداً إلى جهاز المستخدم، وتقوم بإخبار المستخدم بماهية هذه الاتصالات والبرامج التي تقوم بها، لكي يقرر المستخدم بعد ذلك فيما كان يرغب بالسماح بذلك أم لا.

تقوم هذه البرامج بحماية المستخدم على ثلاثة أوجه:

حماية خصوصيته، حيث إنها تخبر المستخدم في حين محاولة أحد البرامج القيام بإرسال معلومات من جهاز المستخدم إلى الشبكة. ومن هنا يتمكن المستخدم من معرفة هذه البرامج ومنعها في حالة كونها برامج دعائية أو تجسسية. ولقد عانت شركة ريال (RealPlayer) من دعوى قضائية رفعت عليها لكونها تتبع اختيارات المستخدمين وتحاول معرفة المقاطع الصوتية التي يستمع لها المستخدمون بكثرة، وهذا فيه اختراق لخصوصية المستخدمين. ولقد تم اكتشاف المعلومات التي يرسلها برنامج ريال بلاير بواسطة أحد برامج جدر الحماية الشخصية.

حماية ملفات المستخدم، حيث إن معظم المستخدمين يتجاهلون إلغاء خاصية مشاركة الملفات في أجهزتهم، أو قد يقومون بفتح مشاركة الملفات دون علم منهم، مما قد يفتح الباب على مصراعيه لمن أراد الحصول على هذه الملفات. وتقوم برامج جدر الحماية الشخصية بتحذير المستخدم وتعطيل خاصية مشاركة الملفات، لمن هم في خارج نطاق الشبكة المحلية الموثوقة.

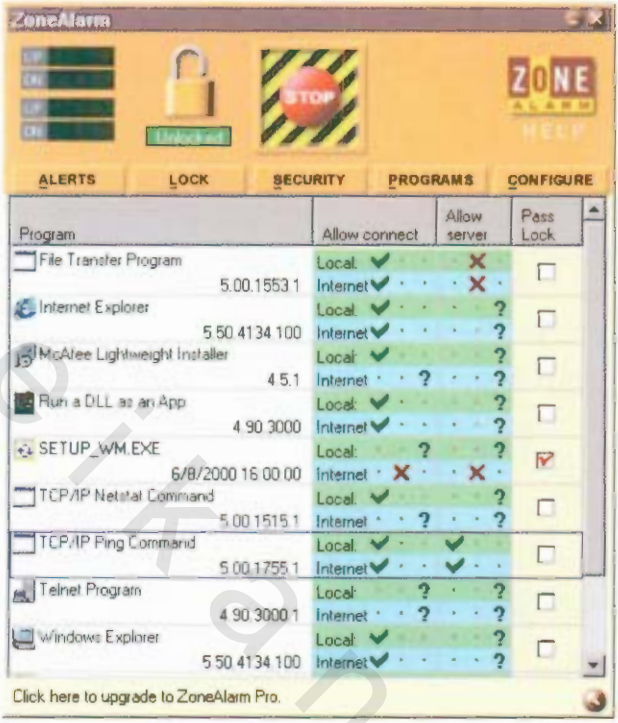
حماية المستخدم من برامج التروجان، أو من الثغرات الموجودة في أنظمة التشغيل التي تعمل عن طريق الشبكة. حيث إنه لو لم يقم برنامج الحماية من الفيروسات باكتشاف ملف التروجان، فإن برنامج جدار الحماية سيقوم باكتشاف محاولة التروجان فتح منفذ على جهاز المستخدم وإخباره بذلك. ويجب عليه في تلك الحالة ألا يقوم بالسماح لها. وهناك أيضاً ثغرات

في أنظمة التشغيل لا يمكن تصنيفها على أنها فيروسات، ولكنها ثغرات تسمح لأي شخص باختراق جهاز المستخدم عن طريق تكوين اتصال على منفذ معين (Port) في جهاز المستخدم. وهذه النوعية من الثغرات لا يمكن لبرامج الحماية من الفيروسات اكتشافها على الإطلاق، ولكن برامج جدر الحماية الشخصية تكتشفها وتخبر المستخدم بذلك.

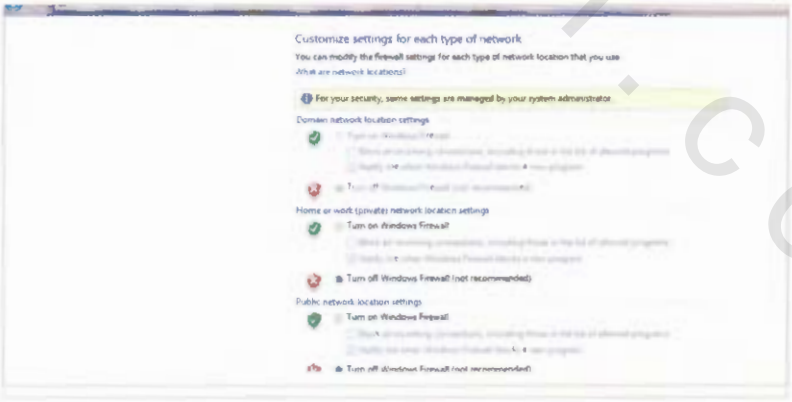
أشهر برامج الحماية من هذه النوعية هو برنامج زون الآرم (ZoneAlarm) الذي ظهر بقوة منذ بدايته ولازال يحتل صدارة البرامج من هذه النوعية. ويتميز هذا البرنامج بسهولة استخدامه وإعداده لضمان سلامة الجهاز. والجدير بالذكر أن هذا المنتج يتبع لشركة (CheckPoint) الإسرائيلية وأغلب أنظمة هذه الشركة تأتي على شكل منتج متكامل (Internet Security suite).

كما أنه من الجدير بالذكر أن أنظمة مايكروسوفت للتشغيل (ويندوز٧، وفيستا، xp) لديها خاصية جدار الحماية، وتسمى ICF) Internet Connection Firewall ) من دون الحاجة لوجود برنامج إضافي، وإن كانت هذه الخاصية في نظام ويندوز أقل مرونة منها في برنامج زون الآرم، إلا أنها تفي بالغرض لمن لا يريد تركيب برامج إضافية.

obeikandl.com




شكل ١٠-٢: برنامج زون الآرم




شكل ١٠-٣: تمكين خاصية جدار الحماية في نظام ويندوز ٧

## ١٠-٣ برامج التشفير

تقوم برامج التشفير أو التعمية بتحويل النصوص المقروءة إلى نصوص غير مقروءة إلا لمن لديه المفتاح الخاص بفك التشفير، ولكثرة اختراق الأجهزة والحواسيب الشخصية في هذا الوقت، فإنه من المفيد تشفير بعض المجلدات على القرص الصلب، فيوضع عليه ما هو حساس من معلومات أو صور خاصة ضمن هذه المجلدات، وبذلك لا يستطيع المخترق من اختراق الجهاز وسرقة هذه الملفات.

كما أنه يمكن استخدام تقنية التشفير للحفاظ على سرية البريد الإلكتروني المتبادل، حيث إنه من المعروف أن البريد الإلكتروني عند انتقاله في الإنترنت معرض لأن تتم قراءته من قبل أشخاص آخرين غير المرسل والمستقبل. لذلك تم إيجاد تقنية (Public Key Cryptography) التي تمكن كل مستخدم من الحصول على وثيقة إلكترونية يكون الهدف منها تمييز الشخص بنفس الطريقة التي تميزه بها بطاقة الأحوال المدنية في الحياة الواقعية. وتحتوي هذه الوثيقة على مفتاح عام يسمح لكل من يريد إرسال رسالة لذلك الشخص أن يقوم بتشفيرها باستخدام ذلك المفتاح. وبعد تشفير الرسالة فإنه لن يتمكن أحد من قراءتها غير الشخص المستقبل، وذلك لأن فك تشفير الرسالة يتم بواسطة المفتاح الخاص (Private Key) الذي لا يمتلكه أي شخص آخر غير صاحب الوثيقة الإلكترونية.

بالنسبة لتشفير الملفات، فيوجد الكثير من البرامج التي تقوم بذلك، ويمكن الحصول عليها من مواقع الإنترنت المختلفة، كذلك أيضا فهذه الخاصية أيضا موجودة في نظام (ويندوز٧، وفيستا، و XP) الذي يمكن الشخص من تشفير ملفاته في القرص الصلب.

أما بالنسبة لتشفير البريد الإلكتروني، فمعظم برامج قراءة البريد تدعم ذلك، وكل ما يلزم الشخص هو الحصول على وثيقة إلكترونية خاصة به عن طريق أحد المواقع المشهورة، مثل: (ViriSign أو Thawte) أو غيرها من الشركات الأخرى.



obeikandi.com


شكل ١٠-٤: خاصية تشفير المجلدات في ويندوز ٧

## ١٠-٤ الحماية من الشبكات اللا سلكية (WiFi)

أعطى التقدم المستمر في تقنية الشبكات المستخدم العادي حدا عاليا من الرفاهية جعله يعتاد على وجود الإنترنت في كل زمان ومكان. فالشبكات اللاسلكية متوفرة في أغلب الأماكن الآن من جامعات وأماكن عمل ومقاهي ومطارات وغيرها. ولكن هذه الزيادة في الرفاهية لا تخلو من الشوائب التي تعكر صفوها. فاعتياد الناس على توفر الإنترنت أعطى فرصة كبيرة للمخترقين للتعدي على خصوصياتهم !

فمن أحد أشهر طرق الاختراق ما يسمى، برجل المنتصف (Man in the middle) والتي يقوم فيها المخترق باستلام البيانات منك، دون علمك، وتمريرها للطرف الآخر، دون علم أي منكما عن وجوده. وسبب خطورة هذه الطريقة هي صعوبة اكتشافها (وأحيانا استحالة اكتشافها !) بحيث يحصل المخترق على جميع البيانات التي أرسلتها أو استقبلتها مثل كلمات السر، والبريد الإلكتروني، و التعاملات الإلكترونية أو غيرها. وانتشرت هذه الطريقة للاختراق مؤخرا، حيث يقوم المخترق بتكوين شبكة لاسلكية وهمية، ويقوم بإعطائها أسماء وهمية ومغرية، مثل، إنترنت مجانية (FreeInternet). بحيث يغري المستخدم العادي بالاتصال بها واستخدامها للوصول للإنترنت. ويقوم المخترق في هذه الحالة بتمرير البيانات عن طريق الشبكة التي قام بإنشائها، مطبقا طريقة (رجل المنتصف) دون علم المستخدم! بالطبع فهناك أكثر من طريقة للقيام بذلك، حيث يمكن للمخترق أن يقوم بذلك عن طريق كرت الشبكة اللاسلكي في جهازه أو ما يسمى بـ (Ad hoc network) أو بإحضار جهاز نقطة اتصال لا سلكية وتكوينها بالشكل الذي يريد. ومن الممكن تجنب الطريقة الأولى بشكل بسيط وذلك بمنع جهازك من الاتصال بأي شبكة من نوع Ad hoc network. أما الطريقة الثانية فهي صعبة الاكتشاف، حيث يصعب تمييز شبكة المخترق من غيرها! لا سيما



obeikandl.com

بأن المخترقين يقومون باختيار أسماء تبدو مشابهة، أو مطابقة، للشبكات الأصلية المقدمة من قبل المقهى أو المطار. ولتجنب ذلك يجب على المستخدم أن يقوم بالاستفسار من صاحب المكان عن اسم الشبكة وإعداداتها، حتى يتمكن من الاتصال بالشبكة الصحيحة. أيضا فيجب على مقدمي هذه الخدمة من وضع إعدادات تشفير للشبكة من أجل حماية المستخدمين بعضهم من بعض وأيضا ليحتاج لها المستخدم ويقوم بالسؤال عنها، ومن ثم يتم تعويد المستخدم على عدم الاتصال بأي شبكة ما لم تكن الشبكة الصحيحة.

## ١٠-٥ الحماية من المواقع غير الأخلاقية

الهدف من الحماية من المواقع غير الأخلاقية هو حماية المستخدمين صغار السن، من المخاطر التي تحتويها الإنترنت لهم (سبق الحديث عن ذلك في الفصل الثاني) فهؤلاء يحتاجون نوعية خاصة من البرامج توفر لهم الحماية على المستوى الأخلاقي. حيث توجد الكثير من البرامج في الإنترنت التي تسمح لولي أمر الطفل بالتحكم في دخول الطفل للإنترنت، وتحديد نوعية المواقع التي يستطيع أو لا يستطيع الدخول عليها. وتسمى هذه النوعية من البرامج بالتحكم الأبوي، وكذلك تساعد هذه البرامج الأبوين على تحديد تطبيقات الإنترنت التي يسمح للطفل باستخدامها، مثل المحادثة أو سحب البريد أو سحب الملفات أو غيرها من التطبيقات الأخرى.

هذه البرامج منتشرة بشكل كبير في الإنترنت، ومن أمثلتها برنامج (Cyber Patrol) وبرنامج (Cyber Nanny) وغيرها. ولكن هذه البرامج في الغالب تكون متبعة لتقاليد البلد المنتجة لها، التي تختلف بشكل كبير عن تقاليد مجتمعاتنا الإسلامية والعربية، لذا فقد كانت هناك عدة محاولات لإيجاد حلول لهذا النوع من المشاكل، ولعل من أبرزها خدمة الشبكة الخضراء التي تؤمن حماية المحتوى وتتفادى الدخول للمواقع ذات المحتوى غير اللائق أو الداعي إلى تفشي الرذيلة أو التطرف والغلو. كما يتم تقديم خدمة الشبكة الخضراء حاليا عن طريق



openkandil.com

خدمة (نقاء) التي تقدمها شركة الاتصالات السعودية مع اشتراكات الإنترنت ذات النطاق العريض (DSL).

## ١٠-٦ أخطاء شائعة

يوجد العديد من الأخطاء الشائعة التي يقع فيها الكثير من المستخدمين، إما لعدم علمهم أو لتساهلهم. وهذه الأخطاء، وإن تكن بسيطة فقد تتسبب في اختراق أجهزتهم وضياع بياناتهم المهمة.

ويتطرق هذا القسم لبعض هذه الأخطاء وبيان كيفية تلافيها.

### ١٠-٦-١ كلمة السر الواضحة أو القصيرة

عند تكوين حساب بريد إلكتروني أو عند إعداد الملف الشخصي في أحد المواقع على الإنترنت، فإن بعض الأشخاص يقومون باختيار كلمة سر بسيطة قد تكون اسم مدينة، أو اسم شخص أو أي كلمة أخرى توجد في القاموس. وبعضهم الآخر يقوم باختيار أقصر كلمة سر ممكنة، أو جعل كلمة السر هي نفس اسم المستخدم بزيادة رقم أو عدة أرقام.

بالطبع فهذا فيه ميزة وهي أن كلمة السر يمكن تذكرها بسهولة من قبل صاحبها، ولكن العيب يكمن في سهولة اختراقها لمن أراد ذلك.

**إن برامج كسر كلمة السر تعمل في الغالب بطريقتين:**

**القاموس:** وذلك يعني أن هذه البرامج تتضمن ملفاً يحتوي على عدد كبير من الكلمات، وهذا الملف يسمى القاموس، وقد تكون هذه الكلمات هي كلمات إنجليزية أو عربية معروفة، أو قد



obeikandl.com

تكون أسماء أشخاص أو مدن أو غيرها من الكلمات الشائعة. ويقوم البرنامج بتجربتها واحدة تلو الأخرى، حتى يتمكن من كسر كلمة السر. بالطبع فإن الحظ يلعب دوراً كبيراً في الوقت الذي يستغرقه البرنامج للوصول لكلمة السر.

تجربة جميع الاحتمالات، وهو ما يعرف بالتخمين الاستنزافي (Brute Force)، حيث يقوم البرنامج بتجربة جميع الكلمات من حرف واحد، ومن ثم من حرفين، ومن ثم من ثلاثة حروف، مرورا بجميع الحروف. بالطبع فإن هذه البرامج ستأخذ وقتا أطول للتنفيذ من القاموس. حيث إن القاموس يحتوي على كلمات لها معنى، أما هذه الطريقة فتقوم بتجربة كل شيء، سواء كانت الكلمة لها معنى أو لم يكن لها معنى على الإطلاق، وهذا ما يجعل هذه النوعية أشمل من نوعية القاموس، ولكنها في الجانب المقابل أبطأ بكثير.

لذا فإن اختيار المستخدم لكلمة سر بديهية، مثل اسم، أو كلمة إنجليزية معروفة سيزيد من احتمالية اكتشافها من قبل طريقة القاموس. أما كلمة السر القصيرة، فلن تحتاج لوقت طويل لاكتشافها.

الحل هنا هو اختيار كلمة سر طويلة وتتكون من حروف صغيرة وكبيرة، ويكون معها أرقام أو رموز خاصة. في الغالب فإن كلمة السر التي تحتوى على أكثر من ثمانية حروف، وليست من ضمن القاموس وبها رقم أو رمز، تكون آمنة.

### ١٠-٦-٢ عدم تغيير كلمة السر بشكل دوري

يعتقد بعض المستخدمين أن اختيار كلمة السر يتم مرّة واحدة فقط، وهذا اعتقاد خاطئ. فكلمة السر يجب تغييرها بشكل دوري. حيث إن بعض المخترقين يتمكنون بشكل أو بآخر من الحصول على كلمة السر الخاصة بالمستخدم، ومن ثم يقومون بقراءة بريده الإلكتروني دون أن يعلم. أي أنهم لا يقومون بإيذاء المستخدم أو مسح بريده، بل يقومون بالتجسس عليه بشكل خفي. وهذا أخطر أنواع الاختراق، وهو أن يكون الشخص أو الجهة مخترقاً من دون أن يعلم. فعند إبقاء كلمة السر دون تغيير، فإن ذلك يعني استمرار المخترق في الحصول على معلومات المستخدم. أما عندما يقوم المستخدم بتغيير كلمة السر بشكل دوري، فإن ذلك يعني أن المخترق سيضطر لمحاولة الحصول عليها مرة أخرى، وقد لا ينجح في ذلك.

السبب الآخر لضرورة تغيير كلمة السر هو أن برامج كسر الحماية من نوع (التخمين الاستنزافي) التي تقوم بتجربة جميع الاحتمالات ستصل إلى كلمة السر لا محالة. صحيحٌ أنها ستستغرق وقتاً طويلاً، ولكنها في النهاية ستصل لكلمة السر. هذا بافتراض أن المستخدم لا يقوم بتغيير كلمة السر الخاصة به. ولكن في حالة تغيير المستخدم لكلمة السر بشكل دوري، فإن ذلك يلغي فاعلية برامج تخمين كلمة السر.

### ١٠-٦-٣ استخدام كلمة سر واحدة لجميع المواقع

بعض المستخدمين يقومون باستخدام كلمة سر واحدة لجميع المواقع التي يزورونها، وهذا خطر جداً. وكما قيل «لا تضع بيضك كله في سلة واحدة». فالذي يحصل على كلمة السر الخاصة بالمستخدم لموقع واحد يستطيع التحكم في حساب المستخدم في جميع المواقع التي اشترك بها.



obeikandi.com

كما أن بعض أصحاب المواقع يقومون بتكوين مواقع وهمية وإلزام المستخدمين بالاشتراك فيها. وبعد أن يقوم المستخدم بالاشتراك في الموقع، يقوم صاحب الموقع بمحاولة الدخول على بريد المستخدم واستخدام كلمة السر التي أدخلها المستخدم في موقعه. وهذه الطريقة غالباً ما تنجح.

لذا يجب على المستخدم أن يقوم باختيار كلمة سر مختلفة للمواقع المختلفة، وخصوصا في المنتديات التي تدار من قبل أفراد قد لا يثق المستخدم بهم. وذلك لضمان أكبر قدر من الحماية لمعلوماته. كما أنه أيضا يمكن للمستخدم أن يقوم باختيار كلمة السر بشكل ذكي، بحيث يكون هناك جزء ثابت لا يتغير وجزء يتغير، وله علاقة باسم الموقع بحيث يكون لديه كلمة سر مختلفة بين المواقع المختلفة، وفي نفس الوقت لا يحتاج لأن يحفظ الكثير من كلمات السر، بل يكتفي بحفظ الجزء الثابت ومن ثم إدخال الجزء المتغير على حسب الموقع الذي دخل به.

### ١٠-٦-٤ عدم تغيير كلمة السر الافتراضية

تأتي بعض البرامج أو أنظمة التشغيل في بعض الأحيان مع كلمة سر افتراضية، يعرفها كل من قام بتركيب البرنامج. ويغفل الكثير من المستخدمين عن تغيير كلمة السر تلك، التي تعد أول كلمة يقوم المخترق بتجريبها في الغالب.

### ١٠-٦-٥ خلل في الاعدادات

يقوم بعض الأفراد بتركيب برامج الحماية المختلفة ولكنهم لا يعدونها بشكل صحيح، وهذا كما ذكرنا مسبقا يلغي فعالية تلك البرامج. فمن قام بتركيب برامج الحماية من الفيروسات، وقام بتعطيل خاصية الفحص التلقائي، فإن برنامج حماية الفيروسات لن يتمكن من فحص جميع



obeikandl.com

الملفات التي يتم سحبها من الإنترنت مباشرة. وهذا يعني احتمالية قيام المستخدم بتشغيل الملف ومن ثم إصابة جهازه بالفيروس.

وينطبق الشيء نفسه على برامج جدر الحماية الشخصية، فلو قام الشخص بتركيب جدار الحماية الشخصي وسمح للبرامج بأن تقوم بإرسال ما تريد من بيانات، وسمح لبرامج التروجان بفتح المنافذ المختلفة في جهازه، فلن تكون هناك أي فاعلية لتلك البرامج. بل انقلب دورها من الحارس إلى الخادم المطيع لبرامج التروجان.

ويشكل الخلل في الإعدادات مشكلة كبيرة، يجب الحذر منها عند استخدام أي برنامج يتطلب إعداداً من المستخدم. والحل لهذه المشكلة هو عدم قيام المستخدم بتحديد أيه إعدادات ما لم يكن واثقاً مما يفعله. وفي حالة عدم تأكده فيجب عليه سؤال من هو أعلم منه في تلك البرامج، وسيجد بالتأكيد من يمد يد العون له.

## ١٠-٦-٦ عدم تحديث البرامج وأنظمة التشغيل بشكل دوري

يتم اكتشاف الثغرات في أنظمة التشغيل وفي التطبيقات المختلفة بشكل يومي. وتقوم الشركات المنتجة للبرامج وأنظمة التشغيل بتزويد المستخدمين بتحديثات لتغطية تلك الثغرات وإصلاحها. ولكن، ما لم يقم المستخدم بسحب تلك التحديثات وتركيبها، فستبقى تلك الثغرات مفتوحة لكل من أراد اختراق الجهاز والعبث به. ونظراً لأهمية هذه المشكلة ولنسيان الكثير من المستخدمين تحديث أجهزتهم بشكل دوري، فإن معظم مصنعي البرامج يقومون بتوفير خاصية التحديث التلقائي لبرامجهم، بحيث لا يتحمل المستخدم عناء البحث عن التحديثات وتركيبها يدوياً، بل كل ما يلزمه هو توفير اتصال إنترنت للبرنامج الذي يقوم بزيارة موقع الشركة المصنعة للبرنامج وسحب آخر التحديثات. انظر الشكل ٨-٥



obeikandl.com

شكل ١٠-٥: إعدادات التحديث التلقائي في نظام ويندوز

obeikandl.com

# الفصل الحادي عشر :
# الحماية في القطاعات والمؤسسات

obeikandl.com

حماية الأجهزة الشخصية هي مهمة سهلة مقارنة بحماية الأجهزة الموجودة في القطاعات والمؤسسات المختلفة. ويتعرض هذا الفصل لبعض النواحي المتعلقة بالحماية من الجريمة في القطاعات والمؤسسات.

يخطئ بعض المستخدمين عندما يعتقدون بأن الحماية تبدأ بعد حدوث الجريمة أو الاختراق، وأنه لا يجب عمل أي شيء قبل حدوث ذلك. والصحيح أن الحماية من الجريمة هي مشوار طويل يبدأ قبل حدوث الجريمة وفي أثناء حدوثها، و يستمر أيضا حتى بعد حدوثها والتخلص من أثرها.

في هذا الفصل سنتطرق لجميع هذه المراحل، وهي:

١. الحماية قبل وقوع الجريمة

٢. الحماية في أثناء وقوع الجريمة

٣. الحماية بعد وقوع الجريمة

وقبل ذلك، يَحْسُن ذكر عدد من الإحصاءات التي توضح مقدار الضرر الحاصل جراء التهاون أو الفشل في تحقيق سياسة أمنية فعالة في الشركات والمؤسسات الاقتصادية، فقد أوضحت إحصائية للحكومة البريطانية أن ٣٣ ٪ من الجهات الحكومية في الحكومة قد تعرضت لمحاولات اختراق. وأن أكثر من ٣٤ ٪ من الجهات المرتبطة بالإنترنت غير واثقة في مقدرتها بالكشف عن الاختراقات حال حدوثها. وأن أكثر من ٣٣٪ من الجهات غير قادرة على البحث والتحري في الحوادث الأمنية التي قد تتعرض لها. وأظهرت إحصائية أخرى أن أكثر من ٦٠ ٪ من المنظمات الحكومية الأمريكية سبق وأن تعرضت لهجمات من قبل الفيروسات. و ٢٠٪ منها تعرضت لعملية اختراق، و٣٨ ٪ منها أبلغت عن سرقة أجهزة كمبيوتر محمولة (laptop).

وبينت دراسات (FBI) مع معهد أمن الحاسبات بأن متوسط الخسائر الناتجة عن الاختراق



obeikandl.com

تقدر بمبلغ ٦,٦ مليون دولار لكل محاولة اختراق. وأشارت إلى أن نصف محاولات الاختراق للشركات ناتجة من داخل الشركة أو من قبل موظفين مفصولين من الشركة.

فيما أوضحت أن فيما ذكرت جريدة لوس أنجلوس تايمز أن خسائر شركة نوكيا جراء اختراق الهاكر كيفن ميتنك لها بلغت (١٣٥) مليون دولار.

وأما شركة كمبيوتر إيكونوميكس للأبحاث (Computer Economics) فقدرت الخسائر الناتجة عن فيروس (Code Red) بـ ١,٢ مليار دولار، مابين خسائر في الإنتاجية أو خسائر لإصلاح الأجهزة.

obeikandl.com

## ١١-١ الحماية قبل وقوع الجريمة

الحماية قبل وقوع الجريمة هي خطوة مهمة، حيث إن التعامل مع الهجمة في حال وقوعها يعتمد بشكل كبير على جودة الاستعداد في هذه الخطوة. والحماية قبل وقوع الجريمة يتلخص باختصار بالاستعداد لها قبل وقوعها، وذلك على ثلاثة مستويات:

- مستوى الأجهزة المستقلة
- مستوى الشبكة
- مستوى الأشخاص والمستخدمين

### ١١-١-١ تحديد ما تريد حمايته

قبل أن يبدأ الشخص المشرف على الشبكة بالتخطيط وتفعيل معايير الحماية، يجب عليه



obeikandl.com

أولاً أن يحدد النطاق الذي يرغب بحمايته. فمثلاً، تكتفي بعض القطاعات بحماية الأجهزة المرتبطة بالإنترنت فحسب، دون حماية الأجهزة الموجودة في الشبكة الداخلية. بينما قطاعات أخرى ترغب في حماية جميع الأجهزة الموجودة في شبكتها، سواءً كانت مرتبطة بالإنترنت أو لم تكن كذلك. وهناك قطاعات أخرى قد ترغب في حماية الأجهزة الموجودة في الإدارات الحساسة، مثل الإدارة المالية وإدارة شؤون الموظفين، بينما لا تهتم بحماية الأجهزة في الإدارات الأخرى. و يجب أيضاً تحديد مستوى الحماية المطلوب، فالجهاز المحتوى على مزود الويب الخاص بموقع الشركة يجب أن يكون محمياً بشكل أكبر مقارنة بجهاز أحد المستخدمين في الشبكة.

وبناء على هذا التحديد يقوم المشرف بتحديد خطة مبدئية لتفعيل الحماية في شبكته، ومن ثم ينتقل لتطبيق معايير الحماية التي يريدها.

### ١١-١-٢ تحديد سياسة أمن الشبكة (Information Security Policy) وسياسة الاستعمال المقبول (Acceptable Usage Policy)

هذه السياسات هي قواعد يقوم المشرف على الشبكة بتحديدها بناء على:

- مستوى الحماية المطلوب توفيره للشبكة.
- الصلاحيات التي ترغب الشركة منحها لموظفيها لاستخدام الإنترنت.

فمثلا، في ناحية السياسة الأمنية للشبكة، فبعض الشركات لا تمانع من استخدام برامج نقل الملفات في شبكتها، بينما شركات أخرى قد تعد ذلك من المخاطر الأمنية لانتشار الفيروسات وتقوم بمنع ذلك. ومثال آخر هو إمكانية الاتصال الشبكي الهاتفي (Dial-up Connection) فبعض الشركات لا تسمح بذلك، بينما شركات أخرى قد تسمح به.

أما من ناحية سياسة الاستخدام المقبول، فهو يتعلق باستخدام الموظفين للشبكة. فبعض الشركات تسمح للمستخدمين بتصفح المواقع أثناء وقت الدوام الرسمي، بينما شركات أخرى لا تسمح بذلك. وكذلك أيضا باستقبال نوعية معينة من الملحقات Attachments في



obeikandl.com

البريد الإلكتروني، فبعض الشركات تمنع استقبال بعض النوعيات من الملحقات عن طريق البريد الإلكتروني الرسمي للشركة.

بالطبع فهناك العديد من النقاط والقواعد التي يجب ذكرها في تلك السياسات، التي يجب أن يطلع عليها الموظف الجديد عند التحاقه بالشركة، ليكون على معرفة بما هو مسموح وما هو غير مسموح له بعمله.

### ١١-١-٣ الاستعداد على مستوى الأجهزة

ويعني بذلك أن المشرف على الشبكة سيقوم بتطبيق معايير الحماية المطلوبة في كل جهاز على حدة. وهذا ضروري جداً على الرغم من أنه متعب عند وجود الكثير من الأجهزة، وهذا ما يزيد من أهمية خطوة (تحديد ما تريد حمايته) المذكورة سابقاً. ونقوم بحصر المعايير الأمنية التي يجب تطبيقها على مستوى الأجهزة بالآتي:

### ١١-١-٣-١ عمل نسخ احتياطية

الهجمات التي تقوم بسرقة المعلومات قد لا تقوم بتدمير البيانات، ولكن هناك أنواع أخرى من الهجمات يقوم المخترق فيها بمسح البيانات. ولهذا يجب القيام بعمل نسخة احتياطية من البيانات المهمة، والتي تختلف من جهاز إلى آخر، والقيام بتحديث هذه النسخة بشكل دوري. ويتم تحديد الفترة التي يجب فيها عمل النسخة الاحتياطية في السياسة الأمنية للشركة التي سيتم الحديث عنها لاحقاً.

ومعروف أن النسخة الاحتياطية ليس الغرض منها هو استرجاع البيانات في حالة الاختراق فحسب. بل إن البيانات قد تضيع لأي سبب آخر، مثل تلف القرص الصلب أو انقطاع الكهرباء بشكل مفاجئ أو غيرها من الأسباب. كما أنها أيضاً قد تستخدم للحفظ



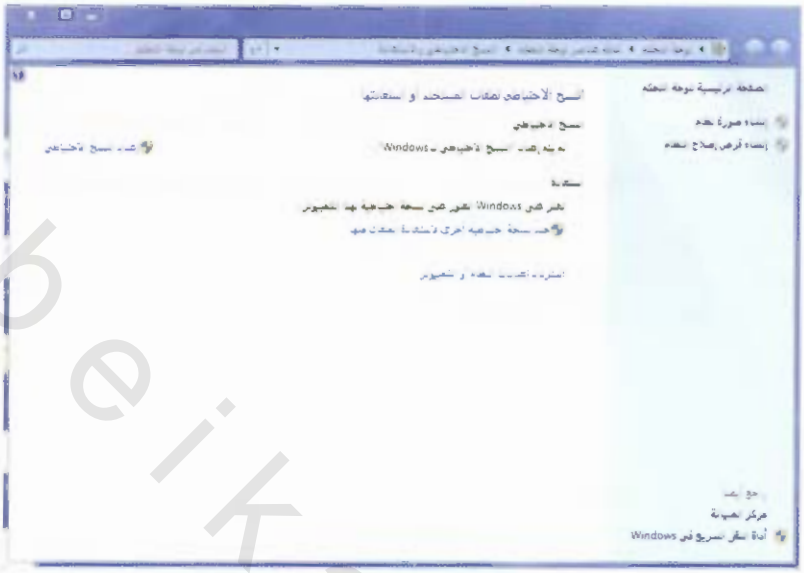
openkandil.com

والتوثيق وتتبع تطور البيانات على مر الزمن، حيث تمكن أصحاب القطاع أو الشركة من رؤية حالة البيانات في الماضي ومقارنتها بالحاضر. ولكن هذا خارج عن السياق الذي نريده وهو الحماية الأمنية.

يجب التنبيه بأن النسخ الاحتياطي لا يعني وجود حماية كاملة للبيانات، فعلى الرغم من أن النسخة الاحتياطية تحتوي على البيانات المطلوبة، إلا أنه في حالة حدوث اختراق فقد يتطلب الأمر وقتاً طويلاً قبل الحصول على جهاز يمكن نسخ البيانات إليه. ويجب أيضاً ملاحظة أن البيانات المنسوخة قد تكون معرضة للعبث والتغيير قبل عمل نسخة احتياطية منها، ومن ثم فإن هذا يعني أن النسخة الاحتياطية عديمة الفائدة. لذلك لابد من وجود خطة واضحة لكيفية النسخ الاحتياطي والاسترجاع، وتجريب هذه العملية بشكل دوري.

ويوجد العديد من البرامج التي تساعد على القيام بنسخة احتياطية، وهي موجودة على مختلف أنظمة التشغيل. وتوجد أيضاً وسائل عديدة لتخزين البيانات المنسوخة بدءاً من الشريط (Tape) وانتهاءً بأقراص (DVD) القابلة للكتابة. وتحديد البرنامج ونوعية الوسيط الذي يتم النسخ عليه هو خارج نطاق الحديث في هذا الكتاب.

obeikandl.com



شكل ١١-١: برنامج عمل النسخ الاحتياطية في ويندوز٧

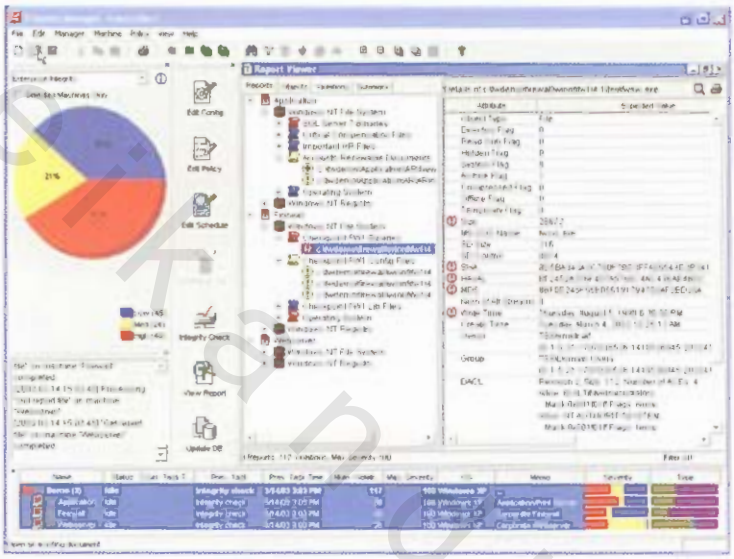
### ١١-١-٣-٢التأكد من سلامة الملفات من التغيير

كما ذُكر آنفاً، فإن عمل النسخ الاحتياطية غير كافٍ بشكل كامل، فعند تعرض النسخة الأصلية للتلف فإن برنامج النسخ سيقوم بعمل نسخة احتياطية من البيانات المعطوبة. ومن هنا تظهر الحاجة لوسيلة تسمح للمشرف على الشبكة أو الجهاز بالتأكد من سلامة البيانات من العبث والتغيير. وهذه هي وظيفة برامج ملخص الرسالة، وهي برامج تستقبل البيانات كمدخل، وتقوم بإخراج رمز صغير يقاس بعشرات البايتات، ويقوم بتمييز هذه البيانات. وميزة هذه الرمز هو أنه مميز للبيانات، بحيث إنه في حالة تغير البيانات، ولو بشكل بسيط، فإن الرمز الناتج سيتغير. وطريقة استخدام هذه البرامج هو أن يقوم المشرف على الشبكة، باستخراج الرموز الخاصة بالملفات التي تحتوي على البيانات المهمة، وتخزين هذا الرموز في مكان آمن.



obeikandl.com

ويقوم دورياً باستخراج الرموز لنفس البيانات. وفي حالة تغير الرموز فهذا يعني أن البيانات قد تم تغييرها بشكل غير مرغوب، ومن هنا يعلم المشرف أن البيانات قد تعرضت للاختراق. ومن أشهر البرامج من هذه النوعية هو برنامج (TripWire) الذي كانت بدايته على نظام يونكس، ومن ثُمَّ تَمَّ إصداره على نظام ويندوز. انظر الشكل ١١-٢.



شكل ١١-٢: لقطة لبرنامج TripWire

### ١١-١-٣-٣ تشغيل التسجيل

وهذا من أهم الاحتياطات التي تساعد على اكتشاف وجود عملية اختراق، ومن ثم تتبع المخترق. ومن دونها لا يستطيع المشرف على النظام معرفه ما يحصل في النظام. ويمكن تقسيم ملفات التسجيل إلى قسمين، الأول هو ملفات التسجيل المتعلقة بنظام التشغيل وخدماته والقسم الآخر هو المتعلق بالتطبيقات المختلفة. وفي الآونة الأخيرة ومع انتباه مصنعي برامج الحاسب إلى أهمية الناحية الأمنية، فإن معظم البرامج تأتي مع خاصية تشغيل التسجيل (Logging) فيها مفعلة تلقائياً. ولكن هذا لا يمنع من أن يقوم المشرف بالتأكد من ذلك، والقيام باختيار المعلومات

التي يريد تسجيلها. ولعل معظم البرامج والأنظمة تقوم بتسجيل عدد كبير من المعلومات، أهمها رقم (IP) للجهاز الخارجي، ونوع العملية المطلوبة وتاريخها، ورد النظام على ذلك الطلب.

### ١١-١-٣-٤ تحصين الأجهزة وتحديثها

توجد مقولة لدى خبراء حماية الشبكات، وهي أن مستوى الحماية في الشبكة يقاس بمستوى حماية أضعف جهاز موجود فيها. أي أنه لا يجب إعطاء مجموعة من الأجهزة قدراً كبيراً من الحماية وإهمال مجموعة أخرى، بل يجب المساواة بينها في مستوى الحماية.

ويمكن تحصين مستوى الحماية في الأجهزة بالشكل الآتي:

- إيقاف الخدمات العاملة التي لا يتم استخدامها. فبعض أنظمة التشغيل تقوم بتشغيل عدد كبير من الخدمات التي لا يتم استخدامها على الإطلاق، وتكون مصدراً للخطر على الجهاز. فجهاز خادم الملفات لا يحتاج لوجود مزود ويب، أو مزود بريد، ولذا يجب إيقافها.
- تركيب برامج اكتشاف الاختراق الخاصة بالأجهزة.
- (Host-based Intrusion Detection Systems) التي تحتوي على قدر من الذكاء يسمح لها بالتعرف على وجود محاولة اختراق وإنذار المشرف على الشبكة لحظيا.
- الحرص على تركيب آخر التحديثات سواء لنظام التشغيل أو للبرامج المختلفة الموجودة في النظام. والكثير من البرامج في الوقت الحالي مصممة بطريقة تسمح لها بالتأكد من وجود تحديثات وإخبار المستخدم بذلك.



obeikandi.com

شكل ١١-٣: شاشة البرنامج المدمج في ويندوز٧ الذي يعمل على تحديث ويندوز بشكل تلقائي

## ١١-١-٣-٥ المعدات البيولوجية

هي معدات يكون الغرض الرئيس منها هو التحكم في الدخول للجهاز، وهي تعتمد على الخصائص البيولوجية التي تميز الأشخاص مثل بصمة الإصبع أو قزحية العين. حيث يوجد بعض العتاد الذي يربط بالجهاز ويقوم بالتغلغل في نظام التشغيل، بحيث لا يسمح للشخص بالدخول للنظام ما لم يكن هو الشخص صاحب النظام. وتقوم الكثير من الشركات بتوفير قارئات البصمة وقارئ قزحية العين. كما أن بعض شركات الأجهزة المحمولة بدأت تصنع أجهزة محمولة بحيث يوجد قارئ البصمة مدمجاً فيها.

وكما ذكر سابقاً، فإن هذه الخاصية تعد مرغوبة ممن يتطلب عملهم قدراً أكبر من الحماية، مثل مديري الشركات الكبرى التي تحتوي أجهزتهم على أسرار شركاتهم وتعاملاتها المختلفة. فهؤلاء



obeikandl.com

يعدّون هذه النوعية من الحماية من باب الحاجة الماسة وليست من باب الرفاهية. ولكني بالنسبة للمستخدم العادي فلا أنصحه باستخدام هذه النوعية من الحماية، فهي مبالغ فيها بشكل كبير.

شكل ١١-٥: قارئ بصمة اليد في الحاسب المحمول

### ١١-١-٤ الاستعداد على مستوى الشبكة

تركز هذه المرحلة على الناحية الأمنية المتعلقة بالبنية التحتية للشبكة. ويوجد العديد من الاحتياطات الأمنية التي يجب أن تفعل على مستوى الشبكة، فبعضها يكون بتركيب البرامج، وبعضها الآخر يكون متعلقاً بتصميم الشبكة. وسيتم تناول هذه الاحتياطات فيما يأتي.

### ١١-١-٤-١ تصميم الشبكة بشكل سليم

ويقصد بذلك تصميم الشبكة بشكل سليم لتقليل الخطر الناتج عن الاختراق. حيث إن بعض المشرفين على الشبكات يظن أن الغرض الوحيد من الشبكة هو إيجاد قناة اتصال بين



obeikandl.com

الأجهزة الموجودة فيها. وهذا اعتقاد خاطئ كلياً. حيث إنه يجب وضع الحماية الأمنية في البال عند تصميم الشبكة. بالطبع فهناك طرق وتقنيات عديدة لتصميم الشبكات، ولكنها خارج نطاق الحديث في هذا الكتاب، وتوجد كتب مخصصة لهذا المجال يجب على من يريد الإشراف على الشبكة أن يقوم بالاطلاع عليها.

### ١١-١-٤-٢ تركيب جدر الحماية(Firewalls) و برامج اكتشاف الاختراق (IDS/IPS)

جدر الحماية هي برامج يتم تركيبها على أجهزة تفصل بين شبكتين مختلفتين، بحيث لا تمر أيه بيانات من شبكة إلى أخرى دون المرور بجدر الحماية. ووظيفتها هي إيقاف جميع البيانات المارة خلالها ومقارنتها بالقواعد والصلاحيات التي وضعها من قام بإعداد جدار الحماية، ومن ثم إصدار القرار إما بالسماح لتلك البيانات بالمرور أو منعها من ذلك. أما برامج اكتشاف الاختراق، فهي برامج يتم ربطها بالشبكة، بحيث تقوم بمراقبة جميع البيانات المارة خلال الشبكة، وبناء على معايير ذكاء صناعي فيها تقوم بتحديد ما إذا كانت هذه البيانات تمثل بيانات لعملية اختراق تجري حالياً، ومن ثم تقوم بإنذار المشرف على الشبكة.

بالطبع تركيب هذه البرامج بحد ذاته لا يكفي لحماية الشبكة، ولكن الكلمة السحرية هنا هي (الإعداد السليم). حيث إن التركيب عملية سهلة لا يلزم فيها سوا نقرة زر حتى ينتهي تركيب البرنامج. ولكن إيجاد الإعدادات السليمة لهذه البرامج هو الأمر الصعب الذي يتطلب خبرة بعلم الشبكات. وبديهي أن الإعداد يختلف من شبكة لأخرى، ويعتمد بشكل كبير على تصميم الشبكة والاحتياطات الأمنية التي يريد المشرف على الشبكة تفعيلها، وعلى السياسة الأمنية للقطاع. وغني عن الذكر أن طرق إعداد مثل هذه النوعية من البرامج لا يمكن تفصيلها في هذا الكتاب بل يجب على من يريد تعلم ذلك أخذ العديد من الدورات في هذا المجال وقراءة الكتب المختلفة حتى يتمكن من ذلك.



obeikandi.com

### ١١-١-٤-٣ تحصين المحولات

وظيفة المحولات هي تمرير البيانات بين شبكتين مختلفتين، وهي عموماً تقوم بعمل ذلك على مستوى الشبكة بعكس جدر الحماية الحديثة نسبياً التي تعمل غالباً على مستوى التطبيقات، فبعض المحولات الحديثة تحتوي على بعض الوظائف الموجودة في جدر الحماية، ولكنها في الغالب لا تحتوي على كافة المميزات، والعكس كذلك صحيح، فبعض جدر الحماية لديها القابلية للوصول لمستوى الشبكة. ولكن الغرض والوظيفة الخاصة بكل منهما مختلفة تماماً لذا يجب عدم الخلط بين الاثنين.

يمكن تفعيل الحماية في المحولات وجعلها مساعدة لجدر الحماية. وذلك بتفعيل وظيفة قوائم التحكم بالدخول التي يحدد فيها المشرف على الشبكة نوعية البيانات التي يسمح بدخولها والشبكات التي يجب أن تأتي منها هذه البيانات. وهذه القوائم تساعد بشكل كبير على التخلص من أضرار هجمات منع الخدمة (DoS)، حيث يمكن التخلص من معظم الطلبات الزائفة قبل أن تصل لجهاز المزود وتشغله عن خدمة الطلبات الحقيقية.

يجب التنبيه إلى أنه من المستحسن جداً أن يفعّل المشرف خاصية التسجيل في المحول، وذلك لكي يتمكن من معرفة نوعية البيانات الداخلة والخارجة من شبكته، وكذلك معرفة محاولات الهجوم التي تحدث على شبكته في الوقت الحالي.

### ١١-١-٥ الاستعداد على مستوى الموظفين

يغفل بعض المستخدمين عن أهمية العنصر البشري في حماية الشبكات، ويعتقدون بأن حماية الشبكات تتم عن طريق تفعيل المعايير الأمنية في الأجهزة الموجودة في الشبكة فقط، وهذا اعتقاد خاطئ كلياً. حيث إن العنصر البشري يؤدي دوراً كبيراً جداً في حماية الشبكات. وأبسط مثال على ذلك مشكلة كبيرة كانت السبب في معظم حوادث الاختراق على الشبكات، وهي أن المشرف على الشبكة يقوم بتحصين الشبكة من الخارج ووضع جميع المعايير الأمنية لحمايتها، ومن ثم يقوم أحد الموظفين في الشركة بوضع جهاز مودم في جهازه بحيث يتمكن من

الاتصال بشبكة الشركة من الخارج. فيفتح هذا العمل باباً خلفياً يسمح للمخترق بالدخول للشبكة من دون الحاجة لتخطي معايير الحماية الأمنية التي قام المشرف على الشبكة بتركيبها. وقد انتشرت في السابق برامج تسمى (War Dialer)، وهي برامج تقوم بالاتصال على رقم شركة معينة، ومن ثم تجربة التحويلات المختلفة واحدة تلو الأخرى بحثا عن جهاز مودم. وغالبا ما يقوم المخترقون بهذه التجربة في الفترة الليلة عندما لا يوجد أحد في المكاتب.

هذا مثال واحد فحسب للخطر الذي قد يتسبب به العنصر البشري على حماية الشبكة وأمنها. ويتطرق هذا القسم لبعض المعايير الأمنية المتعلقة بالعنصر البشري في الشبكة.

### ١١-١-٥-١ جدر الحماية البشرية

هذا المصطلح هو أحد المصطلحات التي ظهرت حديثا بعد الانتباه لأهمية العنصر البشري في حماية الشبكات. حيث لوحظ أن المستخدمين يمكن تشبيههم ببرامج جدر الحماية

التي تساعد على حماية الشبكة. وكما أن برامج جدر الحماية تساعد على ذلك بالإعداد السليم، فإن المستخدمين يساعدون على حماية الشبكة، وذلك بتثقيفهم وتعليمهم بمخاطر الشبكة وكيفية مساهمتهم في حمايتها.

تقع المسؤولية على عاتق المشرف على الشبكة في التأكد من نوعية المستخدمين بمخاطر الشبكة وكيف يمكنهم تجنبها. ويمكنه عمل ذلك بطرق عديدة، أسهلها إرسال رسائل بريد إلكترونية للمستخدمين، أو القيام بعمل ندوة للموظفين بين الحين والآخر. ولكن من أهم المعايير في ذلك هو السياسة الأمنية (Security Policy) وسياسة الاستخدام المقبول (Acceptable Usage Policy) التي سيتم الحديث عنها لاحقاً.

### ١١-١-٥- ٢ الهندسة الاجتماعية

الهندسة الاجتماعية تعدّ من أخطر الطرق لاختراق العنصر البشري في مجال حماية الشبكات. ويذكر الهاكر الشهير كيفن ميتنك في كتابه (Art of Deception) أنه لولا وجود هذه الطريقة لما تمكن من القيام بالعديد من عمليات الاختراق التي قام بها في السابق.

والفكرة هنا هو أن يقوم المخترق باستخدام قدرته في الإقناع للحصول على المعلومات التي يريدها ممن يتحدث إليه. وتنجح هذه الوسيلة في الغالب بسبب سذاجة المستخدمين العاديين وتصديقهم لمن يتحدث إليهم بمجرد استخدامه لبعض المصطلحات التقنية. فكم من مخترق تمكن من الحصول على كلمة السر الخاصة بالمستخدم من المستخدم نفسه عن طريق الهاتف طواعية وبتعاون من المستخدم الضحية.



openkandil.com

## ١١-٢ الحماية في أثناء الجريمة

يفترض هذا القسم أن الجريمة قد حدثت أو أنها جارية الحدوث، فما هي الإجراءات التي يجب على المشرف على الشبكة اتخاذها خلال تلك الفترة؟

من المعروف أن كل جريمة لها ظروفها وملازماتها الخاصة بها التي تجعل منها فريدة في نوعها، مما يجعل من الصعب تحديد قواعد ثابتة يجب القيام بها، ويمكن تطبيقها في جميع الجرائم التي تحصل على الشبكات. ولكن يمكن مناقشة بعض التوجيهات العامة التي قد تكون متوفرة في أي جريمة، من باب توفير بعض الإرشادات التي تساعد المشرف على الشبكة على اتخاذ القرارات التي تتناسب مع ما يواجهه في شبكته.

فعلى الرغم من أن كل جريمة تتميز عن غيرها، وأن كل جريمة قد تتطلب طرق تعامل مختلفة من قبل المشرف على الشبكة. إلا أن هناك بعض الأهداف المشتركة التي يحاول كل مشرفي الشبكات الوصول لها عند تعرض شبكاتهم للاختراق، وهي كالآتي:

- التقليل من الضرر الناتج عن الجريمة
- إزالة الجريمة والعودة إلى نظام العمل الطبيعي
- عدم مسح الأدلة التي قد تساعد للوصول إلى المجرم

### ١١-٢-١ قبل اتخاذ القرار

حدوث جريمة على الشبكة يجعل المشرف عليها يتعرض لضغط نفسي كبير قد يتسبب في تسرعه واتخاذه لقرارات خاطئة. لذا فإن أول نصيحة يجب العمل بها هو التروّي وعدم التهور ومحاولة جمع أكبر قدر من المعلومات التي تساعد على تقييم الجريمة، وتساعد على اتخاذ القرار المناسب في التعامل معها. ولكن في الوقت نفسه يجب على المشرف أيضا ألا يتأخر في اتخاذ



obeikandl.com

القرار، لأن ذلك قد يزيد من الضرر الناتج عن الجريمة.

ويجب على المشرف على الشبكة جمع المعلومات المتعلقة بالاختراق والتي ينبغي أن تحتوي الآتي:

- **الأسئلة الخمسة المشهورة التي يسألها الصحفيون غالباً**: من ؟ متى ؟ أين ؟ ماذا ؟ ولماذا ؟ ومن الطبيعي جداً ألا تتوفر الإجابة الكاملة عن جميع هذه الأسئلة في البداية، ولكن يجب على الأقل إبقاء هذه الأسئلة في البال، ومحاولة الحصول على الإجابة لأكبر عدد منها قبل التعامل مع الجريمة.
- **إحصاء الأجهزة المتضررة من الجريمة**: حيث يجب معرفة أثر الجريمة على الشبكة، وما هي الأجهزة المتضررة من تلك الجريمة. فالجريمة التي يتعرض فيها مزود الويب للاختراق، يختلف التعامل معها عن الجريمة التي يكون تأثيرها متعلقاً بعدد أكبر من الأجهزة. ويجب على المشرف بعد تحديد هذه الأجهزة أن يجمع أكبر قدر من المعلومات عن تلك الأجهزة، مثل:
  - نظام التشغيل
  - الخدمات العاملة على ذلك الجهاز
  - المعلومات المخزنة على ذلك الجهاز
  - موقع الجهاز في الشبكة الخاصة بالمنظمة
  - العتاد الموجود في الجهاز

في حالة التصميم والإشراف السليم على الشبكة، فإن معظم هذه المعلومات يجب أن تكون متوفرة قبل حدوث الهجمة. لأنها ستفيد بشكل كبير في التعامل معها.

- **تحديد نوعية الجريمة**: يعتمد التعامل مع الجريمة على نوعيتها. وذلك ينطبق كذلك على الجريمة في الحياة الواقعية. فالشرطي عندما يقوم بالتعامل مع جريمة سرقة لمنزل معين، فإنه يستطيع أخذ وقته ومحاولة جمع أكبر قد من المعلومات، ولكن في حالة وجود جريمة استخدم فيها السلاح، ويوجد مصابين فمن الضروري التعامل معها بشكل سريع وطلب الإسعاف، لنقل المصابين للمستشفى، ومن ثم القيام بجمع المعلومات المطلوبة. وكذلك هو الحال في



openkandil.com

جرائم الشبكات. فيجب على المشرف على الشبكة تحديد نوعية الجريمة أولاً، ومن ثم يقوم بتحديد طريقة التعامل معها، فجريمة هجمات منع الخدمة مثلاً، يختلف التعامل معها عن هجمات اختراق الموقع وتغيير محتوياته.

### ١١-٢-٢ اتخاذ القرار

تعد هذه هي الخطوة الفعلية تجاه التخلص من آثار الهجمة، وهي من أصعب الخطوات التي يترتب عليها الكثير من العواقب والتبعات. وهناك الكثير من الخيارات التي تتوفر للمشرف على الشبكة عندما يريد البدء في التخلص من الآثار المترتبة على الهجوم، وهذه الخيارات لا يمكن حصرها بشكل كامل في هذا الكتاب، ولكن يمكن تقديم بعض الأمثلة على تلك الخيارات وكيفية الوصول للاختيار الصحيح:

#### ١١-٢-٢-١ إعادة التركيب

لعل من أسهل الخيارات للمشرف على الشبكة في حالة اختراق جهاز معين، هو إعادة تركيب نظام التشغيل بشكل كامل. أو في حالة الهجمة التي تقوم بتغيير الموقع فإن المشرف قد يقوم باسترجاع الصفحات الرئيسة وإعادة الموقع للشكل السليم.

هذا الإجراء سيقوم بالتخلص من أثر الجريمة بشكل سريع، ولكنه لن يكون بالتأكيد بشكل دائم. فمثلا، يمكن أن يتعرض جهاز معين للاختراق من دون أن يحتوي على ثغرات أبداً، ولكنه تعرض للاختراق كنتيجة لاختراق أجهزة أخرى، ووجود علاقة ثقة بينه وبين تلك الأجهزة. ففي هذه الحالة يمكن إعادة تركيب النظام في ذلك الجهاز، والتأكد من التخلص من الجريمة في تلك الأجهزة بطريقة أخرى. ولكن إذا كان الاختراق ناتجًا عن عدم تحديث الجهاز، ووجود ثغرة في نظام التشغيل، فإن إعادة تركيب الجهاز سيزيل أثر الجريمة بشكل مؤقت ولكنه ليس دائمًا، حيث إن المخترق يستطيع استخدام نفس الثغرة مرة أخرى لاختراق الجهاز.

بالإضافة إلى ذلك فإن إعادة تركيب النظام قد يعني إزالة بعض الأدلة التي قد يستفاد منها في الوصول للمجرم. لذا يجب على المشرف على الشبكة التأكد من أن إعادة تركيب النظام هو الخيار السليم للتخلص من الجريمة.

### ١١-٢-٢-٢ إبقاء الجهاز مرتبطا بالشبكة أو عزله

وهذه هي أحد الخيارات التي تواجه المشرف على الشبكة عن حدوث جريمة معينة على أحد الأجهزة في شبكته. حيث يمكنه أن يقوم بالتعامل مع الجريمة والجهاز مرتبط بالشبكة، أو مفصول عنها. في بعض الأحيان، فإن هذا الخيار لا يكون موجوداً أصلاً، مثل أن يكون الجهاز المخترق هو جهاز يستقبل تعاملات مالية من شركات أخرى، ولا يوجد منه نسخة احتياطية، وفي نفس الوقت فإن الاختراق الحاصل لا يؤثر على صحة البيانات المالية، ولكنه يتعلق بناحية أخرى من الخدمات الموجودة في الجهاز. ففي هذه الحالة فإنه من الضروري إبقاء الجهاز عاملاً، وإلا فإن الشركة ستخسر الكثير من التعاملات المالية. وفي أحيان أخرى وفي حالة جهاز آخر مشابه لذلك الجهاز في الوظيفة وفي الإعدادات، فإنه من السهل جداً عزل الجهاز المصاب وتبديله بالجهاز الاحتياطي حتى يتم إصلاح الجهاز الأصلي والتخلص من أثر الجريمة بشكل كامل.

ولكن هناك حالات أخرى تكون المعطيات فيها أعقد بكثير مما هو أعلاه، وفي تلك الحالة فإن القرار يرجع للمشرف على الشبكة، ويجب عليه اتخاذ القرار الذي يترتب عليه الضرر الأقل.

obeikandl.com

### ١١-٢-٣ عدم مسح آثار الجريمة

يوجد قسم مهم من علوم أمن المعلومات يختص بكيفية فحص الجهاز المصاب، والحصول على الأدلة الكافية لتحديد المجرم وهو علم التحقيق في جرائم الحاسب. وهذه من الإجراءات التي غالباً ما تتم بعد إيقاف فاعلية الجريمة، ورغبة المشرف على الشبكة في ملاحقة المجرم ووضعه تحت يد العدالة. وهذا القرار يعتمد بشكل كبير على سياسة الشركة تجاه الاختراقات، فبعض الشركات لا ترغب في الخوض في النواحي القانونية وملاحقة المجرمين وصرف المبالغ الطائلة في محاولة وضعهم في السجون. ولكن هناك شركات أخرى قد ترغب في ذلك.

إذا كانت سياسة الشركة أو المنظمة تتطلب ملاحقة المجرم، فإنه يلزم المشرف على الشبكة أن يقوم بكل ما يلزم لكي لا يفقد الأدلة المتعلقة بالجريمة. وهذا ما يجعل التعامل مع الجريمة يختلف عنه في الحالة الأخرى. ولن نخوض في تفاصيل هذه العملية فهي معقدة وخارجة عن نطاق الكتاب، ويوجد الكثير من الكتب التي تتحدث عنها بشكل مفصل وكافٍ.

obeikandl.com

## ١١-٣ الحماية بعد وقوع الجريمة

تمثل هذه الخطوة تكراراً ومراجعة للخطوة الأولى (الحماية قبل وقوع الجريمة). حيث إن الاستعداد واتخاذ الحذر من الجريمة لا يعني استحالة حدوثها، وحدوث الجريمة الحالية أكبر دليل على ذلك. لذا فمن الضروري على المشرف على الشبكة أن يقوم بمراجعة ما عمله في الخطوة الأولى، ومعرفة مصدر الخلل سواء كان في السياسة الأمنية أو الإعدادات أو خلافه. ومن ثم يجب عليه أن يقوم باتخاذ ما يلزم لضمان عدم حصول ذلك مرة أخرى. وكثيراً ما يكون الخلل في السياسة الأمنية أو في تطبيقها، وهذا يتطلب من المشرف على الشبكة أن يقوم بتحديث السياسة الأمنية والتأكد من تطبيقها بشكل سليم.

obeikandl.com

## الفصل الثاني عشر :

# ماذا يخبئ المستقبل على الإنترنت؟

obeikandl.com

إن أول الحقائق وأهمها والتي يجب أخذها بالحسبان في هذا الخصوص هي أن شبكة الإنترنت تشهد تغيراً وتطوراً مستمرين على الدوام. ولذلك فإن أسئلة عديدة تحول بخاطر الكثيرين، مثل: كيف سيكون حال الإنترنت بعد عشر سنوات، أو عشرين سنة، أو حتى في المستقبل القريب جداً ؟ هل ستشهد الساحة مثلاً تقنيات جديدة، وقوانين جديدة موحدة على نطاق دولي لمواجهة جرائم الإنترنت والاستخدامات الخاطئة لها؟ أم هل ستنشأ جهة مخولة باتخاذ إجراءات قانونية وإيقاع العقوبات بالمجرمين أو المتطفلين والمتسكعين على أبواب المواقع؟ وهل سيؤدي الازدياد الهائل في عدد المستخدمين الجدد للشبكة إلى تغيير واقعها بصورة جوهرية؟

لاشك أن الأسئلة كثيرة ومتباينة والسائلون في ازدياد، ولكن الأجوبة ما تزال قليلة وغير شافية. فواقع الحال يشير بوضوح إلى أن عدد الأخطار ونوعها سيشهدان نوعاً من التغير في المستقبل. وأن المستخدمين سيشهدون المزيد من الخصوصية على الشبكة. ولإلقاء مزيد من الضوء في هذا المجال، يستعرض هذا الفصل فيما يأتي آراء بعض المتخصصين في مجال الإنترنت.

obeikandl.com

## ١٢-١ حقائق وتوقعات

فيما يتعلق بالخصوصية ذكر دانيال باريت في كتابه (قطاع طرق على طريق المعلومات السريع)، أن الخصوصية في الإنترنت هي صديق كل مستخدم للشبكة، ولكنها في الوقت ذاته هي مصدر خطر لكل مدير نظام.

ويقول أيضاً: «إننا إن لم تتوفر لنا الخصوصية الكافية في أجهزة الحاسب، فإن هذه الأجهزة ستصبح غير ذات جدوى، وأما إن توفرت لنا خصوصية غير محددة، فإن مديري الحاسب والأنظمة الحكومية لن يستطيعوا القيام بمهمة مراقبة الأعمال غير القانونية التي يمكن أن تلحق الأذى بالمجتمع». ولذلك فهو يرى أن الحل يكمن في توفر برامج أفضل تضمن التحقق من هوية المرسل لأي رسالة، وكذلك في استخدام نظام التشفير الذي يؤمن خصوصية الاتصالات على الشبكة.



obeikandl.com

وأما فيما يتعلق بالأمن والحماية من خطر الجريمة على شبكة الإنترنت، فهو يقول: «إن الاختراقات الأمنية ستكون في ازدياد حتى يتوفر برنامج أفضل للحماية».

وعليه فإن جرائم التزوير والتزييف والرسائل المنتحلة والخادعة سيزداد عددها، حتى يتم وضع برنامج للشبكات أكثر أمناً وتطوراً، مع ازدياد عدد المستخدمين الذين لديهم القدرة على ارتكاب مثل هذه الجرائم، لأن توفر الأمن عن طريق الغموض والإبهام لن يستمر إلى ما لانهاية. وهو يتوقع أيضاً ظهور المزيد مما يشبه (حروب العصابات) كلما تعلم عدد أكبر من المستخدمين كيفية إلغاء الرسائل الإلكترونية المرسلة من بعضهم إلى بعض.

ولذلك يتضح مما ذكر أن الحلول الموضوعة لحماية الخصوصية ستؤثر أيضاً على الأمن والحماية في الشبكة، لأنه لو توفرت للمستخدمين هويات لا يمكن تزويرها، ونظام تشفير خفي للاتصالات، فإن أعمالهم على الشبكة ستكون أكثر أمناً.

أما براد تيمبلتون الرئيس التنفيذي لصحيفة (كلارينيت كوميونيكيشنز كور)، وهي صحيفة إلكترونية حسنة السمعة تنشر على الإنترنت، فهو يرى فيما يتعلق بمستقبل حماية الخصوصية في الإنترنت، أنه يصعب التنبؤ بما سيكون عليه حال حماية الخصوصية، وأن المتوقع أنه سيكون لها قابلية السير في اتجاهين، وذلك لأن أجهزة الحاسب لها قدرة عظيمة على حماية الخصوصية واختراقها معاً، أكثر من أي تقنية أخرى! وأن ذلك يعتمد بالطبع على طريقة استخدامنا لها، والكيفية التي يسمح لنا القانون أن نستخدم بها التشفير وإغفال ذكر الهوية. ويعتقد تيمبلتون أن التوقيع الرقمي بين الطرفين في الشبكة والتشفير كفيل بأن يجعل الشبكة آمنة بالكامل، فهو لا يعدو كونه تنظيماً للقوانين، والرخص والبروتوكولات. ولذلك فإنه على الرغم من توقع ازدياد معدل الخطر باستمرار، فإن معدل الحماية الأمنية سيجعل المستخدمين أكثر راحة.

ولذلك فهو يرى أن الجريمة على الإنترنت، على الرغم مما ينشر في وسائل الإعلام

المختلفة بخصوصها وتضخيمها، هي قليلة لحد بعيد، وضئيلة جداً إذا ما قورنت بالجرائم التي تقع وسط السكان، وهي لا يمكن أن تزداد بشكل يهدد مستخدمي الشبكة ويجبرهم على الابتعاد عنها.

ويتوقع جول فور، وهو صحفي الإنترنت المشهور، أن تقوم الحكومة الأمريكية بتقديم المساعدة فيما يتعلق بضمان توفر الخصوصية في الشبكة، من خلال إيجاد طرق للتشفير يصعب حل رموزها. ويتمنى (فير) أن يتوفر له برنامجان أحدهما يتيح له تجاهل الحمقى بالكامل، والآخر يمنع تماماً أي شخص من التنصت على اتصالاته. وهو يعتقد بأن وجود الجريمة على الإنترنت سيستمر، ولكن القدرة على فهم الجريمة وما يحيط بها واتخاذ الإجراءات الملائمة، لمحاربتها سيقللان من الوجود الفعلي لها على الشبكة وبدرجة كبيرة.

وأما مايك مير، مستشار الحاسب المستقل، فيرى أن الأشخاص الذين يدفعون أموالهم لصناعة البرامج، هم الذين سيحددون مقدار الخصوصية التي ستتاح للمستخدمين. وهو يعتقد بأن الجريمة على الإنترنت ستزداد لأن الشبكة ستشهد انطلاقة مماثلة لانطلاقة الفاكس، وأن الجميع سيشرعون في القيام بأشياء كثيرة ومتباينة على الشبكة، ولذلك فإن المزيد من المستخدمين يعني المزيد من انتشار الجريمة على الإنترنت.

وفيما يتعلق بمستقبل الأمن والحماية على الإنترنت، والذي سيؤثر بدوره على مستقبل الجريمة على شبكة الإنترنت وسبل مكافحتها، يقول تيم أوريل مؤسس شركة أوريلي ورئيسها، إن العالم يتجه نحو المزيد من المعاملات التجارية الافتراضية التي تحتاج إلى نوع من إثبات الشخصية والتحقق من الهوية، وهو نظام يجب أن يكون متضمناً داخل البرنامج الذي يستخدم على الشبكة. إلا أن المشكلة الكبرى مع نظام التشفير الجيد أنه ليس مدمجاً في البرامج العادية التي نستخدمها كل يوم، ولذلك فإن الحماية تتطلب أن يكون نظام التشفير متضمناً في البرامج، وهو أمر يمكن القيام به بسهولة كبيرة ما لم تعِقْهُ العوامل السياسية التي تحول دون توفر تقنية التشفير.

ويرى أوريلي أن إثارة المخاوف والتنبيه لخطر الجريمة على الإنترنت اليوم، أمر في غاية الأهمية

للمستقبل، عندما تحصل تفاعلات حقيقية أكثر عفوية بين أشخاص لا رابط فعلي بينهم في العالم المادي. فالشخص يتبادل البريد الإلكتروني مع جميع أصناف البشر الغرباء عنه الذين يتحركون في الدوائر الافتراضية ذاتها التي يتحرك هو فيها، فضلاً عن الذين قد يقابل واحداً منهم في مؤتمر مثلاً في أحد الأيام، ويكون معروفا بالنسبة لأشخاص في نطاق دائرة تحركه، فيكون ذلك بداية لتضليل أشخاص بجعلهم يقابلون آخرين في بيئة ليس لها أي وجود مادي.

أما دان كينغز فله رأي آخر، وهو أنه إذا لم تصبح أجهزة الحاسب أكثر ذكاء من البشر، فلن يتوفر برنامج يجعل منها آمنة ١٠٠٪ مهما كانت قوة ما نستخدمه من طرق تشفير، وكلمات سر، وأنظمة ملفات. ولذلك فهو يعتقد أن مستخدمي الإنترنت الجدد سيكونون دائماً عرضة لأن يصبحوا ضحايا لعمليات الخداع والاحتيال، وأن واجب الجميع هو تبصيرهم بكل ما يمكن أن يجنبهم الوقوع ضحايا لخطر الجريمة على الإنترنت. لأنه عندما يذاع على نطاق العالم أن

أحد الأشخاص قد قام بسرقة مجموعة من البنوك بضربة على لوحة مفاتيح أحد الحاسبات الآلية المرتبطة بالشبكة، فإن كل شخص سيتنبه إلى ذلك ومن ثم يحدث انخفاض في معدل الجريمة على الشبكة.

ولكن آبي فرانكومونت جويليوري مدير مجموعة الأخبار يوزنت لشركة تزكاتليبوكا لا



obeikandl.com

يعتقد أن البرامج هي مشكلة بحجم الأمور الاجتماعية التي يصعب كثيراً حلها، والتي تعد على درجة كبيرة من الخطورة. ويعتقد جويليوري أن الجرائم المرتبطة بشكل كامل بأشياء خاصة

بالإنترنت مثل سرقة كلمات السر أو الاستيلاء على معلومات خاصة، ستظل كما هي. وأما إذا كان المقصود هو استخدام مصادر الإنترنت لارتكاب جرائم حقيقية ليس لها تأثير فعلي على فن استخدام الحاسب، كالخداع والاحتيال الذي يتم عن طريق البريد الإلكتروني مثلاً، فإن هذا النوع من الجرائم سيكون احتمال زيادته كبيراً جداً.

وخلاصة القول هنا حول مستقبل الجريمة على الإنترنت، أن الكثير من عمليات الغش والخداع التقليدية البسيطة التي تعج بها الشبكة ستتضاءل، وتختفي بالتدريج كلما زاد عدد المشتركين في الشبكة وأصبحت هذه الأعمال معروفة لديهم. فعندما يصبح السكان أكثر دراية بشبكة الإنترنت، فإن الغموض فيها والرهبة منها، اللذين يميزانها سيزولان، ولن يكون الناس سريعي التصديق بما يلفق عن الشبكة، وذلك بفضل الخبرات التي اكتسبوها من خلال تعاملهم مع الحواسيب والشبكات.

إلا أنه مع تفاوت درجات المعرفة وتباين القدرات على التعامل مع هذه التقنية المتجددة باستمرار، فإنه سيكون هنالك دائماً أشخاص غير آمنين بسبب ما ينشأ من أنواع جديدة من طرق الخداع الماكرة، لأن من يقومون بأعمال الخداع، ويرتكبون مختلف الجرائم على الشبكة هم دائما أكثر براعة وخبثاً من معظم مستخدمي الإنترنت، ولذلك فإنهم سيسخِّرون جميع مهاراتهم وقدراتهم الفائقة، لابتكار الأسلحة والأدوات اللازمة لمواصلة أعمالهم غير المشروعة على الشبكة وجرائمهم المروعة.

والحل الحقيقي يكمن في وجود القوانين والتشريعات الرادعة والمتفق عليها دولياً، والحرص على تطبيقها على كل من يحاول ارتكاب أي مخالفة على الإنترنت مهما كان حجمها. وذلك هو السبيل الوحيد الذي سيشجع الجميع على نقل الإنترنت إلى واقع حياتهم وأساليب عملهم، والاستفادة من القدرات الهائلة التي تتيحها لهم.

وكمرحلة أولى في اتجاه ذلك يجب على الدول العربية تهيئة نظمها القضائية، لمثل هذا النوع من الجرائم وإعداد القوانين والأنظمة الملائمة لظروف مجتمعاتنا وبيئاتنا. كما تبرز أهمية تقديم البرامج التدريبية المتخصصة للتعامل مع جرائم الإنترنت، وآليات تطبيق القوانين والأنظمة. ولعل ما صدر في المملكة العربية السعودية فيما يخص إصدار نظام مكافحة جرائم المعلوماتية والوارد في الفصل التالي هو من سبيل الاستعداد والاتجاه الصحيح فيما يتجه إليه العالم الآن.

ويهدف هذا النظام الذي بُدئ العمل به إلى حماية المجتمع من جرائم المعلوماتية، واحدّ منها والمساعدة على تحقيق الأمن المعلوماتي، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية، والشبكات المعلوماتية، وحماية المصلحة العامة، والأخلاق والآداب العامة، وحماية الاقتصاد الوطني.



obeikandl.com

# الفصل الثالث عشر :
# القوانين الدولية لمكافحة جرائم الإنترنت

obeikandl.com

إن الجريمة على شبكة الإنترنت تتسم بالدولية لأنها تتخطى حدود كل الدول، بسبب الطبيعة العالمية لانتشار خدمات الإنترنت على نطاق العالم أجمع، فقد انتشرت الجريمة على الإنترنت بدرجة كبيرة، ومازالت السلطات في بلدان كثيرة، مثل: الولايات المتحدة الأمريكية، وبريطانيا، وكوريا، والبرازيل، وغيرها، تتلقى بلاغات عديدة يومياً حول حدوث مثل هذه الجرائم. ولذلك، فإن التعامل معها يختلف من دولة إلى أخرى حسب التشريعات والقوانين السائدة في كل منها، فبعض الدول لديها القوانين التي تتعامل بها مع هذا النوع من الجرائم الجديدة، بينما هناك دول أخرى ليس لها مثل هذه التشريعات والأنظمة القانونية التي تواجهها بها.

وبناء على ذلك، فقد بدأت العديد من الدول خاصة التي لم تبحث أنظمة عقوباتها في مشكلة الجريمة على الإنترنت، في وضع قوانين عقوبات لمحاربة هذا النوع الذي لم يكن معروفا من الجرائم، الذي سيكون مصدر تهديد خطير للشركات والأفراد والمؤسسات من نواحٍ عدة؛ نفسية، واجتماعية، ومادية، وسيكون له تأثير شديد الخطورة على مستقبل شبكة الإنترنت وصناعة تقنية المعلومات بصورة عامة.

ولتجنب اتساع الجريمة وانتشارها على الإنترنت، وخاصة التي يقوم بها المتخصصون والمحترفون في هذا المجال أو الحد منها، فهناك إجماع من قبل مقدمي خدمة الإنترنت ومستخدميها والمعنيين بأمرها من أفراد ودول ومنظمات، على أن الخطوة الأولى لضبط استخدام الإنترنت، والحد من الجريمة فيها، هو وضع تشريع عام لأمن المعلومات فيها، ووجود شرطة مدربة، وقضاة مختصين، وضباط معنيين بتطبيق القانون توكل إليهم مسؤولية منع وقوع الجرائم وحدوث أعمال

مشينة في الشبكة، طالما أن القوانين الجنائية التقليدية لم تعد ملائمة لمعالجة هذا النوع من الجريمة، بسبب صعوبة إثبات عناصر الجريمة من خلالها.

وستقاس فعالية القوانين المشرعة للقضاء على الجريمة في الإنترنت، بمدى النجاح الذي تحققه في مقاضاة المجرمين أو مرتكبي الجرائم والمخالفات، والقضاء على هذه الجريمة الخطيرة المنتشرة في كل المجالات، وسد الثغرات والنقص الذي تعاني منه القوانين والتشريعات الحالية لدى معظم بلدان العالم، حتى المتقدمة منها، في هذا المجال التي تعاني من خطر الجريمة بصورة أكبر من غيرها.

ولقد قامت العديد من الدول بإعادة صياغة التشريعات والقوانين التقليدية، لتشمل الاحتيال عن طريق الحاسب الآلي. وكانت أولى هذه الدول السويد حيث كان قانون البيانات السويدي الصادر في أبريل ١٩٧٣، أول تشريع يعالج مشكلة الاحتيال عن طريق الحاسب. وتلتها في هذا المجال الولايات المتحدة الأمريكية التي أصدرت في الفترة من ١٩٧٦ – ١٩٨٥، قوانين مكافحة جرائم الحاسب التي تشمل كل ما يتعلق بأمور الحاسب من احتيال، وسرقة برامج وخدمات ومعلومات، أو إتلافها والهجوم على المعدات والدخول غير المشروع. ثم جاءت بعد ذلك بريطانيا بقانون مكافحة التزوير والتزييف لعام ١٩٨١م. وتلا ذلك تعديل القانون الجنائي الكندي في عام ١٩٨٥، ليشمل معاقبة المخالفين وتدمير الأجهزة والدخول غير المشروع، واستخدام بطاقات الائتمان، وجميع أنواع البطاقات المستخدمة للبنوك والخدمات الأخرى. وجاء بعد ذلك القانون الدانمركي لعام ١٩٨٥، وهو أول قانون جنائي عن الحاسب الآلي.



obeikandi.com

## ١٣-١ الوضع الحالي

لقد أدى انتشار استخدام الإنترنت على نطاق عالمي إلى صعوبة وضع قواعد وقوانين تحكم استخدامها من قبل الناشرين والمستقبلين. وفي الوقت ذاته لم تستطع القوانين المحلية في كل بلد السيطرة على الناشرين خارج حدودها الجغرافية. فمن أهم خواص الإنترنت أنها لا تتبع لجهة محددة تقع عليها مسؤولية تنظيمها أو التحكم في طريقة عملها أو إصدار التشريعات الخاصة بها. ولذلك لا توجد قوانين محددة متفق عليها ملزمة لجميع مستخدمي الإنترنت. ونتيجة لهذا الفراغ التشريعي وعدم الإجماع الدولي على موقف مجمع عليه لجأت كل دولة أو جهة مرتبطة بالإنترنت إلى وضع القوانين والسياسات الخاصة بها.

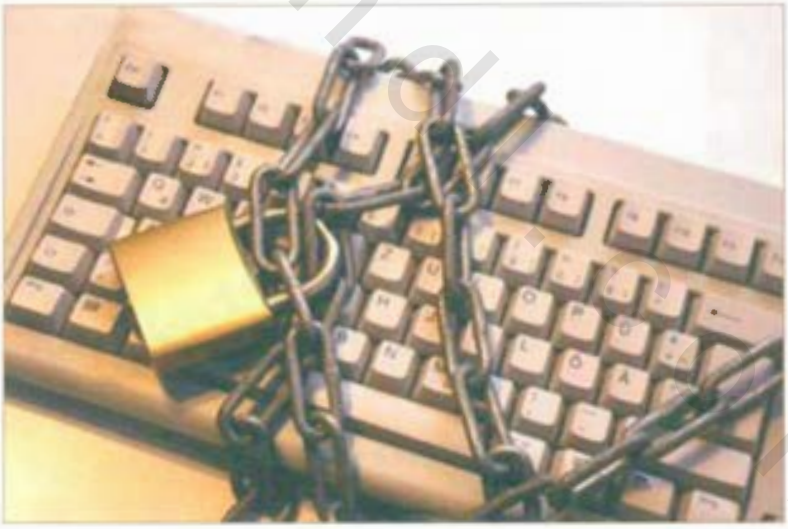
والذي شجع أكثر على ذلك حداثة تقنية الإنترنت وطبيعتها العالمية، فهي تتكون من حاسبات وشبكات منتشرة في مختلف أنحاء العالم. ولذلك، فإن المستخدم يستطيع من أي مكان في العالم الدخول إلى أي معلومات في حاسب آخر أو شبكة حاسبات أخرى مرتبطة بالإنترنت في أي مكان من العالم. وهذا يعني بالطبع وجود حرية كاملة وغير مقيدة في تداول المعلومات على الإنترنت مع تنوع مصادرها وأشكالها ومحتواها. وهو يعني أيضاً إمكانية الحصول على معلومات من موقع تتعارض الأعراف والقيم الاجتماعية السائدة فيه مع قوانين معظم، أو كل دول العالم، مثل: تخصيص مواقع لنشر الرذيلة، والعنف والتمييز العرقي، أو الديني، والإباحية، ولعب القمار، وتجارة المخدرات، والدعاية السياسية، بل أيضا ظهور مواقع تشجع على الانتحار، وجرائم القتل والاغتصاب مقابل أجر يتم الاتفاق عليه، من خلال تلك المواقع التي تديرها عصابات دولية محترفة، تعرض خدماتها لتصفية الخصوم، أو إذلالهم وأهانتهم عن طريق اغتصاب زوجاتهم وبناتهم.

ومن هنا يتساءل كثيرون عن مصير القانون على الإنترنت؟ وهل ستشهد الشبكة محاولات جادة من بعض الحكومات أو الدول جميعها لفرض قوانين وتشريعات محددة على نطاق

دولي؟ وهل ذلك ممكن مع اختلاف قوانين الدول وأعرافها؟

إن الآراء متباينة في هذا الشأن، ولم يطرح أي طرف أجنده محددة لذلك. فبعضهم يرى أن الحاجة أصبحت ملحة لوجود مثل هذا القانون الذي يؤمل أن يتم من خلاله حماية المستخدمين من الأخطار العديدة التي تنطوي عليها شبكة الإنترنت، وعالمها الافتراضي الذي لا يعرف الحدود أو القيود.

ولكن هل تحتاج الإنترنت فعلاً إلى قانون لتنظيمها والتحكم في أنشطتها؟ وهل هذا القانون لا يتناقض مع حرية التعبير لو افترضنا أنه معمول بها في شتى أنحاء العالم؟ إن النقاش في هذا الموضوع ساخنٌ جداً في أجهزة الإعلام، فالناس يتناولون جوانبه المختلفة بحماس شديد، فهناك من يرون تعارضه مع حرية التعبير، وهناك من يعتقدون بأن أنواعاً معينة من الاتصالات يجب عدم السماح بها على الإنترنت، بينما يرى آخرون أنها يشملها التعديل الأول لقانون الاتصالات الأمريكي.



وكذلك يعتقد بعض المختصين أن المراقبة المباشرة على الشبكة ليست هي الأداة التي تقضي على الممارسات الخاطئة أو الجريمة على الشبكة. لأن الشبكة مجرد وسط للاتصالات يتميز

بالسرعة وانخفاض التكلفة، ولذلك لا ينبغي معاقبتها على ما ينشر فيها من مادة غير مقبولة، أو ما ينتشر فيها من جرائم. والقائلون بهذا قد يكونون محقين في ذلك، فالعقاب يجب أن يطال من يقومون بالنشر والترويج ومن يرتكبون الجرائم، ولكن كيف؟ وبأي قانون وأية آلية؟ وهل يصلح القانون الأمريكي، أو الألماني، أو الهولندي، أو الصيني لمعالجة هذه المشاكل؟

ولنأخذ مثلاً لاختلاف القوانين على مستوى العالم وتباينها فيما يتعلق بالإنترنت. فالولايات المتحدة مثلاً تمنع وضع الصور والأفلام الإباحية لمن تقل أعمارهم عن السنّ القانوني، ولكن كثيرين يشاهدونها في مواقع أخرى في العالم، إسبانية كانت، أم روسية أم نرويجية.

وهناك قوانين كثيرة في بلدان عديدة تحظر ممارسة القمار، أو الأعمال غير الأخلاقية، أو ترويج الجريمة، ولكن للأسف هذه القوانين لم يكن لها تأثير كبير وبقيت محصورة ضمن الحدود الجغرافية للبلدان التي فرضتها.

ففي ألمانيا قامت شركة الهاتف الألمانية بقطع الخدمة الهاتفية عن مقدم خدمة أمريكي، بسبب بثه مادة دعائية للنازية في وقت تنشر فيه هذه المواد من قبل دول أخرى وتعد قانونية جداً. وكذلك أوقفت ألمانيا أحد أكبر مقدمي خدمة الإنترنت العالميين، وهو (كوميو سيرف) إلى أن قام بإزالة مئتي مجموعة إخبارية، ولم تكتفِ بذلك بل قامت بملاحقة المدير المحلي للشركة قضائياً بتهمة علمه بمرور المعلومات الممنوعة.

وفي خطوة أكبر من ذلك دعا البرلمان الأوربي إلى تحرك عالمي لضبط تبادل المواد الإباحية والعنصرية على الإنترنت، ودعا إلى تكوين (شرطة للإنترنت)، ووضع اتفاقيات دولية لمحاكمة من يسيئون استخدام الإنترنت، مركّزاً على ضرورة الاتفاق على معايير لتحديد المواد والاستخدامات غير المرغوب فيها على الشبكة.

وفي ماليزيا، حدد القانون أقل عمر لمستخدم الإنترنت بخمسة وعشرين عاماً. وفي الصين يتطلب استخدام الإنترنت تصريحاً من الشرطة. وفي دولة الإمارات العربية المتحدة

شكلت لجنة من الشرطة، ووزارة الإعلام، ومؤسسة الإمارات للاتصالات، وجامعة الإمارات، لوضع إستراتيجية قومية لاستخدام شبكة الإنترنت عندما اعترف مقدم الخدمة الرئيس بصعوبة التحكم بالشبكة.

وفي دبي طالبت الشركة المقدمة لخدمة الإنترنت علناً برقابة أفضل على الإنترنت. أما في سنغافورة فالإنترنت تصنف على أساس أنها وسيلة بث إعلامية، ومن ثم تخضع للرقابة الإعلامية عند نشر معلومات سياسية أو دينية.

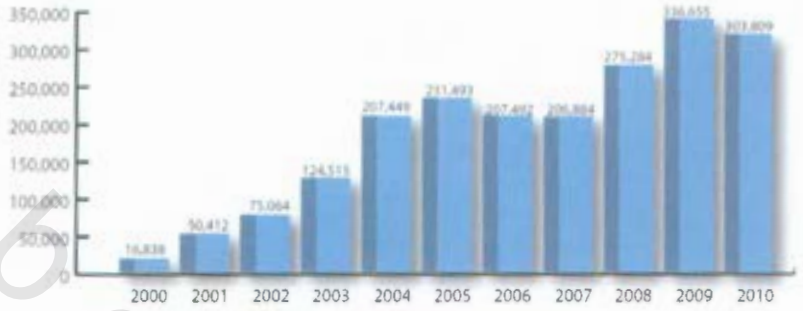
ومع وجود كل هذه الاختلافات، فهناك إجماع عام على ضرورة حماية الأطفال، والحيلولة دون دخولهم إلى المواقع الإباحية، والحد من الجريمة على الشبكة أياً كان نوعها، وخاصة في الدول الإسلامية.

وعلى الرغم من عدم وجود تسجيل دقيق لجرائم الحاسب على نطاق العالم، فتشير التقارير المتداولة والمعلومات المتوفرة إلى أن جرائم الحاسب في تزايد مستمر.

فكما جاء في تقرير مركز شكاوى الإنترنت لعام ٢٠٠٨، أنه في الفترة من ١ يناير ٢٠٠٨ -- ٣١ ديسمبر ٢٠٠٨ ، كان هناك (٢٧٥٢٨٤) من الشكاوى التي وردت إلى (IC٣). الذي يشكل زيادة (٣٣,١ ٪) بالمقارنة مع عام ٢٠٠٧، الذي ظهرت به شكاوى عددها (٢٠٦٨٨٤). ومع تتبع هذه البيانات التي بدأت في عام ٢٠٠٠، وسجلت شكاوى عددها (١٦٨٣٨). ومنذ ذلك الحين، تضاعفت الشكاوى في كل عام وصولاً إلى عام ٢٠٠٤ ، عندما بلغت الشكاوى (٢٠٧٤٤٩). ومن عام ٢٠٠٤ حتى عام ٢٠٠٧، ظلت حول نفس النسبة . وفي عام ٢٠٠٨، كان هناك تصاعد من جديد إلى ما يقرب من (٧٥٠٠٠) شكوى التي شكلت ما مجموعه (٢٧٥٢٨٤). وقفزت في عام ٢٠٠٩م، إلى (٣٣٦،٦٥٥) غير أنها تراجعت في العام ٢٠١٠م إلى (٣٠٣،٨٠٩) شكاوى. ويوضح الرسم البياني الآتي في الشكل



openkandil.com




شكل١٣-١: يوضح الزيادة المطّردة في عدد بلاغات جرائم الإنترنت وشكاواها

وتعد الزيادة في عدد جرائم الحاسب نتيجة طبيعية لاستخدام الحاسب في المجتمع الأمريكي على نطاق واسع وفي جميع المجالات. واختراع الحاسب مثلُه كغيره من الاختراعات، فتح الأبواب أمام مجرمين لسرقته، أو لاستخدامه في تسهيل القيام بجرائم أخرى. فالحاسب قد يكون أداة للهجوم عندما يستخدمه أحد الأشخاص ليسهل عليه ارتكاب بعض الجرائم التقليدية كالغش، باستخدام أحد البرامج لسرقة الأموال من حسابات المودعين مباشرة. أو خزن السجلات المتعلقة بتجارة المخدرات بدلاً عن الاعتماد على نظام الدفاتر القديمة.

وعلى الرغم من أن أجهزة الحاسب قد تكون في بعض الأحيان ثانوية في ارتكاب الجريمة، فهي مهمة جداً بالنسبة للجهات المعنية بتطبيق القانون لأنها تحوي أدلة على الجريمة.

ولقد أثارت الطرق المختلفة التي يستخدم بها المجرمون الحاسب نقاشاً فلسفياً بين المعنيين، بتطبيق القانون في الولايات المتحدة الأمريكية. فبعضهم يحاول إقناع الآخرين بأن جرائم الحاسب هي مجرد جرائم تقليدية يتم ارتكابها، بمعدات جديدة ذات تقنية عالية. ولكن آخرين يصرون على خلاف ذلك رافضين مساواة جرائم الحاسب بالجرائم التقليدية، انطلاقاً من أن مقاومتها تتطلب وجود أساليب مبتكرة لتطبيق القانون وإصدار قوانين جديدة خصيصا لمواجهة



obeikandl.com

سوء استغلال التقنيات الحديثة.

ففي عام ١٩٨٤، تبنى الكونغرس وجهة النظر الأخيرة، وسنَّ تشريعاً منفصلاً لمواجهة الجريمة في المجالات الإلكترونية. وبما أن بعض جرائم الحاسب وجدت أصلاً في التقنيات الحديثة، فيجب مقاومتها بقانون خاص. فمثلاً التخريب الواسع الذي يحدث بسبب إطلاق الفيروسات في شبكات الحاسب العالمية لا يمكن القضاء عليه أو الحد منه بطريقة فعالة من خلال الاعتماد على قانون عام لتشريعات مكافحة الجريمة. فهل كان من الممكن أن يحاكم مثل من حوكموا بسبب إطلاق الفيروسات، كروبرت موريس المسؤول عن إطلاق دودة موريس وتعطيل حوالي (٦٠٠٠) حاسب آلي على نطاق العالم، أو الهاكر الأعظم كيفن ميتنك، أو غيره من مرتكبي الجريمة على الإنترنت ما لم يكن الكونغرس قد أصدر قانون مكافحة الغش وسوء استخدام الحاسب؟

ولإعطاء صورة واضحة عن نوعية التشريعات والقوانين الخاصة بالإنترنت، وحجم الخطر الذي تواجهه، سنناقش هذا الموضوع على ضوء ما يجري في الولايات المتحدة الأمريكية بوصفها المؤسس لشبكة الإنترنت، وأكثر بلدان العالم استخداماً لتقنية المعلومات وأجهزة الحاسب وتعرضاً لجرائم هذه التقنية.

وإن جرائم الحاسب، سواء وصفت بأنها جرائم قديمة أو جديدة كلياً، فهي تتسبب في حدوث مشاكل لا حصر لها للجهات المعنية بتطبيق القانون، واحتواء الخطر على الصالح العام في الولايات المتحدة. وأصعب ما قد تواجهه الجهات المشرعة هو وضع التشريعات المتعلقة بنقل التقنية من شيء مادي إلى بيئة غير ملموسة كبيئة الإنترنت، وإلى صيغ إلكترونية غير محسوسة. فهل يمكن أن تخضع الجرائم التي ترتكب بواسطة أجهزة الحاسب على الشبكة للضوابط أو القوانين العادية المعمول بها؟

إن جرائم السرقة والأذى كانت في السابق لها حدود مادية، فاللص يمكنه في ليلة واحدة اقتحام عدة منازل، ولكنه لا يستطيع أن يأخذ إلا أشياء محدودة. ولكن في عصر المعلومات



obeikandi.com

والأجهزة والشبكات المرتبطة بالإنترنت لم تعد الحدود المادية لها وجود. فقد أصبح بإمكان المجرم الاستيلاء على المعلومات المخزونة، من أي جهاز حاسب مرتبط بشبكة يمكن الوصول إليها عن طريق الاتصال بالهاتف في أي مكان في العالم. ومن ثم، فإن كمية المعلومات المسروقة أو مقدار الضرر الذي يحدثه المهاجم بواسطة شيفرة برمجية ذكية لا يحد منه إلا سرعة الشبكة، ونوعية معدات الحاسب الخاصة بالمجرم. وبالطبع فإن هذه الجرائم والسرقات يمكن أن تحدث داخل أي بلد وعبر حدوده.

وفي واقع الأمر، إن الانتقال الواضح إلى بيئة غير مادية وبلا حدود، كشبكة الإنترنت، وزيادة تعرض المعلومات إلى خطر السرقة وتحويلها إلى صيغ إلكترونية، يجعل من الصعوبة بمكان مواجهة هذا الواقع اعتماداً على قوانين قديمة أعدت أساساً لحماية الممتلكات المادية فقط. والأمثلة على ذلك كثيرة، فالتشريع الخاص بنقل الممتلكات المسروقة بين الولايات الأمريكية، مثلاً: )البند رقم ٢٣١٤ من المادة ١٨ USA)، يتحدث عن البضائع والأدوات والتجارة، ومن ثم فهو كما وصفته عدة محاكم في ولايات مختلفة لا ينطبق على الممتلكات غير المادية. وبالطريقة ذاتها، فإن قانوناً مثل قانون الابتزاز الأمريكي مثلاً، والمعروف منذ فترة طويلة يجعل العنف المادي الذي يهدد الممتلكات غير قانوني. فالتهديد بتفجير قنبلة في مبنى مثلاً يقع تحت طائلة هذا القانون، ولكن التهديد بحذف ملف لم يكن أصلاً وارداً في تصور واضعي القانون.

ولمواجهة مشكلة جرائم الحاسب المتنامية في الولايات المتحدة ومختلف أنحاء العالم، فقد اتفقت آراء معظم الذين تناولوا هذه المسألة بالدراسة على منهجين للمواجهة. الأول: يقوم على مراجعة جميع القوانين المتعلقة بهذا الموضوع في الولايات المتحدة للتعرف على كل تشريع، يمكن أن يتأثر فعلياً باستخدام التقنيات الحديثة للحاسوب، وأنظمة المعلومات وتعديله بالصورة المناسبة. والثاني: هو تركيز التعديلات الأساسية على قانون مكافحة الخداع، وسوء استخدام الحاسب الناجم عن استخدام التقنيات الحديثة.

ولقد أقر المشرعون في الولايات المتحدة المنهج الثاني للمواجهة، وهو تركيز التعديلات

الأساسية على قانون مكافحة الخداع وسوء استخدام الحاسب لأسباب عديدة، منها: أن الولايات المتحدة قد استمرت تواجه المسائل الجوهرية لأمن المعلومات على المستويين المحلي والدولي بتشريع واحد يتعلق بالمحافظة على سرية المعلومات والأنظمة وسلامتها وتوفرها، لأن هذه الموضوعات ( السرية، والسلامة، والتوفر) تُعدُ القاعدة الأساسية للتعاون والنمو الاقتصادي لأية منظمة، والموجّهَات الرئيسة لأمن المعلومات، حسب ما هو وارد في (مسودة المبادئ) الخاصة بتوفر المعلومات السرية واستخدامها (رقم ٤٣٦٢ بتاريخ ٢٠ يناير ١٩٩٥). ولذلك فإن الولايات المتحدة الأمريكية تكون من خلال تكييف قانون مكافحة أعمال الخداع وسوء استخدام الحاسب مع موجهات أمن أنظمة الحاسب، قد بدأت بإعادة التفكير في كيفية مواجهة جرائم تقنية المعلومات، وفي الوقت ذاته حماية السرية والمحافظة على سلامة المعلومات وأنظمتها وضمان توفرها.

إن تبني هذا الخيار من قبل الولايات المتحدة سيؤدي إلى تشجيع دول أخرى على اتباع أطر عمل مماثلة، ومن ثم إيجاد طريقة أكثر شمولاً واتساعاً لمواجهة خطر جرائم الحاسب والشبكات على البنية التحتية العالمية الحالية للمعلومات. وبذلك تكون الولايات المتحدة قد وفرت نقطة مرجعية واحدة للمحققين والمدعيين العامين والمشرعين، وهي المادة (٣٠) من قانون مكافحة الخداع وسوء استخدام الحاسب، ليستندوا عليها في تحديد ما إذا كان سوء استخدام معين للتقنية الجديدة يشمله، أو لا يشمله، قانون الجريمة الاتحادي.

وبما أن قانون الجريمة يتطلب إعادة نظر كلما دخلت تقنيات جديدة مجال الاستخدام، فإن عملية الموالفة الدقيقة للمادة (٣٠) من القانون قد تكون ملائمة جداً، بحيث لا يصبح من الضروري البحث المستمر في مدونة القوانين الأمريكية بكاملها.

إن هذا القانون سيوفر فهماً أفضل لحدود جريمة الحاسب والشبكات وأبعادها، ويتيح إمكانية الحصول على إحصائيات أكثر موثوقية فيما يتعلق بسوء استخدام الحاسب.

ويمكن أن تتم محاكمة جرائم الحاسب بموجب هذا القانون، وتحت تشريعات مكافحة



onekanoon.com

الجريمة المسمى (A Host Criminal Statute) ومن المحتمل جداً أن ينجح هذا الوضع في الحد من الجريمة إذا اعتمدت الولايات ا لمتحدة طريقة المزج بين القوانين، وقامت بتعديل الشروط المختلفة للمادة (١٨) لتشمل جرائم الحاسب الجديدة لأن وجود تفسيرات وتطبيقات مختلفة للقانون سيؤدي إلى تفاقم مشكلة موجودة أصلاً.

## ١٣-٢ مشكلة تأخر المحاكمات في جرائم الإنترنت

إن عقد المحاكم لمحاكمة المتهمين في جرائم الإنترنت يتأخر كثيراً بسبب تعقد نوعية القضايا، وقلة عدد الذين يتمتعون بخبرة في هذا المجال من القضاة وممثلي الاتهام، والأمثلة على ذلك كثيرة. فلقد استغرق الأمر أربع سنوات وخمسة أشهر لينتقل الهاكر المشهور (كيفن ميتنك) من مرحلة الاعتقال بتهمة الاحتيال، إلى مرحلة قضاء العقوبة. وقد تم ذلك دون محاكمة كافية. فهذا الهاكر الذي حُكم عليه بموجب هذه التهمة في اليوم الثامن من شهر آب/ أغسطس من عام ١٩٩٩بعقوبة سجن مدتها ستة وأربعون شهراً، والذي أطلق سراحه في بداية عام ٢٠٠٠، ليس هو الوحيد الذي عانى من هذه المسألة. فالهاكر كيفن بولسن، هو الآخر قد اعتقل في عام ١٩٩١، وظل محتجزاً في السجن لمدة تزيد عن العام ونصف العام، قبل أن توجه إليه وزارة العدل الأمريكية تهمة التجسس، التي رفضتها المحكمة مؤخراً. ولكنه في آخر الأمر أمضى خمس سنوات وشهرين دون محاكمة. وفي صفقة مع هيئة الاتهام اعترف بتهمة واحدة هي إجراء محادثة لاسلكية للفوز بسيارة بورش.



obeikandl.com

وقد كان التأخير الطويل في هاتين الحادثتين الشهيرتين بالرغم من عدم ارتباطهما ببعضهما يعزى جزئياً إلى وجود كميات هائلة من الأدلة المعقدة. وقد أثبتت دراسة حديثة أن عالم الجريمة ذات التقنية العالية يكون في كثير من الأحيان معقداً جداً إلى درجة يصعب على ممثلي الادعاء التعامل معه بصورة مناسبة، وهي حقيقة كانت نتيجتها القيام بعمليات تفتيش واعتقال وتعطيل غير لازم للمحاكمات.

وقد ذكر ديفيد بانيسار أحد العاملين في مركز (خصوصية المعلومات الإلكترونية) أنه: «لا يوجد كثير من المحامين الذين يتولون الدفاع في جرائم الحاسب، ولا المدعون العامون، أو ممثلو النيابة، الذين يتمتعون بالخبرة الواسعة في هذا المجال». ويقول أيضاً: «إنه في بعض الأحيان يكون الشخص الوحيد المؤهل لمناقشة هذه المسائل التقنية هو المتهم نفسه، والذي لن يصدقه أحد على كل حال».

## ١٣-٣ كثرة الاعتقال وقلة المحاكمات

وجد ديفيد بانيسار من خلال المعلومات التي حصل عليها من وزارة العدل الأمريكية بموجب حرية المعلومات، أن (٤١٩) قضية من قضايا الاحتيال بالحاسب قد أحيلت إلى المدعين العامين الاتحاديين بسبب نقص الأدلة. وهو وضع يدل على وجود مشكلة حقيقية فيما يتعلق بتطبيق القانون في هذا المجال.

وتدل الإحصائيات على أن معدل الاتهام قد ظل ثابتا منذ عام ١٩٩٣، على الرغم من



obeikandl.com

تضاعف عدد القضايا ثلاث مرات. ففي كل عام يتم استبعاد ما بين ٦٤٪ - ٧٨٪ من قضايا الاحتيال بالحاسب، أو إرسالها إلى الولايات للمقاضاة.

وهذا يعني أن الشرطة تحصل على ضمانات بحث للتحري في الجرائم المزعومة، والقيام بالاعتقالات اللازمة في قضايا أضعف من أن تتم المقاضاة فيها على المستوى الاتحادي. وقد ذكر بانيسار أنه: «كما يوجد العديد من الجرائم الأخرى، فهناك عدد كبير من المخالفات الفنية للقانون التي يجب إيقافها بطرق أخرى». ولكن ينبغي أخذ الأمر بالحجم المعقول، وعدم المبالغة فيه، وهو يعطي مثالاً على ذلك قائلاً: «إذا كان كل شخص يتجاوز السرعة القصوى المحددة في الساعة بميل واحد يتم توقيفه، فإن البلد لا محالة ستتحول إلى دولة بوليسية». وهو يدعو إلى إيجاد الحلول اللازمة لهذه المشكلة القانونية والتقنية في الوقت ذاته.

## ١٣-٤ حلول مقترحة

أول هذه الحلول لهذه المشكلة هو تثقيف الشرطة وممثلي الادعاء في المسائل التقنية الخاصة بهذا المجال، وهو أمر يتطلب في أحسن الأحوال كثيراً من الجهد والمثابرة. ومع ذلك فإن إدارة الرئيس كلينتون التي أصدرت سلسلة من الأوامر الإدارية، وقدمت كثيراً من الاقتراحات حول الجريمة على الإنترنت، اتهمها البعض بأنها تحاول تقليص الخصوصية على الشبكة حتى يتسنى لها تنفيذ قوانين يصعب حتى تطبيقها في العديد من الحالات. ففي السادس من شهر آب/ أغسطس من عام ١٩٩٩، وقّع الرئيس كلينتون أمراً تنفيذياً بتكوين مجموعة عمل بمستوى استشاري لتقرر ما إذا كانت القوانين الحالية كافية للبت في قضايا جرائم الإنترنت. وقد كلفت المجموعة أيضاً بالبحث في التقنيات والأساليب والسلطات القانونية الجديدة التي يمكن أن تساعد الشرطة في محاربة الجريمة على الشبكة. وقد قوبل الجزء الأخير من هذا الأمر التنفيذي

الذي أصدره الرئيس الأمريكي بسيل من الانتقادات، بدعوى أنه ذريعة مغلفة لعودة صكوك التنفيذ، وفتح باب خلفي لفرض تنفيذ القانون، للحصول على مفاتيح حل شيفرة ما يسمى ببرامج التشفير القوية.

ومع ذلك فإن مسؤولاً إدارياً على صلة لصيقة بمجموعة العمل صرح بأن التشفير لن يدخل ضمن التحريات التي تقوم بها المجموعة، وأن الأمر يتعلق فقط باستخدام القوانين والأدوات الحالية بطرق جديدة. وهو يركز على الاعتماد على التنظيم الذاتي أكثر من إعطاء سلطات إضافية للشرطة.

وبالإضافة إلى محاولات إدارة الرئيس كلينتون إصدار قوانين تنفيذية جديدة، فإن وزارة العدل ومكتب التحقيقات الاتحادي (FBI) ووزارة الدفاع ووكالة الأمن الوطني تسعى جميعها إلى طلب زيادة في ميزانياتهم لمحاربة جرائم الإنترنت، ومواجهة حرب المعلومات، على الرغم من حقيقة أن أقل من ربع القضايا التي وصلت إلى السلطات الاتحادية قد تم إصدار أحكام فيها في نهاية الأمر، وهو ما تزعم الانتقادات الموجهة إلى ما تقوم به إدارة الرئيس كلينتون في هذا المجال بالإضافة إلى ما تسعى إليه هذه الوزارات والإدارات من انهماك في إنشاء إمبراطورية باستخدام تهديد مبطن باللجوء إلى إعداد برامج جديدة وبسط نفوذ إداراتها. وكان نائب وزير الدفاع جون هامري الذي وصف الهجوم الذي تعرض له مقر وزارة الدفاع الأمريكية في شهر فبراير من عام ١٩٩٨، بأنه أعنف هجوم قضائي واجهه المقر حتى الآن، قد استطاع إقناع الكونغرس بتخصيص مزيد من الأموال لمحاربة إرهاب الشبكة. وقد تم ذلك حتى بعد اكتشاف أن الهجمات قد قام بها ثلاثة مراهقين أحدهما إسرائيلي عمره ١٨ سنة، والآخران مراهقان من كاليفورنيا يستخدمان ثغرة معروفة على نطاق واسع في نظام تشغيل الحاسب. وهو شبيه بالوضع الذي يحدث الآن بخصوص فرض تنفيذ القوانين دون استخدام الإجراءات الوقائية الصحيحة، والخبرات المناسبة في مجال الحاسب. ولذلك فإن المسؤولين يستطيعون من خلال

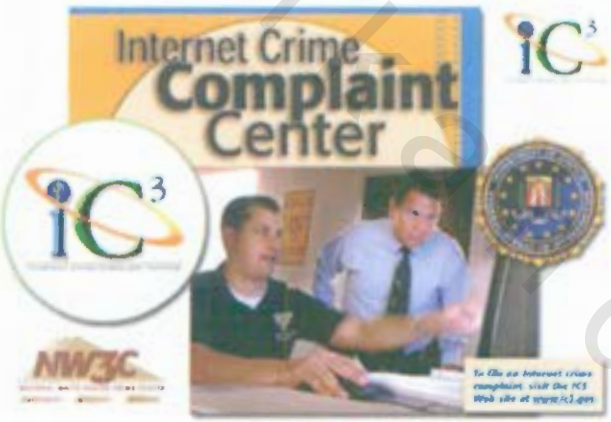


obeikandl.com

استخدام المزيد من الأموال القيام بمزيد من الاعتقالات في مجال الجريمة المرتبطة بالإنترنت وأجهزة الحاسب.

ومع ذلك فإن العدد الفعلي للمحاكمات والإدانات حسب بيانات ديفيد بانيسار ستظل كما هي.

## ١٣- ٥ مركز الشكاوى الخاصة بجرائم الإنترنت (IC3)




إن مركز الشكاوى الخاصة بجرائم الإنترنت (IC3) هو كناية عن نظام تبليغ وإحالة شكاوى الناس في الولايات المتحدة والعالم أجمع ضد جرائم الإنترنت. ويقدم المركز استمارة للشكاوى مرسلة على الإنترنت، ويقوم المركز بواسطة فريق من الموظفين والمحللين، بخدمة الجمهور ووكالات فرض تطبيق القوانين الأميركية والدولية التي تحقق في جرائم الإنترنت.

وقد نشأ مركز الشكاوى الخاصة بجرائم الإنترنت كمفهوم سنة ١٩٩٨م، بإدراك أن الجريمة بدأت تدخل الإنترنت لأن الأعمال التجارية والمالية كانت قد بدأت تتم عبر الإنترنت، ولأن مكتب التحقيقات الفدرالي أراد أن يكون قادراً على تعقب هذه النشاطات وعلى تطوير تقنيات تحقيق خاصة بجرائم الإنترنت.

ولم يكن هناك آنذاك أي مكان يمكن للناس التبليغ فيه عن جرائم الإنترنت، وأراد مكتب التحقيقات الفدرالي التمييز بين جرائم الإنترنت والنشاطات الإجرامية الأخرى التي تُبلّغ عنها عادةً الشرطة المحلية، ومكتب التحقيقات الفدرالي، والوكالات الأخرى التي تطبق القوانين الفدرالية، وهيئة التجارة الفدرالية (FTC)، والمكتب الأميركي للتفتيش البريدي (USPIS)، وهو الشعبة التي تطبق القوانين المتعلقة بمصلحة البريد الأميركية، وغيرها من الوكالات.

وقد تم تأسيس أول مكتب للمركز سنة ١٩٩٩ بولاية وست فرجينيا، وسمّي مركز شكاوى الاحتيال على الإنترنت. ومثّل المكتب شراكة بين مكتب التحقيقات الفدرالي والمركز القومي لجرائم موظفي المكاتب، وهذا الأخير مؤسسة لا تبغي الربح متعاقدة مع وزارة العدل الأميركية مهمتها الأساسية تحسين قدرات موظفي أجهزة تطبيق القانون، بهدف اكتشاف جرائم الإنترنت أو الجرائم الاقتصادية ومعالجة أمرها.

وفي العام ٢٠٠٢، وبغية توضيح نطاق جرائم الإنترنت التي يجري تحليلها، بدءاً من الاحتيال البسيط إلى تشكيلة من النشاطات الإجرامية التي أخذت تظهر على الإنترنت، وأعيدت تسمية المركز فأطلق عليه اسم مركز الشكاوى الخاصة بجرائم الإنترنت، ودعا مكتب التحقيقات الفدرالي وكالات فدرالية أخرى، مثل: مكتب التفتيش البريدي، وهيئة التجارة الفدرالية، والشرطة السرية، وغيرها، للمساعدة في تزويد المركز بالموظفين، وللإسهام في العمل ضد جرائم الإنترنت.

وقد أصبح هناك اليوم في مركز الشكاوى القائم بولاية وست فرجينيا، ستة موظفين فدراليين وما يقرب من أربعين محللاً من القطاع الأكاديمي، وقطاع صناعة الكمبيوتر، وخدمات الإنترنت، يتلقون الشكاوى المتعلقة بجرائم الإنترنت من الجمهور، ثم يقومون بالبحث في الشكاوى، وإعداد ملفها، وإحالتها إلى وكالات تطبيق القانون الفدرالية والمحلية والتابعة للولايات، وإلى أجهزة تطبيق القانون الدولية، أو الوكالات التنظيمية، وفرق العمل التي تشارك



obeikandl.com

فيها عدة وكالات، للقيام بالتحقيق فيها.

ويمكن للناس من كافة أنحاء العالم تقديم شكاوى بواسطة موقع مركز الشكاوى الخاصة بجرائم على الإنترنت (gov.http://www.ic٣). ويطلب الموقع اسم الشخص وعنوانه البريدي ورقم هاتفه؛ إضافة إلى اسم، وعنوان، ورقم هاتف، والعنوان الإلكتروني- إذا كانت متوفرة- للشخص، أو المنظمة، المشتبه بقيامه بنشاط إجرامي؛ علاوة على تفاصيل تتعلق بكيفية وقوع الجريمة حسب اعتقاد مقدم الشكوى ووقت وقوعها وسبب اعتقاده بوقوعها؛ بالإضافة إلى أي معلومات أخرى تدعم الشكوى.

وكما جاء في موقع الحكومة الأمريكي www.america.gov/ar أن مركز الشكاوى الخاصة بجرائم الإنترنت، يعمل أيضاً مع منظمات دولية، مثل: هيئة الجرائم الاقتصادية والمالية (EFCC) في نيجيريا، حيث توجد مستويات عالية من الجرائم الاقتصادية والمالية كتبييض الأموال، والاحتيال بقبض أموال مسبقة لمشاريع وهمية، أو ما يسمى احتيال ٤١٩، مما كانت له عواقب سلبية شديدة على ذلك البلد.

وتجمع جريمة احتيال ٤١٩، التي أطلق عليها اسمها لخرقها الفقرة ٤١٩ من مدونة القوانين الجنائية النيجيرية، ما بين جرم انتحال الشخصية وتشكيلة متنوعة من مؤامرات قبض الأموال مسبقاً لمشاريع وهمية. فالضحية المحتملة تتلقى رسالة، أو رسالة إلكترونية، أو فاكس، من أشخاص يدعون أنهم موظفون حكوميون نيجيريون أو أجانب، يطلبون فيها المساعدة في إيداع مبالغ طائلة من المال في حسابات في مصارف خارجية، عارضين حصة من الأموال مقابل ذلك. ويعتمد المخطط على إقناع الضحية الراغبة في التعاون بإرسال مبلغ من المال إلى كاتب الرسالة على دفعات لأسباب متنوعة.

وقد أدى خطر هذه الجرائم في نيجيريا إلى تأسيس لجنة الجرائم الاقتصادية والمالية هناك. وخلال السنة الماضية، قام مركز الشكاوى الخاصة بجرائم الإنترنت بعدة عمليات جديدة صودرت فيها بضائع، وتم إلقاء القبض على أشخاص في أفريقيا الغربية، نتيجة لهذا التحالف بين

المركز ولجنة الجرائم الاقتصادية والمالية، ونتيجة لتحالفات أخرى.

ويعمل مركز الشكاوى عن كثب أيضاً مع المنظمة الكندية المسماة؛ )الإبلاغ عن الجرائم الاقتصادية على خط الإنترنت) (RECOL) . ويدير هذه المنظمة المركز القومي للجرائم المكتبية في كندا، وتدعمها شرطة الخيالة الملكية الكندية، ووكالات أخرى. وتنطوي منظمة الإبلاغ عن جرائم الإنترنت على شراكة متكاملة بين وكالات تطبيق القوانين الدولية والفدرالية والإقليمية من جهة، وبين المسؤولين عن وضع أنظمة العمل وتطبيقها، والمنظمات التجارية الخاصة التي لها مصلحة تحقيقية مشروعة في تلقي شكاوى الجرائم الاقتصادية، من جهة أخرى.

وهناك مجموعة متنامية من الوكالات الدولية المنخرطة في محاربة جرائم الإنترنت. ويعمل مركز الشكاوى الخاصة بجرائم الإنترنت مع المسؤولين عن تطبيق القانون في بلدان عديدة، بينها أستراليا والمملكة المتحدة. كما يحضر ممثلو مركز الشكاوى أيضاً اجتماعات دورية للمجموعة الفرعية حول جرائم التقانة المتقدمة التابعة لمجموعة الثماني (كندا، وفرنسا، وألمانيا، وإيطاليا، واليابان، وروسيا، والمملكة المتحدة، والولايات المتحدة). ويعمل قسم من هذه المجموعة الفرعية على محاربة جرائم الإنترنت وتعزيز التحقيقات بشأنها.

ويشكل مشروعا مركز الشكاوى الخاصة بجرائم الإنترنت (IC3)، ووحدة مبادرات جرائم الإنترنت ودمج مواردها (CIRFU)، فريق عمل متطور ومتقدم باستمرار. وفي أثناء هذا التقدم، يراجع موظفو ومحللو مركز الشكاوى ما أثبت نجاحه وما ثبت فشله من إجراءات، ويسعون باستمرار لتأمين مساعدة الخبراء والمصادر التي تزودهم بمعلومات استخباراتية، ليصبحوا أكثر فطنة بخصوص جرائم الإنترنت، ولكي يتعلموا كيف يمكنهم محاربتها بصورة أكثر فعالية.



obeikandi.com

## ١٣-٦ المركز الوطني الإرشادي لأمن المعلومات

يعمل المركز الوطني الإرشادي لأمن المعلومات بهيئة الاتصالات وتقنية المعلومات، على رفع مستوى الوعي والمعرفة بأخطار أمن المعلومات ويقوم بالتعاون مع أعضائه وشركائه على تنسيق جهود الوقاية والتصدي للأخطار والحوادث المتعلقة بالأمن الإلكتروني في المملكة العربية السعودية. ومن ضمن أهداف المركز أيضاً؛ رفع مستوى الثقة في التعاملات الإلكترونية، فضلاً عن تقديم المشورة والنصح للأفراد وللمؤسسات في ما يتعلق بأمن المعلومات.


شكل ١٣-٢ المركز الوطني الإرشادي لأمن المعلومات



obeikandl.com

## ١٣-٧ مركز التميز لأمن المعلومات

قامت وزارة التعليم العالي بإنشاء وتمويل مركز التميز لأمن المعلومات بجامعة الملك سعود، بهدف جمع أفضل الباحثين و المتميزين في أمن المعلومات لنقل الخبرة وتوجيه الأبحاث في هذا المجال، لتقييم وحل المشاكل الوطنية في أمن المعلومات. ويهدف المركز إلى الاستثمار في الخبرات الوطنية من خلال التعاون الدولي والداخلي مع الجامعات ومراكز الأبحاث و الشركات لحل المشاكل المختصة بأمن المعلومات ونقل الخبرات وتقديم برامج تعليمية وتثقيفة متميزة ومبدعة تشجع على التخصص في أمن المعلومات وتحذر من المخاطر الأمنية. انظر شكل ١٣-٣ مركز التميز لأمن المعلومات.


شكل ١٣-٣ مركز التميز لأمن المعلومات

## ١٣-٨ كرسي سمو الأمير مقرن لتقنيات لأمن المعلومات

مع التواصل والعولمة المعلوماتية المتصاعدة عبر الإنترنت، باتت قضية (أمن المعلومات) أولوية رئيسة لحماية الأمن الوطني والعالمي في هذا العصر.ومن هذا المنطلق جاءت مُبادرة صاحب السمو الملكي الأمير مقرن بن عبد العزيز، بتمويل كرسي بحثي في مجال (تقنيات أمن المعلومات) في جامعة الملك سعود. ويطمح الكرسي إلى أن تكون نشاطاته متفاعلة مع مُتطلبات تقنيات أمن المعلومات على المستوى الوطني من جهة، ومع التطور العلمي الذي يشهده العالم في مجالاتها من جهة أخرى ويهدف إلى تحقيق إنجازات في البحث العلمي، وتطوير منتجات تقنية تختص بأمن المعلومات، إضافة إلى تقديم الاستشارات المتخصصة بواسطة عدد من الخبراء المحليين والدوليين.


شكل ١٣-٤ كرسي الأمير مقرن لتقنيات لأمن المعلومات.



obeikandl.com

# ١٣-٩ نظام مكافحة الجرائم الإلكترونية في المملكة العربية السعودية

أثبتت الإحصائيات تصدر المملكة العربية السعودية المركز الأول على مستوى دول الخليج العربي في التعرض للجرائم الإلكترونية وذلك وفقاً لما ذكرته شركة (ترينـد مايكرو) إلى وجود أكثر من (٧٠٠) ألف حالة انهيار نظامي خلال تسعة شهور فقط في السعودية بنسبة ٦٤٪.

مما أدى إلى اهتزاز الثقة بالتعامل الإلكتروني عبر الإنترنت مما يحتم وجود قانون مكافح لمثل هذه الجرائم. وعليه فإن مجلس الوزراء السعودي أقر في جلسته يوم الاثنين ٧ ربيع الأول ١٤٢٨هـ، برئاسة خادم الحرمين الشريفين الملك عبد الله بن عبد العزيز – حفظه الله – نظام مكافحة جرائم المعلوماتية، بتحديد الجرائم والعقوبات المقررة لها للحد من نشوءها. وتتجاوز مجموع العقوبات المالية الواردة في النظام مبلغ (١١) مليون ريال، موزعة بالتفاوت المبني على فداحة الجرم الالكتروني المرتكب.

## ١٣-٧-١ أبرز مواد نظام مكافحة الجرائم الإلكترونية :

**المادة الثالثة:**

في هذه المادة يعاقب الشخص بالسجن لمدة سنة وبغرامة خمسمائة ألف ريال إذا ارتكب أحد الجرائم الآتية: كالتنصت والدخول غير المشروع من أجل الابتزاز والتخريب والمساس بالحياة الخاصة، وقد نصت هذه المادة على الآتي:

« يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمس مئة ألف ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

١- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظام صحيح أو التقاطه أو اعتراضه.



obeikandi.com

٢- الدخول غير المشروع لتهديد شخص أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.

٣- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

٤- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها.

٥- التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة»

**المادة الرابعة:**

في هذه المادة يعاقب الشخص بالسجن لمدة ثلاث سنوات وبغرامة مليوني ريال إذا ارتكب أحد الجرائم الآتية: كالاستيلاء على مال منقول أو على سند والوصول دون مسوغ إلى بيانات بنكية أو ائتمانية، وقد نصت هذه المادة بالآتي:

« يعاقب بالسجن مدة لا تزيد عن ثلاث سنوات وبغرامة لا تزيد على مليوني ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

١-الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

٢-الوصول دون مسوغ نظام صحيح . إلى بيانات بنكية أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات»

**المادة الخامسة:**

في هذه المادة يعاقب الشخص بالسجن لمدة أربع سنوات وبغرامة ثلاثة ملايين ريال إذا ارتكب أحد الجرائم الآتية: كالدخول غير المشروع لإلغاء أو إتلاف بيانات خاصة، وإيقاف الشبكة المعلوماتية عن العمل وإعاقة الوصول إلى الخدمة، وقد نصت هذه المادة بالآتي:



openkandil.com

«يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

١-الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها أو إتلافها أو تغييرها، أو إعادة نشرها.

٢-إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدميرها، أو مسح البرامج أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.

٣-إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت».

**المادة السادسة:**

في هذه المادة يعاقب الشخص بالسجن لمدة خمس سنوات وبغرامة ثلاثة ملايين ريال إذا ارتكب أحد الجرائم الآتية:إنتاج ما فيه المساس بالنظام العام أو القيم الدينية وإنشاء مواقع للاتجار في الجنس البشري أو المخدرات، وقد نصت هذه المادة بالآتي:

«يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

١-إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة أو حرمة الحياة الخاصة أو إعداده أو إرساله،أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.

٢-إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره للاتجار في الجنس لبشري، أو تسهيل التعامل به.

٣-إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة، و نشرها، أو ترويجها.

٤-إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار لمخدرات أو المؤثرات العقلية أو ترويجها أو طرق تعاطيها، أو تسهيل التعامل به».



openkandil.com

**المادة السابعة:**

في هذه المادة يعاقب الشخص بالسجن لمدة عشر سنوات وبغرامة خمس ملايين ريال إذا ارتكب أحد الجرائم الآتية: كإنشاء موقع لمنظمات إرهابية أو الدخول غير المشروع لغرض الحصول على معلومات أمنية، وقد نصت هذه المادة بالآتي:

«يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

١-إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره، لتسهيل الاتصال بقيادات تلك المنظمات أو أي من أعضائها، أو ترويج أفكارها أو تمويلها. أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية.

٢-الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني».



openkandl.com

# خاتمة

إن الجريمة الإلكترونية أصبحت جزءاً من مفهوم الجريمة التقليدية، ومهما بلغت درجة الاحتياط لها، فإن ذلك لن يمنع الجريمة الإلكترونية من الحدوث، وإنما قد يسهم في الحد منها، فطبيعة التطور العلمي المتفجر لحظياً، تحمل في ثناياها الخير الكثير بمثل ما تحمل من أخطار، وكلما خرج كَشْف جديد، فرح به أكثر الناس وحاولوا توظيفه لما فيه خيرهم وخير المجتمع، بينما تجد بعضهم ينظرون إلى الاستفادة منه بطرق سلبية، وكانت وسائل التقنية في العصر الراهن أكبر برهان لهذا الاختلاف بين بني البشر، ولذا ينبغي الحرص في استعمال وسائل التقنية ولاسيما الإنترنت، وتحصين الممتلكات الخاصة المتاحة من خلاله بالحماية أولاً، والانتباه واليقظة ثانية، حتى لا يقع المرء فريسة سهلة لضعاف النفوس من مجرمي الإنترنت.

وإن الإنترنت تعج بالمتطفلين بأنواعهم المختلفة ويستخدمون الأدوات المتجددة والذكية للقيام بعملية التطفل والتلصص والتخريب.

وإن كنا لا نستطيع إيجاد حلول كاملة لجرائم الإنترنت إلا أن اتخاذ بعض الإجراءات الوقائية على مستوى الفرد وعلى مستوى المؤسسة مهم جداً للحد من مخاطر الإنترنت. من مثل الحرص على وجود برامج حماية فعالة ومحدثة باستمرار من قبل الفرد لتأمين جهازه، أو الحرص على خصوصية الشبكة اللاسلكية التي يعمل عليها، وكذلك الاهتمام بالأمن المعلوماتي للمؤسسات والعمل على بقاء الجاهزية العالية له، إضافة إلى أمور وحلول أخرى عديدة يتناولها الكتاب.

وخلاصة القول بأن شبكة الإنترنت تعد مصدراً معرفياً ضخما الأكبر من نوعه في تاريخ البشرية، والله أعلم، ووسيلة سهلة للتواصل والتحاور، إلا أنه يجب تعزيز الوعي الأمني لدى الأفراد والمؤسسات لكي تكون الاستفادة من الشبكة بأقل الأضرار.



obeikandl.com

obeikandl.com

# فهرس المصطلحات

المصطلحات المستخدمة في الكتاب

التجارة الإلكترونية (E-Commerce)

انعدام الهوية(Anonymity)

استخدام هوية زائفة(Pseudonymity)

التجسس(Spyware)

السوق الإلكتروني (online auctions)

المجتمع الافتراضي(Virtual Society)

إدمان الإنترنت(Internet Addiction)

المنظمة العالمية للملكية الفكرية (WIPO)

مواقع(WAREZ)

محاكيات (Emulators)

الملاحقة(Stalking)

المضايقة (Harassment)

غسيل الأموال(Money Laundring)

صانعو الأدوات (Tool Users)

الخبراء(Elite)

مستخدمو الأدوات (Script kiddies)

فاحصات المنافذ (Port Scanners)



obeikandl.com

obeikandl.com

obeikandi.com

obeikandl.com