الفصل الخامس عشر
العلاقات الاجتماعية
على الإنترنت

الفصل الخامس عشر
العلاقات الاجتماعية على الإنترنت

العلاقات الاجتماعية على الإنترنت، أو استخدام الخدمات الالكترونية للتواصل مع الآخرين والتفاعل معهم حول الاهتمامات أو النشاطات المشتركة هو أمر يمكن أن يقدم وسيلة ممتازة لمتابعة الهوايات وتأسيس الصداقات الجديدة وتعزيز تلك المكونة أصلا، وممارسة الألعاب والتشارك بالأفكار.

ولكن بالرغم من كثرة فوائد التواصل على الإنترنت، إلا أن نشر الكثير من معلوماتك الشخصية على صفحات موقعك الخاص أو مدونتك الإلكترونية أو حتى أثناء تبادل الحديث على الإنترنت قد يشكل مخاطر عليك.

وللتقليل من تلك المخاطر على الإنترنت:

- تحكم في من له الحق في الوصول إلى معلومات عنك.
- فكر مليا قبل الإفضاء بالمعلومات الشخصية (مثل اسمك، سنك، عنوانك البريدي أو الإلكتروني(أو تفاصيلك المصرفية (خاصة تفاصيل بطاقات الائتمان أو الحساب المصرفي)
- طبق ترتيبات الخصوصية والسرية على الإنترنت عند خلقك للنبذة الشخصية وراجع تلك الترتيبات لضمان أنك على علم بمن يستطيع الحصول على المعلومات المتعلقة بك.
- أعرف إلى من تلجأ بحثا عن المساعدة إذا وقعت في مشكلة أو حدث خطأ ما.

إن عدم المبالاة وأنت على الإنترنت يمكنها أن تؤدي إلى الإساءة إلى سمعتك من جراء استعمال تفاصيلك الشخصية بطرق لم تنويها، أو لتعرضك إلى الاحتيال، سرقة الهوية، النصب، والرسائل الإلكترونية الإعلانية

المزعجة، والتحرش بك (ويشمل المطاردة الإلكترونية والتنمر الإلكتروني(وتركيب برامج مضرة بالصدفة على جهاز حاسوبك.

الإساءة إلى سمعتك

يمكن أن تستعمل المعلومات أو الصور التي قمت بنشرها على نبذتك الإلكترونية أو المدونة أو الموقع على الإنترنت خارج السياق الخاص بها لإحراجك أو الإساءة إلى سمعتك. وهناك حالات استعمل فيها أصحاب العمل نبذات علانية لموظفيهم لطردهم من العمل ولممثلي الإتهام في المحاكم استعملوا المعلومات المتاحة علانية على الإنترنت لكسب قضاياهم.

يمكنك التقليل من هذه المخاطر باتخاذ بعض الخطوات البسيطة:

- استعمل أدوات الأمن والخصوصية المتاحة على كل مواقع التواصل الاجتماعي المحترمة على الإنترنت بحيث يكون الوصول إلى معلوماتك "شخصيا".
- لا تتضمن شيئا على نبذتك لا تريد العالم أن يعرفه عنك.
- راقب معلوماتك وتعلم كيف تزيل معلوماتك الشخصية أو صورك التي لا ترغب في وجودها على الإنترنت.
- تذكر بأن أي معلومات متاحة علانية عنك على الإنترنت يمكن لها أن تبقى هناك إلى الأبد. يمكنك معرفة المعلومات المتاحة عنك علانية على الإنترنت من خلال كتابة اسمك في محركات البحث.

الاحتيال وسرقة الهوية على الإنترنت

كل ما زادت كميات المعلومات التي تقدمها على الإنترنت من خلال مواقع العلاقات الإجتماعية على هيئة صور، نبذ عنك، رسائل تكتبها والأحاديث الحينية، كلما سهل أمر استعمال هذه المعلومات من قبل المجرمين لسرقة مالك أو هويتك.

قلل من المعلومات الشخصية (مثل تواريخ الميلاد، الأسماء أو الألقاب الكاملة، إلخ(. التي تتشارك بها على الإنترنت وتأكد من التالي قبل نشر أي معلومات شخصية عنك:

- تحكم في من يستطيع رؤيتها.
- استعمل مواقع حسنة السمعة.

تذكر دائما بأن الأشخاص الذين تقابلهم على الإنترنت قد لا يصدقون القول بشأن شخصياتهم.

النصب

يمكن لأي شخص أن يقع ضحية مجرمين ينتحلون شخصيات وهمية لسرقة أموالك. أعمال النصب تنجح لأنها تقدم للإنسان أشياء يرغب فيها (كالعطلات، وكسب المال السهل، أو علاقة عاطفية(مقابل القليل من المجهود أو تخيفه ليصدق بأنه سيفقد مالا إن لم يجيب على الرسالة.

وتأتي المطالبات بتقديم المعلومات الشخصية والمصرفية وعروض البضائع والهدايا من أغراب، بل يمكنها أن تأتي ممن تعتقد بأنهم "أصدقاؤك".

لذا لا ترد على طلبات غير متوقعة للحصول على معلوماتك الشخصية أو المصرفية عند استخدامك لمواقع العلاقات الاجتماعية، بل أخبر مؤسستك المالية عنها أو أكتب تقريرا بها إلى مؤسسة مراقبة النصب SCAMwatch. يمكنك معرفة المزيد عن أعمال النصب المعتادة وأن تبلغ عنها على الموقع www.scamwatch.gov.au أو بالإتصال على الرقم ١٣٠٠ ٣٠٢ ٥٠٢

الرسائل الإعلانية المزعجة

الرسائل الإعلانية المزعجة ((Spam هي بريد تطفلي إلكتروني – رسائل لا ترغب في الحصول عليها تعلن عن منتجات وخدمات، ترسل إلى بريدك الإلكتروني أو هاتفك الجوال.

وقد يروج بعضا من هذه الرسائل لمنتج أو تدعوك لزيارة موقع ما. وتحاول الرسائل الدعائية غيرها أن تنصب عليك لتستثمر في مخططات وهمية أو تكشف عن تفاصيل حسابك المصرفي أو بطاقة الائتمان الخاصة بك.

وتعتبر الرسالة الإلكترونية رسالة دعائية مزعجة إذا:

- لم تطلبها أو أرسلت إليك من دون إذنك.
- لا تشتمل على المعلومات الدقيقة بشأن مرسلها.
- لا تقدم لك طريقة إلغاء الاشتراك حتى لا تستمر في الحصول على غيرها من الرسائل، أو لا تقوم بإلغاء اشتراكك بعد تقدمك بالطلب لذلك في خلال ٥ أيام عمل.

لتفادي الرسائل الإعلانية المزعجة عليك:

- التأكد من أن مقدم خدمة الإنترنت الذي تتبعه لديه مرشحات لهذه الرسائل.
- أن تستعمل برامج ترشيح الرسائل الدعائية.
- فهم الطريقة التي سوف يستخدم بها عنوانك الإلكتروني قبل إعطائه لأحد على الإنترنت.
- مراجعة بنود وشروط أي شيء قبل التوقيع عليه أو الاشتراك به. هل توافق على إرسال الرسائل التجارية الإلكترونية إليك؟
- لا ترد على الرسالة إذا بدت لك مشبوهة. لا تنقر على أي وصلات ضمن الرسالة الإعلانية مهما كانت، ولا تشتري منتجات أو خدمات تعلن عنها هذه الرسائل لأن العديد منها احتيالي.
- في حالة لم تكن متأكدا من كون صاحب الرسالة صادق، اتصل بمؤسسة SCAMwatch .
- إذا كنت تعرف صاحب الرسالة ولا ترغب في الحصول على المزيد منها، ألغي اشتراكك بها.

• أما إذا وصلتك رسالة إلكترونية تجارية على هاتفك الجوال، فأوقفها بكتابة " STOP " إلى المرسل.

للحصول على المزيد من المعلومات المتعلقة بالرسائل الإعلانية المزعجة، بما في ذلك الأسئلة الشائعة أو للتقدم بشكوى تتعلق بهذه الرسائل، راجع الموقع . www.spam.acma.gov.au

التحرش

عندما تكون معلوماتك الشخصية متاحة علانية، يمكن للبعض أن يجد طرقا للتحرش بك أو تهديدك. وقد يكون هؤلاء أشخاص تعرفهم أو قد يكونوا مجهولين لديك.

ومن أفضل وسائل حماية نفسك من التحرش بك على الإنترنت هو التحكم في من يستطيع الوصول إلى معلوماتك الشخصية على الإنترنت وعدم نشر الكثير منها من خلال النبذ الموجودة عنك على مواقع العلاقات الاجتماعية.

دائما احتفظ بعنوان سكنك وموقعك خصوصيا. فكر جليا قبل نشر الأسماء أو الصور التي تبين أرقام سيارتك، أو أسماء الشوارع أو الأماكن التي تكثر من زيارتها بصورة تمكن الغير من ربطها بشخصك.

البرامج الضارة

البرامج الضارة، أو الخبيثة، هي أنواع من برامج الحاسوب تركب ذاتيا على حاسوبك بدون علمك. وقد صممت هذه البرامج لتجمع معلومات حساسة مخزنة على جهاز حاسوبك، مثل كلمات السر التي تستعملها لإجراء الصفقات المصرفية على الإنترنت، أو تفاصيل بطاقات الائتمان الخاصة بك. وسوف تستعمل هذه البرامج وصلة الإنترنت الخاصة بك لإرسال هذه المعلومات إلى مجرمين ليستعملونها في سرقة المال من حسابك المصرفي أو لارتكاب النصب والاحتيال باسمك.

وكثيرا ما يتم تركيب هذه البرامج الخبيثة من خلال تنزيل ملفات من مصادر غير مؤمنة أو النقر على وصلات إلى مواقع من داخل الرسائل الإلكترونية أو الدعوات التي قد تؤدي بك إلى مواقع إلكترونية تحتوي على فيروسات أو برامج ضارة. ويزداد خطر تنزيل البرامج الضارة على حاسوبك إذا قمت بتقديم معلومات خاصة عنك في بيئة الكترونية غير مؤمنة (مثل جهاز حاسوب في موقع عام، أو وصلة لاسلكية غير مؤمنة).

للتقليل من خطر تنزيل البرامج الضارة، تأكد من التالي:

- مراجعة أوضاع الخصوصية على مواقع العلاقات الاجتماعية على الإنترنت إن وجود نبذة علانية على الإنترنت يعني أنه بإمكان الغرباء إرسال ملفات إليها أو توصيلها بمحتوى ضار.
- لا تفتح مرفقات أو تنقر على وصلات من داخل رسائل البريد الإلكتروني إلا إذا كنت واثقا من أنها تأتي من مصدر موثوق به. إن لم تكن متأكدا، لا تفتح الرسالة ما لم تراجع مصدرها أولا.
- كن حذرا عند إعطاء برامج العلاقات الاجتماعية الجديدة إذنا بالتواصل مع نبذتك أو حاسوبك.
- لا تنقر على الوصلات من داخل شاشات الإنترنت الفرعية، أو التي تشير إلى مواقع على الإنترنت لست متأكدا من موثوقيتها. فقد تأخذك دون علمك إلى موقع يقوم بتنزيل البرامج الضارة تلقائيا.
- تأكد من أن جهاز الحاسوب الخاص بك محمي باستعمال برنامج صد (firewall) ومكافح للفيروسات (anti-virus)، إذ أن هذه البرامج قد لا تكون جزءً من حاسوبك عند شرائك له.
- تحدث مع مقدم خدمة الإنترنت الذي تتبعه حول ما يمكنك القيام به لتأمين وصلة الإنترنت الخاصة بك.

•فكّر أنك تعمل ليك حساب إيميل منفصل لرسائل إيميلاتك المهمة شديد، زي إيميلات التسويق أو المعلومات الممكن يكون عندك فيها اشتراك. وده بساعد في أنك تحافظ على سلامة حساب إيميلك الرئيسي.

مراقبة الأطفال أثناء تواجدهم على الإنترنت

مستخدمي الإنترنت هم المسؤولون عن كمية المعلومات التي يفصحون عنها على الإنترنت. ومعظم المعلومات التي تنشر على الإنترنت متاح للجميع قرأتها وقد يصعب إزالتها منه. كما قد تستخدم هذه المعلومات لأغراض لم تصمم لها.

إن مراقبتك لأطفالك أثناء تواجدهم على الإنترنت يساعد على إبقائهم آمنين وذلك من خلال تذكيرهم بإتباع الخطوات التالية:

•عدم التشارك بكلمات السر أبداً، مهما كانت ثقتهم بأصدقائهم.

•استعمال كلمات سر قوية تتكون من مجموعة أحرف وأرقام، ولا يسهل التكهن بها – أي ليست اسما للمغني المفضل لدى الطفل أو حيوانه الأليف.

•عدم النشر على مواقع العلاقات الاجتماعية (بما في ذلك النبذ(لمعلوماتهم الشخصية أو معلومات أصدقائهم الشخصية، مثل الأسماء والأعمار، عناوين وأسماء المدارس التي يدرسون بها، عناوين بريدهم الإلكتروني أو أرقام الهواتف.

•عدم نشر صور غير لائقة لهم أو لأي شخص آخر، وطلب الإذن قبل الكتابة عن غيرهم من الأشخاص أو نشر صورهم.

•عدم الرد على رسائل إلكترونية مقرفة (ولكن الاحتفاظ بنسخ منها في حالة احتاجوها كدليل لو وقعت مشكلة ما).

•منع وصول الرسائل من مرسلي الرسائل غير اللائقة أو البغيضة، أو مسح الشخص من قائمة العناوين الخاصة بهم إذا كان عليها.

•عدم إعطاء رقم الهاتف الجوال الخاص بهم لأشخاص لا يعرفونهم أو لا يثقون بهم.

• الاحتفاظ بكل الرسائل المقرفة التي تصل إلى حساب البريد الالكتروني الخاص بهم أو هاتفهم الجوال كدليل، وإبدائها لشخص راشد.

الاتصال بشركة الاتصالات اللاسلكية لسد أرقام هواتف مسببي المشاكل على خدمة الهاتف الجوال الخاصة بالطفل.

للحصول على المساعدة والنصح بشأن سلامة الأطفال على الإنترنت، الرجاء الاتصال بمركز السلامة على الإنترنت (Cybersafety Contact Centre) على الرقم ٨٨٠١٧٦ ١٨٠٠ أو خط الأطفال (Kids Line) على الرقم ١٨٠٠ ٥٥١٨٠٠.

أما للحصول على معلومات أكثر بشأن المساعدة في الإبقاء على الأطفال آمنين على الإنترنت، قم بالإطلاع على موقع www.acma.gov.au وموقع السلامة على الإنترنت www.cybersmart.gov.au. (سيكون متاحا من ١ يوليو/تموز ٢٠٠٩).

+ أين تحصل على المساعدة

على معظم مواقع العلاقات الاجتماعية معلومات وأدوات للتبليغ عن المشكلات ومساعدة المستخدمين للموقع على ضبط من له الحق في الوصول إلى معلوماتهم. راجع هذه المعلومات والأدوات عندما تشترك بالموقع، وتأكد من حفاظك على إجراءات الأمن والخصوصية محدثة دائما.

بلغ عن أي نشاطات جنائية إلى الشرطة في ولايتك أو إقليمك.

www.accc.gov.au (مفوضية التنافس والمستهلك الأسترالية)	للحصول على النصح بشأن عمليات النصب وكيفية التبليغ عنها اتصل بمفوضية التنافس والمستهلك الأسترالية (ACCC) أو بهيئة مراقبة النصب SCAMwatch على الرقم ٥٠٢ ٣٠٢ ١٣٠٠.

www.acma.gov.au (سلطة الاتصالات والوسائط الإعلامية الأسترالية)	بالإضافة إلى المعلومات حول مساعدة الأطفال في البقاء آمنين علي الإنترنت، فإن لدى سلطة الاتصالات والوسائط الإعلامية الأسترالية ((ACMA خط إنترنت ساخن للتبليغ عن محتويات منافية للقانون على الموقع www.acma.gov.au/hotline أو بالاتصال على الرقم ١٨٠٠ ٨٨٠ ١٧٦. يمكن التقدم بالشكاوى حول الرسائل الإعلانية المزعجة (البريد الإلكتروني، أو الرسائل الهاتفية القصيرة(إلى السلطة على موقعها www.spam.acma.gov.au.
www.asic.gov.au (مفوضية سوق المال والاستثمارات الأسترالية)	تقوم مفوضية سوق المال والاستثمارات الأسترالية ((ASIC بالتحري في عمليات النصب التي تشتمل على منتجات وخدمات، ومنها الاتصالات الهاتفية وعمليات النصب الاستثماري الهاتفية، وبرامج الاستثمار المنافية للقانون.

هيئات شؤون المستهلك والتجارة العادلة في الولايات والأقاليم: ولاية نيو ساوث ويلز: مكتب وزارة التجارة العادلة www.fairtrading.nsw.gov.au ولاية فيكتوريا: مكتب شؤون المستهلك في ولاية فيكتوريا (CAV) www.consumer.vic.gov.au ولاية كوينزلاند: مكتب وزارة التجارة العادلة (OFT) www.fairtrading.qld.gov.au الإقليم الشمالي: مكتب شؤون المستهلك (وزارة العدل) www.caba.nt.gov.au ولاية جنوب أستراليا: مكتب شؤون المستهلك والأعمال التجارية (OCBA) www.ocba.sa.gov.au غرب أستراليا: وزارة حماية المستهلك والتوظيف (DOCEP) www.docep.wa.gov.au ولاية تاسمانيا: مكتب شؤون المستهلك والتجارة العادلة (CAFT) www.consumer.tas.gov.au إقليم العاصمة الأسترالية: مكتب الخدمات التنظيمية www.ors.act.gov.au	تقوم وكالات شؤون المستهلك والتجارة العادلة بحماية المستهلك والترويج لمصالحه من خلال تقديمها للنصح والمساعدة، وفرضها تطبيق قوانين الاستهلاك بالولايات والتحري في الشكاوى وحل النزاعات.