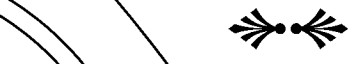
الفصل الخامس

قلّص تعرضك لمشكلات الكمبيوتر



اقترن نمو التجارة بالطرق الإلكترونية بمتاعب الأساليب الإلكترونية وعناوينها الرئيسية من قبيل الفيروسات التي تكلف الملايين وتدمير المواقع على الشاشة... الخ.

ومع أن التباين قد يكون قائماً بين الأعمال التجارية الكبيرة والصغيرة من عدة وجوه، فمن المحزن أن الأمر ليس كذلك عندما يتعلق بمشكلات التكنولوجيا العالية. فجميع الشركات، بغض النظر عن حجمها، يمكن أن تكون عالقة في مشكلة من هذا القبيل، مع أنه يستحيل بناء شركة دون أجهزة كمبيوتر ودون موقع على الشبكة، إلا أنه من شبه المستحيل أن تحمي نفسك وشركتك بمجرد شراء أجهزة الكمبيوتر وشراء موقع على الشبكة.

تُرى ما الذي يمكن أن يحدث؟ يمكن أن تكون ضحية أعطال في جهاز الكمبيوتر أو ضحية برامج كمبيوتر فاسدة، أو يمكن أن تكون هدفاً لمشاكسات المنافسين وهدفاً لزبائن لديهم بطاقات ائتمانية مزورة، أو قد تكون ضحية مستخدمين ساخطين أو أفراد أشرار، أو مجموعة من لصوص أجهزة الكمبيوتر مجهولي الأسماء الذين يتعيشون من تغيير الأشياء على شبكة الإنترنت.

هناك دراسة نشرتها مجلة (إنفورميشن ويك Information Week) وأعدتها إحدى المؤسسات تقدر أن الشركات من سائر الأحجام خسرت ما مجموعه ٦.١ تريليون دولار في عام ١٩٩٩ بسبب انتهاك أمن أجهزة الكمبيوتر وهجمات الفيروس. وفي دراسة أخرى أجرتها مجموعة (غارتنر غروب Gartner Group) أفادت هذه الدراسة أن عدد المرات التي تعرض فيها التجار الذين يتعاملون بطريقة الكمبيوتر لتزوير بطاقات ائتمانية كانت بنسبة ١٢ إلى ١ مقابل التجار الذين لا يتعاملون بهذه الطريقة.

وإلى جانب الساعات التي لا تحصى التي يجب أن تمضيها في استعادة المعلومات التي فقدتها، وتبديل المعدات، وتعويض الإيرادات التي خسرتها،

أو استعادة سمعتك التي شوهها آخرون، فإنك قد تجد نفسك دون أن تدري في مشكلة قانونية بتهمة انتهاك الخصوصية، أو انتحال عمل الغير، أو الافتراء، أو عدم تنفيذ أحد العقود.

أسوأ من ذلك، أن المستخدمين وغيرهم من الذين لهم حضور في داخل شركتك، يستمرون في تشكيل خطر أمني جدي لك أكثر مما يشكله الذين من خارج الشركة، وفقاً لما يقول (أندي بريني Andy Briney) رئيس تحرير مجلة (إنفورميشين سكيوريتي Information Security). في دراسة أجرتها المجلة حول الأمن المعلوماتي في عام ٢٠٠٠ أن «الشركات التي تتعرض لسرقة إلكترونية، أو تخريب إلكتروني، أو إفشاء معلومات خاصة قد ازداد عددها بنسبة ٤١٪ عما كان في عام ١٩٩٩». ويقول (بريني): مع أن هذه الدراسة تناولت أساساً الأعمال التجارية الكبيرة، فإن الأرقام الواردة فيها تشير إلى تزايد القلق من جراء الأخطار الأمنية الداخلية لدى الأعمال التجارية من سائر الأحجام.

إذا أخذنا بالاعتبار فوائد وجود الكمبيوتر المثالي في المكتب بالنسبة لأي عمل تجاري، يصعب أن نتخيل مدى ما يسببه هذا الكمبيوتر للعمل التجاري ذاته من تعرض للأذى. حتى التعرض للفيروسات والأخطاء الاستراتيجية في استخدام البريد الإلكتروني يمكن أن يتسبب في فوضى تحل بالمكتب. ذلك أن كل كلمة في كل رسالة يرسلها المستخدمون ستتخزن وتحفظ في الأرشيف مما يجعلها في متناول يد اللصوص والمنافسين وتجعل العمل التجاري وصاحبه عرضة لتشويه السمعة، والتفرقة، ويعرض أسرار الشركة أو معلوماتها التسويقية للانكشاف.

إن سلامة أجهزة الكمبيوتر الخاصة بعملك تستحق أيضاً التفكير بها. حتى إن كان المكتب في منزلك فإن جهاز الكمبيوتر يمكن أن يتعرض للأعطال بسبب الحرارة، والدخان، والمؤثرات المغناطيسية، والاهتزاز، والصدمة، والكهرباء الساكنة، والعواصف الكهربائية...

وفيما يتعلق بأجهزة الكمبيوتر، تقول مجلة (ساكسس Success) في عدد أيار (مايو) ١٩٩٩ أن معظم أصحاب الأعمال التجارية الصغيرة يتعرضون لنفس الكوابيس الرئيسية، وفي مقدمتها أربعة كوابيس مشتركة سببها:

(١) الباعة الذين يرفضون صيانة المعدات التي يبيعونها.

(٢) انهيار الأنظمة.

(٣) الانتهاكات الأمنية التي تهدد جريان الدم في عروق العمل التجاري.

(٤) الانصراف المفاجئ من قبل خبير التكنولوجيا الداخلية أو مدير تكنولوجيا المعلوماتية. إن كل وضع من هذه الأوضاع الأربعة يمكن أن يسبب في الواقع انهياراً مدوياً. وبصورة تقليدية، يتطلب كل وضع منها رداً مكلفاً جداً، ولهذا السبب بالذات، تجد الأعمال التجارية الصغيرة، بسيولتها النقدية المحدودة، صعوبةً في الحصول على مساعدة.

إن هذا الفصل سيبسّط الخطوات الوقائية التي يمكن أن تتخذها الآن لتفادي هذه المتاعب وغيرها من المتاعب. ولك، بطبيعة الحال، أن تختار ما يناسبك من النصائح، مما يلائم العمل التجاري في المنزل الذي يمتلك جهاز كمبيوتر واحداً قد لا يكون ذا أهمية كبيرة لمكتب يضم مئة شخص ويتعامل مع شبكة في المنطقة المحلية.

الخطوات الوقائية

البدائل إلزامية وليست أموراً محتملة

لقد تحدثتُ إلى أكثر من رب عمل محبط أدرك بعد فوات الأوان، عند حدوث عطل في جهاز الكمبيوتر، أن كل المعلومات الحيوية التي يحتاج إلى استعادتها بعد وقوع المشكلة، مخزونة في الكمبيوتر الذي تعطل.

ما العمل؟

لا ترتكب نفس الغلطة. اطبع في أقرب وقت ممكن المعطيات الرئيسية التي يحتويها الكمبيوتر، من قبيل: المعلومات الجاهزة، وأرقام المساندة التقنية، والأرقام المتسلسلة وأرقام تعريف المنتجات، وأرقام موزري البرامج للكمبيوتر، وكلمات المرور للبريد الإلكتروني، ومزوّد الخدمة على الإنترنت، وأرقام الحسابات.

نعرف جميعاً أنه يفترض بنا أن نحتفظ بنسخ احتياطية لجميع المعطيات، وفي موقع مختلف عن مكتبنا بحيث لا تتلف كلها. ولكن عندما تعرضت مؤسسة (دورسي تريلورز) في بلدة (البا) بولاية (ألاباما) لفيضان، لم تستفد المؤسسة كثيراً من السجلات والاضبارات الاحتياطية. السبب، كما تقول (ماريلين ماركس) المديرة التنفيذية لهذه المؤسسة، أن السجلات والإضبارات كانت مودعة في قبو أحد المصارف، ولكن المصرف أيضاً تعرض للفيضان. ولذلك فإن (ماريلين ماركس) توصي بإيداع الوثائق الحيوية واختبارات الكمبيوتر الاحتياطية في مكان يبعد عن الشركة ما لا يقل عن خمسين ميلاً.

فيما يلي طريقة مختصرة للحصول على معلومات احتياطية في يوم كان مزدحماً بالعمل. فإذا كنت مسرعاً للخروج من المكتب ولم يتوفر لك الوقت لإعداد نسخة احتياطية كاملة لحماية المشروع الذي عملت عليه طوال النهار، الحل البسيط هو أن ترسل نسخة منه إلى نفسك بالبريد الإلكتروني. بهذه الطريقة، إذا جرى تلاعب بجهاز الكمبيوتر قبل عودتك، تظل قادراً على استعادة المعلومات بواسطة ربط حسابك بجهاز كمبيوتر آخر. أفضل من ذلك، أن تستخدم خدمات بريد إلكتروني أخرى. بهذه الطريقة يمكنك أن تستعيد بريدك من أي جهاز موصول بشبكة الإنترنت.

هناك خيارات لإعداد احتياطي للمعلومات بصورة منتظمة: أن تفعل ذلك بنفسك مستخدماً شريطاً، أو قرصاً صلباً، خزن كل ملفاتك في آن واحد على محرك مرآة، وليكن ذلك (أون لاين). إذا فعلت ذلك بنفسك فكّر في تخزين المعطيات وتطبيقاتها.. ومع أن اللجوء إلى إعداد احتياطي للمعطيات هو عملية أسرع وأسهل، لكن لابد من استعادة تطبيقاتك من القرص المدمج الأصلي. لك عدة خيارات لإعداد نسخ احتياطية.

إذا كنت تتعامل مع شبكات المنطقة المحلية، يجب أن يكلف شخص واحد بدور المدير. وأحد أهم الواجبات التي يجب أن يقوم بها هذا الشخص، هو إعداد ملفات احتياطية بشكل دوري، وهذه الملفات يمكن استخدامها لإعادة النظام إلى وضعه التشغيلي عقب توقفه عن العمل أو إصابته بعطل. ووسيلة الدعم الأكثر شيوعاً (والأقل كلفة عند كتابة هذه السطور) هي استعمال محرك تسجيل مغناطيسي. هذه الأشرطة تتسع لأحجام كبيرة من المعلومات، ويسهل استعمالها والتخزين فيها، وهي بصورة عامة يمكن الاعتماد عليها.

إن معظم خبراء الكمبيوتر ينصحون أصحاب الأعمال التجارية بأن يحتفظوا بما لا يقل عن ثلاثة أجيال، وربما أكثر، من أشرطة الاحتياط، بمعنى إذا أعددت دعماً واحداً كل أسبوع، سيتوفر لك ما يعادل ثلاثة أسابيع من الدعم. ومن المهم أيضاً أن تعرف أن بعض الإخفاقات لا تؤثر في الملفات، وبالتالي، فإن خطط التعافي من إخفاق (لان LAN) يجب أن يتضمن أكثر من استعادة ملف. وإذا أخفقت محطة عمل وسط تطبيق عملي، يجب أن يكون هناك أسلوب لكيفية استعادة التطبيق والعمل المفقود.

يجب أن يكون هناك إلى جانب الأسلوب المكتوب، شرح مكتوب لكيفية تشغيل كل جانب من جوانب (لان LAN)، بما في ذلك كيفية إضافة وحذف محطات العمل والحسابات. وعلى أي حال، فإن من يتولى إدارة (لان LAN) يمكن أن

يصبح مستخدماً سابقاً من يوم إلى آخر. ويمكن أن تكون النتيجة كارثة مؤقتة لإنتاج العمل إذا لم تكن هناك تعليمات.

أعطال الكمبيوتر لا مفر منها

قواميس المستقبل قد تعرّف كلمة «ذعر» بطريقة جديدة عامة: «التعرض لمشكلات كمبيوتر في أثناء السباق للوفاء بموعد محدد واكتشاف أن المساندة التقنية من الهاتف غير موجودة عملياً». الأمر المحزن أن هذا الوضع يتجاوز الذعر ليكون كارثة لبعض الأعمال التجارية الصغيرة التي يتوقف نموها على الحصول على مواد أنتجت وجرى تسليمها اليوم.

إن شراء أحد برامج الكمبيوتر والاحتفاظ به لا يحل كل المشكلات. فلدى ظهور برامج (مايكروسوفت وندوز) لأول مرة عام ١٩٩٨، ساعدت شركة (مايكروسوفت) المبيعات بإعلانها أن طبعة عام ١٩٩٨ صححت أكثر من ٥,٠٠٠ عملية تلصص على برنامج (وندوز) لعام ١٩٩٥. هل كان ذلك مدعاة للتباهي؟ هذا يثير لديك التساؤل عن عدد المشكلات التي صححها برنامج عام ٢٠٠٠ في طبعة ١٩٩٨.

ما العمل؟

خلال معظم أعطال الكمبيوتر، يزول (المودم Modem) أيضاً، وبالتالي ينعدم خيار طلب المساعدة (أون لاين). أما إذا لم يحدث ذلك، اتصل بموقع صانع جهازك على شبكة الإنترنت. وعادة يمكن أن تجد إرشادات تقنية وأجوبة على أسئلة طرحت كثيراً، وخطوات يمكن أن تجربها لحل المشكلات، وحلولاً مختزنة في الكمبيوتر. احتفظ دائماً بعنوان صانع الجهاز على الشبكة في متناول يدك (ابحث عن مواقع مساندة تقنية أخرى مذكورة في المصادر). إذا زال (المودم Modem) فأنت بحاجة إلى إجراء اتصال هاتفي. هذا يعني أن

تحتفظ بأرقام المساندة التقنية في متناول يدك، لا أن تكون مخزونة في الكمبيوتر. تذكر أنك عندما تشتري جهاز كمبيوتر أنك تختار أكثر من جهاز. كذلك فإنك تختار بائعاً، وهذا البائع يجب أن يكون قادراً على مساعدتك عند حدوث المشكلات، وأن يقدم لك الصيانة والمساندة.

برنامج (وندوز) كثيراً ما يتعطل في بعض المحلات الصغيرة. لتجنب الأسباب الأكثر شيوعاً لتعطل برنامج (وندوز) جرّب ما يلي:

- لا تنفذ أعداداً كبيرة جداً من البرامج في وقت واحد.
- ابدأ من جديد تشغيل جهاز الكمبيوتر أو محطة الشغل كل يوم بدلاً من ترك الجهاز شاغلاً لعدة أيام. هذا، بطبيعة الحال، يتوقف على أساليبك في العمل. إن بعض الأعمال التجارية تفضل إعداد المساندات ليلاً عندما ينصرف مستعملو الأجهزة، وفي هذه الحالة قد يكون ضرورياً أن يبقى الكمبيوتر مداراً دوماً. في الحد الأدنى، أوقف الكمبيوتر عن العمل في نهايات الأسابيع.
- احتفظ على جاهزية برنامج مكافحة الفيروس. راجع خدمات من نوع (WWW.McAffee.com) التي تحفظ جاهزية برنامجك (أون لاين) لقاء أجر شهري.
- انتبه إلى أن الكابلات ولوحات المفاتيح موصولة بشكل صحيح.
- إذا بدا أن المشكلة هي من نوع الفيديو تحديداً، راجع موقع بائع لوحة المفاتيح على الشبكة للحصول على محرك أحدث.
- زُر موقع الإصلاح (أون لاين) للحصول على نصيحة مجانية، ولكنها مهنية.

نظّف فضاء القرص الصلب (هارد درايف Hard Drive)

قد يبدو تنظيف القرص الصلب (هارد درايف) فكرة جيدة أكثر مما هو ضرورة، ولكن فكّر بمدى ما يصيبك من إحباط عندما تكتشف أنك خارج الفضاء عندما تعمل جاهداً للوفاء بموعد لابد من الالتزام به.

ما العمل؟

ابدأ عمل التنظيف الآن بواسطة:

- إزالة الملفات والوثائق القديمة وضغط أو إزالة ملفات الوثائق القديمة.
- إعادة تجميع أجزاء القرص بانتظام.

التعافي من الحذوفات الناجمة عن حوادث

قدرتك على الطباعة بسرعة يمكن أن تعني أيضاً أنك سريع في العثور على مفتاح الحذف واستعماله، إن حذف ملف بالمصادفة يمكن أن يكون من أكبر أسباب هدر الوقت؛ لأنه يعني أنك ستضطر إلى إعادة صنع الملف، إذا كان ذلك ممكناً.

ولكن إلغاء المعلومات لا يكون سببه دائماً خطأ بشري. إن مؤسسة (أون تراك داتا إنترنشيونال On track Data International) وهي مؤسسة مقرها في منيسوتا، وتقدم خدمة استعادة المعلومات المفقودة، تقول: إن ٤٤ ٪ من المعلومات المفقودة سببها أعطال ميكانيكية، و١٤ بالمئة سببها مشكلات في البرامج، ونحو ٧ ٪ سببها فيروسات، و٣ ٪ سببها كوارث طبيعية، وبذلك يبقى ٣٢ ٪ عائدة إلى خطأ بشري.

ما العمل؟

للتعافي من الحذف، ركّب (أدوات نورتون Norton Utilities) لبرامج (وندوز) أو (عدم حذف برامج المدير Executive Software Undelete For Windows). كلا هذين البرنامجين يعمل بشكل أفضل من علبة تخزين وندوز العادية الخاصة باستعادة ملف.

إذا كنت على وشك تنفيذ ميزانية ضيقة، اختزن ونزل برنامج (عدم الحذف الطارئ Emergency Undelete) من الموقع المحدد على الشبكة (www.executive. com/undelete/ eudfree/ eudguest. htm.).

هناك خيار آخر هو ما يسمى برنامج (المفقود الذي عثر عليه Power Quest Lost and Found) من موقع: (www. powerquest. com).

إلى أي حد جهاز الكمبيوتر الخاص بك آمن؟

يُحتفظ عادة بالمخدّم محمياً بالقفل والمفتاح، ولكن ما قولك في القرص المدمج الاعتيادي فوق الطاولة؟ (Standard desktop Pc). إن برنامج سلامة الجهاز في كولومبوس في ولاية أوهايو، أكبر مؤمن للكمبيوتر الشخصي في الولايات المتحدة يفيد بأن نحو ٥,١ مليون جهاز كمبيوتر قد سرقت، أو جرى تعطيلها أو تدميرها في عام ١٩٩٩ (آخر عام توفرت فيه هذه المعلومات). وعقب تحليل ادعاءات إتلاف أجهزة الكمبيوتر الشخصية في سائر مجالات الصناعة على مدى ثلاثة أعوام، تبين لبرنامج (سلامة الجهاز Safeware) أن ٢٥٪ من سائر مفقود الأجهزة على الطاولة كان بسبب السرقة.

وحتى إذا وجدت أن جهاز الكمبيوتر الخاص بك لا يزال ماثلاً على طاولتك بعد عطل، فهذا لا يعني أن كل ما هو ضروري بقي سالماً. بل إنك قد تجد أنه لم يبق لك سوى القشرة.

دعنا نواجه المشكلة. فإذا كنت أنت قادراً على نزع وإبدال محرك قرص صلب بسهولة، فإن أشخاصاً آخرين يمكنهم أن يفعلوا ذلك. المحركات لا يمكن نزعها ونسخها وإبدالها، أو، ما هو أسوأ من ذلك، إبدالها بمحرك صلب مختلف. إن الأشرار قادرون حتى على تركيب برنامج على المحرك الصلب في جهازك الذي يسجل كلمات المرور (Passwords) ورسائل البريد الإلكتروني وغير ذلك من المعلومات الحيوية. لهذه الأسباب كلها، تستخدم شركات كثيرة أجهزة كمبيوتر (دون أقراص diskless)، المعروفة أيضاً باسم (محطات صامتة dummy stations) فمحطة الشغل التي دون قرص

المربوطة بـ (لان) ليس فيها أي محركات قرص محلية. إنها بدلاً من ذلك تعمل بنظام (بوت لوجيك boot logic) في شريحة (اقرأ فقط الذاكرة Read only memory) أي شريحة (Rom). ومع أن الكمبيوتر دون قرص يعتمد كلياً على المخدم في كل برامجه ولا يمكنه أن يعمل دون الشبكة، فإن له ميزات الكلفة الأقل، والأمن الأفضل، والتحكم الأشد من قبل مالك العمل التجاري.

ما العمل؟

ضع سياسة تتطلب من المستخدمين أن يضعوا الأقراص والأشرطة في خزائن مقفلة بالمفاتيح عند انتهاء يوم العمل. أنصحهم باستخدام قفل لوحة المفاتيح لتعطيل اللوحة. يمكنك أيضاً، إذا كان ذلك ممكناً، أن تطلب من المستخدمين استعمال حماية كلمة المرور لبرامج (وندوز) وكلمات المرور لمنقذات الستارة، ولكن نبههم إلى عدم ترك كلمة المرور ظاهرة للعيان.

إن خط الدفاع الواضح والأسهل هو أن تضع قفلاً على باب مكاتبك، ولكنك قد ترغب في تركيب المزيد من وسائل الحماية. إن الشركات التي تموّن المكاتب تعرض الآن للبيع صناديق كمبيوتر عالية الأمان. هذه الصناديق مزودة بأزرار تمكنك من أن تعرف هل جرى عبث بالكمبيوتر منذ استعماله آخر مرة. هناك خيارات أخرى منها علب محكمة، ولاصقات قوية، وحاجزات الكوابل، وأجهزة إنذار.

أخيراً، إن وضع علامات على معداتك قد لا يحول دون سرقتها، ولكن من المؤكد أنه يساعد الشرطة على تمييزها عن غيرها من الأجهزة المسروقة التي تستعاد كل عام. ضع علامة على معداتك بقلم ذي لون بنفسجي غامق. في هذه الحالة لا يستطيع اللصوص أن يحاولوا إزالة العلامة لأنهم لن يروها. كما يمكنك أن تحصل على بطاقات تعريف ذات أرقام متسلسلة تلقى

بصورة دائمة على أجهزة الكمبيوتر. ابحث عنها منذ الآن في المحلات التي تشتري منها معدات مكتبك.

بوجود البريد الإلكتروني أنت معرض للمشكلات

في اللحظة التي يتوفر فيها البريد الإلكتروني لمستخدميك، فأنت لا تسهل فقط جوانب الاتصالات في أعمالهم، بل إنك قد تعرض للخطر أمن ونزاهة شركتك. فالمستخدم مثلاً يمكنه عندها:

- أن يرسل رسالة فيها عبارة عرقية أو جنسية.
- أن يرسل إلى منافس معلومات سرية عن شركتك.
- أن يكتب بسرعة رسالة وهو في حالة غضب فيها شتائم للباعة الذين تشتري منهم.
- أن يضع معلومات سلبية عن شركتك في غرفة ثرثرة على الإنترنت.

لقد أقرت المحاكم شرعية استخدام الوثائق الإلكترونية كبيّنات في المحكمة، ولذلك فإن ما يكتبه ويرسله مستخدموك يمكن استعماله ضدك. كذلك، فكر في الطريق الطويل الذي تجتازه المعلومات و«الأيدي» الكثيرة التي تمر بها خلال عبورها شبكة الإنترنت. وهذا من شأنه أن يقنعك بوضع سياسة أشد حيال المعلومات الحيوية لدى شركتك.

ما العمل؟

بطبيعة الحال، لا يمكنك دائماً أن تحول دون حدوث هذه الأوضاع، لأنك غير قادر على فرض رقابة كاملة على مستخدميك، ولكن هنالك ثلاثة أشياء تستطيع أن تفعلها لحماية شركتك من الإدانة في حالة إقامة دعوى قضائية:

١ - **زد تغطية شركتك لحمايتها من المساءَلة القانونية.** تأكد من أن التأمين ضد المساءَلة القانونية يشمل الرسالة الإلكترونية، وإلا زد تغطيتك أو بدّل

سياساتك بحيث تكفل تغطيتك. تعلم المزيد من حاجات تأمين الأعمال التجارية الصغيرة من الفصل السادس.

٢ - **ضع سياسات خاص.** بك اكتب سياستك الداخلية فيما يتعلق بما هو مناسب وغير مناسب بشأن البريد الإلكتروني. اشرح للمستخدمين أن الرسائل غير الواضحة يمكن أن يساء تفسيرها. اطلب من المستخدمين الامتناع عن كتابة النكت، وعبارات السخرية، والعبارات المتسرعة، وأي شيء يمكن تفسيره بأنه تحرش، أو تفرقة، أو كلام مخالف للقانون. وضح لهم كيف تريدهم أن يحافظوا على معلومات الشركة السرية، اختتم بيان سياستك بنصيحة مفادها أنه إذا خامرهم شك في أمر ما، يجب أن يطلبوا إيضاحاً. احرص على تزويد جميع مستخدميك بنسخ من سياساتك، وأن يقرؤوها ويوقعوا على استلامها وقراءتها.

٣ - **إذا كنت لا تزال متشككاً، حاول أن تعرف ما هي حقوقك القانونية في ولايتك.** قد تكون قادراً على رصد ما يفعله مستخدموك من خلال البريد الإلكتروني، بحيث «تراقب» دورياً نشاطات المستخدمين. لمعرفة المزيد، اتصل بمحاميك، والسلطة المختصة في الولاية، أو الاتحاد الوطني للأعمال التجارية المستقلة. والقوانين هي بصورة عامة لمصلحتك. بعد ذلك، ابدأ بالتدقيق في رسائل البريد الإلكتروني وراقب النشاط في البريد الإلكتروني من حين إلى آخر.

الدخول على الإنترنت يجلب السرور والألم

إذا كان الدخول على البريد الإلكتروني كما وصفناه يتيح للمستخدمين الدخول أيضاً على شبكة الإنترنت، فإن مشكلاتك قد تزداد أكثر فأكثر. نظرياً، إذا كان لك موقع على شبكة الإنترنت فستعد من الناحية التقنية ناشراً، وبالتالي فإنك ستتحمل نفس مسؤولية الناشرين الكبار، بما في ذلك ملاحقتك قضائياً بتهمة انتهاك حقوق المؤلف أو انتحال عمل المؤلف. وإذا ما أقدم أحد الموظفين على تفريغ المعلومات لمصلحة استخدام الشركة فقد تعدُّ مذنباً.

إن التطفل على الشبكة يمكن أن يكون درباً تدخل عن طريقه معلومات عرقية أو معلومات فاضحة أو معلومات تنم عن الكراهية إلى موقع شركتنا، مما يؤدي إلى المساءلة القضائية. على سبيل المثال مستخدمو شركتي (سيتي غروب City Group) و(مورغان ستانلي Morgan Stanley) أقامتا دعوى على مستخدميهما بسبب الأسى الذي سببته نكت عرقية وصلت عبر البريد الإلكتروني للشركة.

إن المستخدمين يمكنهم أيضاً أن يكلفوك ساعات لا تحصى من وقت العمل غير المثمر عندما يتنقلون على الشبكة ويتسوقون من محلات (أون لاين)، ويتابعون المناقصات، ويبحثون عن الخيارات لقضاء عطلتهم، أو يقومون بإدارة ملفات أسهمهم. إن شركة أبحاث (إن.أر.أو NRO) ومقرها في مدينة (توليدو) بولاية (أوهايو) تبين لها أن نحو ٥٠٪ من مستخدميها يكثرون من التنقل على الشبكة لأسباب شخصية خلال ساعات العمل.

بيد أن الخطر الأكبر الذي يواجهك قد يأتيك من مستخدمين ساخطين. إن اسم (تيموثي لويد Timothy Loyd) معروف تماماً في سائر أنحاء عالم المعلوماتية التكنولوجية. ففي عام ١٩٩٦ سبب هذا الرجل ما يقدر بمبلغ ١٢ مليون دولار قيمة أضرار لرب عمله في ذلك الحين شركة (أوميغا انجينيرينغ Omega Engineering). كيف حدث ذلك؟ لقد علم لويد آنذاك أنه على وشك أن يُطرد من عمله ولذلك زرع قنبلة منطقية أدت إلى محو كل عقود أوميغا وبرامجها المستخدمة في الكمبيوتر وشوهت حضورها على الشبكة.

هناك أسماء مماثلة لاسم (تيموثي لويد) في مؤسسات صغيرة. وفيما كان هذا الكتاب قيد التأليف، كانت هناك مواقع مراقبة على الشبكة تتحدث عن مستخدمة في أحد المستشفيات، استندت إلى مجرد شائعة عن طردها من العمل، فرتبت طريقة مريحة لفصلها من العمل بواسطة نسخ معلومات تخص

مريضاً في حالة حرجة وأضافت إلى ذلك عبارات زرعتها على موقع المستشفى في الشبكة. ولقاء مفتاح إزالة النسخ وافق صاحب المستشفى على منحها تعويضاً مجزياً عن نهاية العمل كما وافق على عدم إقامة دعوى ضدها.

بطبيعة الحال، المستخدمون ليسوا الهم الوحيد للشركة عندما يتعلق الأمر بالإنترنت. فهنالك الوضع المألوف جداً حيث تجد الشركة نفسها ضحية أكاذيب تطلق من خلال الإنترنت. هذا الوضع يمكنه أن يؤثر ليس فقط في أرباح الشركة، وأسعار أسهمها، ومبيعاتها، وسمعتها، بل إن الشخص الذي بث المعلومات الكاذبة إذا كان يستعمل حساباً في أثناء العمل، فإن رب عمل هذا الشخص يمكن أن يقع في مشكلة أيضاً.

إن بعض الإساءات المعروفة جيداً عن طريق الإنترنت تشمل ما يلي:

- مصمم الأزياء (تومي هيلفيجر Tommy Hilfiger) اتُّهم بأنه أدلى بأقوال عرقية في حفل، لم يكن مهماً أن هيلفيجر لم يحضر قط ذلك الحفل ولا أنه يسوّق إنتاجه بصورة واسعة لسكان من الأقليات، إلا أن المعلومات رغم ذلك انتشرت انتشاراً سريعاً عبر الشبكة.
- اتهمت صفحة شركة مايكروسوفت بأنها موبوءة بالفيروس. في الواقع لم تكن موبوءة.
- مؤسسة (ليكسيس نيكسيس Nexis – Lexis) اتهمت بأنها تبيع أرقام التأمين الاجتماعي لمواطنين مقابل ربح. وفي الواقع إنها لم تفعل ذلك، مع ذلك فإن سمعتها قد تلوثت.
- شركة ماكدونالدز كثيراً ما تتعرض لحملات بشأن المواد التي تضيفها إلى وجباتها.
- شركة السيدة (فيلد Field) لصنع الكعك اتهمت من قِبل الناشطين المعادين للعنف بأنها قدمت منتجاتها مجاناً إلى جماعة تبرئة (أ.ج. سمبسون) والحقيقة أن ذلك لم يحدث إطلاقاً.

والآن نقدم قصة اطلع عليها (دان جانال Dan Janal) رئيس مجلس إدارة شركة (جانال) للمواصلات (www. janal. com). القصة تقول: إن الشركة خاضت صراعاً طويلاً وصعباً مع نقابتها ودافعت عن نفسها مفنّدة المعلومات الكاذبة التي ظهرت بشأنها على الشبكة. والقصة تقول:

«في أحد الأيام بحث أحد المديرين عن معلومات جديدة بشأن الإضراب. وقد وجد موقعاً يحتوي على العديد من الأكاذيب وعلى معلومات كاذبة من ضمنها مقابلة تلفزيونية مزعومة بين مذيع المحطة التلفزيونية المحلية ورئيس النقابة. الكلام المزعوم في المقابلة كان مختلفاً بالكامل، لأن المقابلة التلفزيونية لم تحدث إطلاقاً. وهذا الكلام المزعوم احتوى على أقوال كاذبة ومضللة. مع ذلك فإن أي شخص قرأ هذا الكلام على صفحة الإنترنت لابد أن يكون قد اعتقد أن المعلومات صحيحة، إذ إنه لم يكن هناك سبيل ليعرف خلاف ما قرأ. المدير المذكور اتصل بمحامي الشركة وبدأ بإعداد إستراتيجية. لقد اطلعا على الصفحة فلم يجدا أية معلومات عن اتصال. ولكنهما نظرا إلى شيفرة المصدر الخاص بالصفحة. فلم يجدا اسماً ولا رقم هاتف للشخص الذي دسّ الصفحة على الإنترنت، ولكنهما وجدا عنوان بريد إلكتروني. عندئذ ذهبا إلى مؤسسة (ديجانيوز Dejanews)، وهي مؤسسة أبحاث للرسائل المتبادلة بين جماعات. وقد طبعا عنوان البريد الإلكتروني فوجدا أن مستخدم الصفحة كان قد دسّ عدة رسائل. وتبين أن هذا الشخص امرأة مدمنة على حضور اجتماعات جماعة الناجين من مرض السرطان وجماعة موسيقى (البلوز) وجماعة تشجيع الزواج، ومع أنها لم تضع اسمها على صفحة النقابة المسيئة إلا أنها أبلغت الجميع اسمها ورقم هاتفها بواسطة الرسائل التي بثتها.

لاحظ المحامي والمدير شيئاً آخر: إن صفحة الشبكة لم تدس على موقع النقابة، بل على موقع وكالة بيع عقارات. ولدى قيامهما بأبحاث (أوف لاين offline) تبين لهما أن المرأة التي دست الصفحة تعمل في مجال بيع العقارات لمصلحة الشركة التي ظهرت على موقعها على الشبكة الصفحات المسيئة.

ولما تسلحا بهذه المعلومة، اتصل المحامي بالمرأة. دار الحديث بينهما على النحو التالي: مرحباً، نعرف أنك مصابة بسرطان الثدي، وأن فنان موسيقى (البلوز) المفضل لديك هو (ب.ب.كنغ .B.B King) وأن ابنتك ستتزوج في شهر تموز (يوليو). ونعرف أيضاً أنك دسست صفحة على الشبكة مليئة بالمغالطات عن النقابة. إذا لم تسحبي الصفحة خلال ساعة واحدة، سنتصل بمديرتك، وقد لا تكون سعيدة إذا علمت أنك عرضت ترخيصها للخطر عندما دسست معلومات فيها تشهير على موقعها على الشبكة. وسنتصل بمجلس الولاية الخاص بتثبيت الوقائع لإبلاغهم أنك نشرت معلومات تشهير بالآخرين، مما يشكل انتهاكاً لترخيصك. وسنتصل أيضاً بالمذيع ونظهر له المقابلة التي اخترعتيها. وبالمناسبة، لقد نسخنا الصفحات، وبالتالي إذا أردنا أن نذهب إلى المحكمة أو إلى مجلس الولاية فإننا نستطيع الذهاب.

خلال خمس دقائق كانت الصفحة قد سحبت».

ما العمل؟

الخطوة الأولى لحماية نفسك من الاتهام بأنك دسست مواد مسيئة هي أن تضع سياسة تبين للمستخدمين بوضوح كيف يمكنهم وكيف لا يمكنهم استخدام الإنترنت.

ولكن انتبه إلى أن معاملة المستخدمين وكأنهم يشكلون خطراً محتملاً، قد تكون لها نتيجة معاكسة؛ لأن هذه المعاملة تؤذي معنوياتهم.

إن أحد أفضل الحلول لتفادي سوء استعمال الكمبيوتر من قبل المستخدمين هو أن تتخذ خطوات إضافية لضمان عدم توظيف شخص قد يعمد إلى هذا الفعل. عزز إجراءات التوظيف وضاعف التدقيق بخلفيات الأشخاص خلال عملية التوظيف بحيث تستبعد المسيئين المحتملين. يجب أن يكون معلوماً منذ اليوم الأول أنك ترصد نشاط الكمبيوتر بدقة، واطلب من المستخدمين أن يقرؤوا ويوقعوا على سياسة الأمن. بعد ذلك، إذا أمكن، اسمح لمستخدمين اثنين بدلاً من واحد بالاطلاع على رموز الدخول على الشبكة، وكلمة المرور، والمعلومات الحيوية ـ والاثنان اللذان أقصدهما يجب ألا يكونا ممن لا يختلطان بالناس بغير ضرورة خارج المكتب. بهذه الطريقة تُنشئ نظاماً مبسطاً يراقب من خلاله أحد المستخدمين عمل مستخدم آخر.

أخيراً، احمل التخريب عبر الإنترنت على محمل الجد. ويجب أن يعرف المستخدمون أنك لا تتهاون في ذلك وأنك دائب على البحث عن احتمالات التخريب كدأبك على مراقبة محاولات سرقة ممتلكاتك. (راجع أيضاً الفصل الثاني الذي يتحدث عن خطوات للحد من الجريمة).

إن البيان الذي أصدرته صناعة أمن المعلومات (كما ورد في مجلة أمن المعلومات) لعام ٢٠٠٠م، والذي اقتبسنا منه في هذا الكتاب، أظهر أن عدد المؤسسات التي أفشى مستخدموها أو خرّبوا عمداً معلومات الشركات ازداد بنسبة ٤١٪ من عام ١٩٩٨ إلى عام ١٩٩٩. ومع أن هذه الدراسة تعكس تشديداً قوياً على الأعمال التجارية الكبيرة، فإن المختصين بالأعمال التجارية الصغيرة يعتقدون أن النتائج تعكس أيضاً الأعمال التجارية الصغيرة؛ لأن معظم المؤسسات الصغيرة تفتقر إلى بنية تحتية للأمن المتعدد الطبقات الذي يجعل من الصعب الغش في المعلومات الحساسة. على سبيل المثال، يقول معهد أمن الكمبيوتر: إن إساءة من داخل المؤسسة تكلف المشروع المستهدف

حوالي ٢,٧ مليون دولار وسطياً، بينما الإساءة من الخارج لا تكلف أكثر من ٥٧,٠٠٠ دولار وسطياً.

أما فيما يتعلق بالمادة التي تدس ضد شركتك، يجب أن تعرف أن هذا ممكن الحدوث وأنه يندر أن تتمكن من فعل أي شيء للحيلولة دون حدوثه. إن الإنترنت قد أعطى وسيلة للوشاة على الشبكة لإظهار قدراتهم، هؤلاء الناس الذين لولا ذلك لالتزموا الهدوء. لسوء الحظ، أن هؤلاء الناس يستطيعون اتخاذ أسماء وعناوين مزورة لإخفاء هوياتهم إلى حد أنه يستحيل في أكثر الأحيان على الشركات أن تفعل أي شيء بشأن المعلومات. وإن ما يثبط الهمة بالقدر ذاته أن المعلومات الموجودة على الشبكة كثيراً ما تعتبر معلومات يعتمد عليها لأنها تبدو هكذا. وإن مواقع الشبكة والقصص التي تُروى من خلالها تتخذ مظهر العمل الصحفي ولكن دون العرق والعمل المضني في التدقيق، واعتماد المصادر الموثوقة، ووزن الآراء الموضوعية، هذه الأمور التي تعتمدها الصحافة الأخلاقية.

إن المهاجم يستطيع أن يقول ما يحلو له دون أن يتعرض للمساءلة لأنه لا يوجد حافز صحفي يفرض عليه التدقيق في الحقائق، ولا توجد هيئة تحرير تطلب منه ذلك، على نحو ما هو قائم في وسائط الإعلام الأخرى.

إن مؤسسة (جانال) تعرض الخطوات السبع التالية لحماية شركتك:

١ ـ **عيِّن شخصاً ما لمراقبة جماعات الأخبار ومراكز البحث مرة في الأسبوع على الأقل.** دقق في أسماء الشركات وأسماء المنتجات. إذا كانت شركتك منظورة جداً، دقق في أسماء كبير المديرين التنفيذيين أو حتى رئيس مجلس الإدارة.

٢ ـ **إذا وجدت رسائل على الشبكة في مجموعات الأخبار اقرأ الرسائل جميعاً فيما يتعلق بالموضوع وقرر ما إذا كانت هناك حاجة للرد.** في بعض الحالات

يتلاشى الموضوع. أو أن الأشخاص الأشد ذكاء الذين يبثون الرسائل يتصلون بالمصدر للتأكد من معلوماته.

٣ ـ **إذا رأيت أنك بحاجة للرد من أجل تصحيح الأمور افعل ذلك.** إن القواعد المتبعة من قبل مجموعة الأخبار تحظر الإعلان بمجموعات الأخبار، ولكنها لا تحظر تبادل المعلومات الذي يتسم بالأمانة والصدق. والواقع أنك إذا لم تذكُر الجانب الذي تعرفه من القصة، فقد يفترض الناس أن الصمت يعني الموافقة.

٤ ـ **اتصل بالمصدر مباشرة لترى إن كان بالإمكان تسوية المشكلة.** ربما كان هناك خلل في الاتصالات أحدث سوء تفاهم. معظم الناس يمكنهم أن يكونوا معقولين. وحقيقة الأمر أن أكبر أنصار الشركات هم أشخاص سبق أن تعرضوا مرة لمشكلات في خدمة الزبائن جرت تسويتها. فقبل أن تتصل أو تكتب، اعرف ما إذا كان الشخص قد بثَّ رسائل أخرى في مجموعات أخبار أخرى. إن مؤسسة (ديجانيوز) توفر مسالك اتصال مع كل الرسائل التي بثها الشخص. إذا قرأت الرسائل سيتبين لك ما إذا كنت تستطيع أن تقيم علاقة مع ذلك الشخص.

٥ ـ **إذا وجدت موقعاً محتالاً على الشبكة، حاول أن تعرف هل بإمكانك التحدث إلى صاحب الموقع لكي تعرف ما المشكلة.** فإذا كان صاحب الموقع قد تلقى خدمة زبائن سيئة أو اشترى منتجاً فيه عيب، خذ علماً بذلك، لأن هذا الشخص يمكن أن يكون ناطقاً بلسان أشخاص كثيرين واجهوا مشكلات مماثلة مع شركتك. في هذه الحالة تكون مشكلتك في الواقع مشكلة داخلية. فإذا سويت المشكلة من المحتمل أن يزول الموقع المحتال، وإلا فإن الصفحة ستظل حية إلى ما لا نهاية على غرار (يو.إس. ورست.U.S.Worst)، وهي صفحة هجومية لشركة (يو.إس. وست.U.S.West)، شركة الاتصالات

العملاقة. بإمكان الناس أن يبثوا قصص الرعب التي لديهم على الموقع. وإلى حين من الزمن يتمكن الزائرون من العثور على رقم هاتف منزل رئيس الشركة وبذلك يتمكنون من تقديم الشكوى له مباشرة.

٦ ـ **من الصعب تحدي أصحاب مواقع الشبكة المحتالين، لأنهم محميون بموجب التعديل الأول للدستور الذي يضمن حرية الكلام.** بيد أنهم يخضعون لنفس قوانين التشهير كما في العالم الحقيقي. وهكذا إذا نشروا معلومات مزورة مع علمهم أنها مزورة، تستطيع أن تلاحقهم قضائياً وتخرسهم.

٧ ـ **احرص على نسخ الصفحات على جهاز الكمبيوتر الخاص بك واطبعها على الورق.** فهذه هي بيّنتك. أما إذا لم تنسخها وتطبعها وأزال المعتدون المادة المسيئة، فلن يبقى عندك أي إثبات لجريمة التشهير.

إن برامج من نوع (وب هاكر Webwhacker) و(وب بدي Web Buddy) يمكنها نسخ مواقع بكاملها بما في ذلك النص والصور و(البريد الإلكتروني).

احذر الأوغاد

كلنا سمعنا التعبير القائل، «لا تصدق كل ما تقرأ». لا يصح هذا الكلام أكثر مما يصح في المواد التي تظهر على الشبكة. من ناحية أخرى تعرض الشبكة العديد من ضربات الحظ والفرص التي لا تجدها في أي مكان آخر. فكيف يمكنك أن تثق بأن ما تقرأه صحيح؟

ما العمل؟

اتبع غريزتك. إذا بدت صفقة ما بأنها جيدة إلى حد لا يصدق، فمن المحتمل أنها جيدة جداً. ولكن للتأكد يجب أن تزور هذه المواقع الخاصة بأحدث الإنذارات من الأوغاد:

- موقع (About.Com) وبالأخص برامجها عن أساطير الحضر والموروث الشعبي: (www. about. com).
- مكتب العمل التجاري الأفضل أون لاين (Better Business Bureau online) الموقع (www. bbb.org).
- الائتلاف ضد البريد الإلكتروني غير المنشود (Coalition against unsolicited Commercial E-mail) الموقع (www. cauce. org).
- وحدة حماية المستهلك التابعة للجنة التجارة الفدرالية، الموقع: (www. Ftc. gov / ftc/ consumer. htm) .
- مكافحة الغش على الإنترنت، الموقع: (Spam. abuse.net).
- الأوغاد المخربون على الإنترنت، الموقع: (www. scambusters.com).
- عصبة المستهلكين الوطنية، الموقع: (www. natlconsumersleagve. org).
- المركز الوطني للإعلام عن الغش، الموقع: (www. fraud. org).

لا وجود لك على الشبكة

يصعب أن نتصور أي عمل تجاري لا وجود له على الشبكة، مع ذلك فإني مازلت ألتقي بين حين وآخر أصحاب أعمال تجارية لديهم قناعة بعدم الحاجة إلى موقع على الشبكة. فزبائنهم، حسب حجتهم التي يطرحونها، هم من السكان المحليين، وهم يقدمون للزبائن خدمة أو منتجاً لا يحصل عليهما المستهلك إلا بزيارة مستودعاتهم أو دكاكينهم ـ مثلاً، مستهلك يريد تبديل إطارات سيارته، أو تسجيل السيارة، أو قص شعر رأسه. بيد أني أرد بالقول أن هناك العديد من مراكز خدمة السيارات والحلاقين في معظم البلدات الصغيرة. وسيأتي يوم (وبسرعة) سيوازن المستهلكون بين التسوق على الشبكة والتجول في البلدة لمعرفة الأسعار. على أي حال، فهذه هي طريقة العيش التي اعتمدها المراهقون ـ وهم مستهلكو منتجاتك وخدماتك في

المستقبل. فدون تواجد على الشبكة، لن يجد العمل التجاري الصغير مكاناً في مسيرة الحياة.

أما مؤسسات البيع بالمفرق التي ليس لها موقع على الشبكة، فإني أعتبر تفكيرها قصير النظر ولا ينسجم مع الإدارة بعيدة النظر. ففي كل مجال من المجالات التي تمسها الشبكة (ولا تمسها) استطاع المستهلكون الإفادة من الأسعار الأدنى. وكل شخص لم يقتنع بعد بأن الحضور على الشبكة ضروري، سيعرف عما قريب أن ولاء المستهلكين سيتعثر بنسبة مباشرة إلى الوفورات التي يمكن تحقيقها من خلال التسوق على الشبكة.

إن نفقات الإدارة المتخصصة في أعمال البيع بالمفرق عبر الإنترنت تسمح للأعمال التجارية التي تتبع هذا الأسلوب بتحويل الوفورات إلى الشاري. وهذا يعني الوفورات المتحققة من المبيعات لدى المحلات التقليدية ناجمة عن غياب نفقات الشحن وعن الخدمة المباشرة للمستهلك. وإذا ما كنت لا تزال غير مقتنع بأهمية الموقع على الشبكة بالنسبة لعملك في المستقبل، ينبغي أن تفكر بما يلي: إن مشتريات المستهلكين عبر الشبكة سترتفع من ٥,٤ بليون دولار في عام ١٩٩٨ إلى ٣٣,٣ بليون دولار مع حلول العام ٢٠٠٢، وفقاً لدراسة شركة (أي ماركتر E. marketer) وهي شركة في مدينة نيويورك تتابع اتجاهات التسويق عبر الإنترنت وإحصاءات (أون لاين).

إن معرفتك بتوجهات التكنولوجيا من شأنها أن تكون ذات تاثير إيجابي على طريقتك في تطوير عملك التجاري. وخلال كتابتي لهذا الكتاب، كانت شركات الطيران تتيح للمستهلكين فرصة مسح الشبكة وهم على مقاعدهم في الطائرة، كما أن شركة (جنرال موتورز) تخطط لتزويد مقدم لخدمة إنترنت متحركة. خلاصة القول، إن الإنترنت له حضور دائم ويجب أن يكون أمراً واقعاً يمثل عاملاً تأخذه في الاعتبار خلال عملك التجاري، إذا أردت أن تحافظ على قدرتك على المنافسة.

ما العمل؟

اعرف ما يفعله منافسوك على الشبكة، ثم توسع في البحث لتعرف ما تفعله الأعمال التجارية الأخرى في بقية أنحاء البلد. اتصل بها، واسأل ما هي النواحي الناجحة وما هي غير الناجحة. وعندما تكوّن فكرة عن النواحي الناجحة لديها، أنشئ موقعك المتميز على الشبكة، بعد ذلك سجل موقعك على الشبكة على سائر أوراقك.

احمِ حضورك على الشبكة

جاء في مجلة المرأة العاملة (Working Woman Magazine) في عدد أيار (مايو) ٢٠٠٠ في الصفحة ٤٦ أن حملة بوش للفوز بالرئاسة سجلت أسماء أربعة وخمسين مجالاً عندما كان جورج دبليو بوش مرشحاً للرئاسة في عام ٢٠٠٠. فلا عجب في ذلك: فلقد اكتشفوا موقعاً على الشبكة لصورة تهكمية تحت عنوان (www.gwbush.com)، وهذه الصورة بدت ليس فقط أنها رسمية بل هي تبيع أزراراً عليها صورة بوش وفوق أنفه ملعقة من فضة مع عبارة تقول: «إنه النفاق، أيها الغبي». في أثناء ذلك، اكتشفت حملة بوش موقعاً بعنوان (www.allgore.com) فيه صورة مرشح خيالي اسمه (All Gore) يريد أن يلغي السيارات في المدن التي يربو عدد سكانها على ٥٠,٠٠٠ ويريد من التجمعات السكنية أن تمنع بقوة القانون العلكة. هذا التحامل وتشويه السمعة استمرا طوال صبيحة يوم الانتخابات، عندما فوجئ زوار موقع اللجنة الوطنية للحزب الجمهوري على الشبكة بنداء مؤلف من ألف كلمة لصالح المرشح (غور) مع وصلة إلى موقع (غور) على الشبكة.

إن شركات لا يحصى عددها تعرضت هي أيضاً لرسوم تهكمية أو مواقع شتيمة. مثال ذلك، إن من قام بزيارة موقع (www.untied.com) وجد موقعاً

مكرساً لحملة مقذعة على شركة (يونايتد إيرلاينز United Airlines). لقد تعلمت الشركات أنه ينبغي لها أن تسجل ليس فقط موقعها على الشبكة إذا أرادت أن تحمي اسمها من المفترين، والزبائن الساخطين، والمنافسين.

ما العمل؟

احمِ اسم شركتك:

- بتسجيل صيغتي الجمع والمفرد.
- سجل الشركة مع إضافة أل التعريف إلى الاسم.
- سجل الصيغ التي تتوسطها علامة وصل (-) إذا كان الاسم مركباً.
- سجل أخطاء التهجئة (من قبيل Untied بدلاً من United) وفق ما هو مذكور أعلاه.
- سجل جميع الامتدادات الثلاثة: (.com,.net,.org)
- اربط كل هذه التسجيلات بصفحة منزلك على موقعك «الحقيقي».

بإمكاني أن أتحدث عن هذا الدرس من واقع خبرتي الشخصية. عندما أسسنا أنا وشريكتي معهدنا الخاص بالكتابة على الإنترنت (www.writeDirections.com) قبل سنوات. لم نجد سوى اسم واحد (من يتذكر سذاجة المتعاملين بالإنترنت في تلك الأيام؟). بعد فوات الأوان، اكتشفنا أن كاتبة لا تنتمي إلى شركة أو مؤسسة سجلت تحت عنوان (www.writeDirection.com)، ومما أضاف إلى الأذى إهانة أن اسمها الأول كان (ديبرا). إنني كثيراً ما أتساءل عن عدد الزبائن الذين وجهناهم إليها، وعدد الذين ينسحبون لدى اكتشافهم أن الموقع ليس هو ما ظنوا أنه المقصود.

موقعك على الشبكة يستضيف انهيار شركات

تصور إرسال كاتالوج بالبريد إلى أكثر من ستين مليون إنسان عارضاً عليهم الشحن مجاناً لمدة معينة إذا طلبوا شراء أشياء من موقعك على الشبكة. والآن تصور أنهم عندما يحاولون الاستفادة من هذا العرض ضمن المدة المحددة، يتعذر عليهم الاتصال بالموقع. فإذا كان تشويه صورتك لا يكفي بحد ذاته لارتفاع نبضات القلب، فإن ثمن الكاتالوجات وأجرة البريد تقوم بالمهمة.

هذا الوضع حدث لإحدى الشركات في أواخر عام ١٩٩٩، وحدثت مشكلات مماثلة لعدد لا يحصى من الشركات التي تتخذ من الإنترنت قاعدة لها. على سبيل المثال شركة (إي بي e Bay)، بزبائنها الذين يزيد عددهم على المليون، قد اضطرت للتوقف عن العمل عدة مرات، وفي إحدى هذه المرات لأكثر من عشرين ساعة. وحتى شركة (أمازون كوم Amazon.com) اختفى وجودها على الشبكة عدة مرات. أعطال هذه المواقع تحدث لعدة أسباب: عطل في المخدّم، أخطاء في البرمجة، مشكلات في أقراص البرامج، خطأ بشري، الخ. والأعمال التجارية الصغيرة معرضة بصورة خاصة للأعطال لأنها لها علاقة بشريحة مضيفة على الشركة تقوم بعرض بيئة مخدم مشتركة.

ما العمل؟

مع أنه من المستحيل أن تكون الشركة آمنة مئة بالمئة، إلا أنه من الممكن إيجاد شركات مضيفة هي أهل للثقة أكثر من غيرها. فإذا كان بوسعك أن تجد استضافة مخلصة، بمعنى أن تجد شركة مضيفة تكرس مخدماً لشركتك وحدها، تعامل معها. إن العديد من الأعمال التجارية الصغيرة لا تستطيع أن تفعل ذلك، لأن الرسوم تبدأ ١٥,٠٠ دولار شهرياً. لذلك فإن أحد الخيارات هي أن تحاول التسوّق لدى نقابة الشركات المضيفة على الشبكة، التي تقول

إن مهمتها هي «حماية المستهلِكين من المضيفين غير الأمناء، وأن تساعد على تحديد من هي الشركات المضيفة والأمينة والشرعية الموجودة».

ولكي تصبح الشركات المضيفة أعضاء في النقابة يجب أن تحصل على ترخيص. عندما تتحدث عن شركة مضيفة اطرح العديد من الأسئلة. حذارِ أن تفترض أن جميع الشركات المضيفة تعمل بنفس الطريقة. إسأل عما إذا كان موقعك على الشبكة سيكون محمياً للمخدمين بحيث إذا تعطل أحدهما يحوّل كل بريدك إلى الآخر. واسأل هل سيكون موقعك على الشبكة مراقَباً كل يوم وبأية طريقة. اطلب وصفاً للخطة البديلة في حالة حدوث مشكلة.

موقعك على الشبكة خلال أزمةٍ: سيأتي الناس

إذا رغبت في أن يزور مزيد من الناس موقعك على الشبكة، يجب أن تكون حريصاً على معرفة سبب هذه الرغبة. إحدى الطرق لضمان مجيئهم هو لتجربة الأزمة. عندما تكون شركتك واقعة في مشكلة أو أن الشائعات منتشرة بشأنك، فإن الناس يريدون أن يتحققوا من الأمور، ربما للمرة الأولى، وهذا يعني أنه من الأفضل أن تكون قادراً على التعامل مع الاهتمام الزائد بك.

ما العمل؟

إذا تمكن زوار الموقع من إرسال رسائل، وطرح أسئلة، وتقديم طلبات، فأنت بحاجة إلى مزيد من الأشخاص للاهتمام بالأجوبة. عيِّن شخصاً واحداً ليكون مسؤولاً عن كل الأجوبة، وكلِّف هذا الشخص بضبط الموقع. وسواء أكان هذا الشخص رجلاً أم امرأة فإن بإمكانه أن يبعث برسائل إلى أشخاص آخرين للإجابة عليها. فقط تأكد من أن الأجوبة متماسكة وأن رسالتك قد وصلت.

إذا كان شيء ما على الموقع هو جزء من المشكلة، فأنت بحاجة لأن تتمكن من إزالة هذا الشيء بسرعة. وإذا تطلَّب بث شيء جديد على الموقع وقتاً طويلاً منك، فإن إجراء التبديلات لن يسير بسرعة أكبر خلال الأزمة. حدد ما هي خياراتك. وهذه نصيحة تنطبق أيضاً على تسويق مادة على الموقع تتعلق بخدمة أو منتَج يمر بأزمة.

بالتأكيد أنت تريد أن تستمر في الدعاية لسلامة كرّاجة أطفال إذا وجدت نفسك للتو في مشكلة قانونية لأن ثلاثة أولاد أصيبوا بجراح خطرة من جراء انفلات كراجاتهم. إن أفضل عمل تقدم عليه في هذه الحالة هو أن توقف المعلومات عن المنتَج المعطوب وتُحِل محلَّها نشرة إخبارية تتضمن وصفاً لرد فعلك على الأزمة وما تنوي أن تفعله بهذا الشأن.

أخيراً، لاشك في أنك التزمت تقنيات جيدة للكتابة على الشبكة عندما أعددت موقعك، وذلك بإضافة لغة يخاطَب فيها الزوار من شخص إلى شخص، ولذلك حافظ على اللغة نفسها عندما تقدِّم رسائلك ذات الطبيعة السلبية أيضاً. لابد لك من أن تظهر لمستك الإنسانية. إن مادتك في الأزمة ستكون تبايناً جارحاً مع الأخبار «الودية» على الموقع إذا ما ملئت هذه الأخبار بلغة الشركة.

موقعك على الشركة خلال أزمة: لن يأتي الناس

نوع آخر من الأزمة يحدث عندما تُنشر أخبار كاذبة تحذِّر الناس داعية إياهم للابتعاد عن موقعك. وهذا ما حدث لشركة (بلو ماونتن آرتس Blue Moun-tain Arts)، وهي دار نشر صغيرة تملكها أسرة وتقوم بطباعة بطاقات معايدة، وكتب تتضمن قصائد شعر، وبطاقات إلكترونية، وحدث ذلك في مطلع عام ١٩٩٩ عندما تم تمرير الرسالة التالية على الإنترنت:

«الموضوع: فيروس (بلو ماونتن آرتس)»

«تنبّه» !!!

«التاريخ: السبت ٢٧ شباط (فبراير) ١٩٩٩»

«تلقينا للتو اتصالاً من العائلة. أحد أصدقاء العائلة منتج بطاقة من إنتاج (بلو ماونتن) فتعطّل النظام. امتنعوا عن فتح بطاقات بلو ماونتن حتى إشعار آخر».

على غرار ما تفعله التحذيرات من الفيروس فإن هذا التحذير اكتسب حياة خاصة به إذ بدأ الناس يتناقلونه على نطاق دولي إلى كل من يعرفونه كما بدأوا يوصلونه إلى مراكز الأخبار ويتحدثون عنه في كل مكان. بالعودة إلى الوراء، يقول خبراء الكمبيوتر إنه كان من الغباء أن يعتقد أي شخص أن بطاقات (بلو ماونتن) يمكن أن تكون ناقلة لفيروس، وذلك لأنها مجرد بطاقات رُسِمت عليها خطوط ورسوم ونصّ ولا شيء غير ذلك. لقد كان من المحزن بالنسبة لدار نشر (بلو ماونتن) أن هذه القضية كانت قضية مفهوم لا يتلاءم مع الواقع ولكن هذا المفهوم فرض انتقال الرسالة السلبية.

ما العمل؟

ليكن ردك سريعاً. إن مؤسس (بلو ماونتن) السيد (ستيفن شوتز) أصدر بياناً بثّه على الموقع قال فيه أن الشائعة كانت حكاية مختلقة وأن الموقع سليم تماماً. في الوقت ذاته كان ابنه قد شرع يتحدث إلى وسائط الإعلام.

بطبيعة الحال سيكون أمراً مساعِداً لك إذا تمكنت من معرفة البادئ في نشر الشائعة، عندئذ تكون قد تزودت بمادة دسمة تقدمها إلى وسائط الإعلام. في حالة (بلو ماونتن) افترض الابن المدعو (جاريد Jared) أن الرسالة السلبية بدأت كنتيجة لعمل تخريبي. في ذلك الحين نقل عنه موقع (www.About.com) قوله: إن سرعة الانتشار جعلتني أشتبه بأن شخصاً

أو أشخاصاً ناشطين في نشر هذا التحذير.. نكاد نفقد عقلنا لمعرفة كيف نكافح هذا العدو غير المنظور».

الأمر الآخر الذي كان يمكن أن يساعد أسرة (شوتز) هو أن يبثوا رسائلهم الخاصة لدى مراكز نشر الأنباء والمخدِّمات وجمع أمثلة عن أعمال نشر أخبار كاذبة أخرى على الشبكة؛ لأن هذا كان من شأنه أن يمكّن وسائط الإعلام من صياغة قصة أشد تأثيراً. فأسرة (شوتز) باستنادها إلى مزيد من الأمثلة لم يكن يبدو طلبها فضح الشائعة في وسط الإعلام وكأنه خدمة ذاتية.

المتلصصون على الشبكة يمكنهم أن يسببوا أذىً شديداً للعمل التجاري

إذا كانت أنظمة الكمبيوتر في البنتاغون «وزارة الدفاع الأمريكية»، واللجنة الوطنية للحزب الجمهوري، وجريدة «نيويورك تايمز» يمكن أن تكون ضحايا تلصص من قبل المتلصصين على الكمبيوتر، فما الذي يجعلك تظن أنك لن تتعرض لمثل ذلك؟ إن المتلصصين يمكن أن يكونوا أشخاصاً مخيفين بالنسبة لعملك التجاري، والسبب أنهم ليسوا بالضرورة أفراداً مجهولي الأسماء يريدون أن يقتحموا موقعك وأن يسرقوا معلومات عن بطاقة الائتمان، إنهم بدلاً من ذلك في أحوال كثيرة مستخدمون في العمل التجاري، أو مستشارون، أو متعهدون، أو أشخاص ساخطون لديهم إمكانية الأذى. في إحدى الحالات التي تعرضت لها جريدة «نيويورك تايمز»، أراد المتلصصون عقد ندوة يقدمون فيها شكوى مفادها أن زميلاً لهم سُجن وعومل معاملة سيئة من قبل مراسل للجريدة.

لحسن حظ جريدة «نيويورك تايمز» أن عملية التلصص كانت واضحة، ولذلك أمكن اكتشافها بسرعة وتصحيحها. ولكن مثل هذه العملية قد لا

تكون بنفس الوضوح لك إذا كنت أنت الضحية. فالمتلصص يمكنه أن يبدل فقط بضعة أرقام أساسية في موقعك أو أن يرسل رسالة بالبريد الإلكتروني تتضمن انتحالاً لعمل فكري أو أن يسرق معلومات لنقلها - أو لبيعها - إلى أحد المنافسين. ومن بين حيل المتلصصين الأخرى شديدة الأذى تخريب الملفات، أو زرع فيروسات، أو محو ملفات.

ما العمل؟

ثمة خطوات عديدة يمكنك أن تتخذها للحد من احتمال الأذى الذي يسببه أحد المتلصصين.

- لا تترك أجهزة الكمبيوتر الخاص بك موصولة بشبكة الإنترنت إذا لم تكن في حاجة لبقائها موصولة. أما إذا اضطررت لإبقائها موصولة فالاحتمالات القائمة هي أنك لن تتمكن من مراقبة كمبيوترك بنفسك ولذلك استخدم شركة للقيام بذلك بدلاً منك. إن إحدى مؤسسات الخدمات الأمنية يمكنها أن تراقب جهازك أربعاً وعشرين ساعة يومياً، وسبعة أيام في الأسبوع، مقابل رسوم أدنى من خمسين دولاراً في السنة. فقط ابحث عن مثل هذه الخدمات الأمنية على الشبكة وستجد الآلاف منها. ولكن انتبه إلى الحصول على أسماء زبائن هذه الشركات واتصل بهم لتتأكد من أن الشركة التي ستتعاقد معها أفعالها مطابقة لأقوالها.
- ركب ما يسمى أمن الجدار الناري Fire wall security (وهو مزيج من سوفت وير وهارد وير مصمَّم للحيلولة دون استخدام الإنترنت من قبل أشخاص غير مسموح لهم بذلك). وفيما تفعل ذلك، تأكد من أن الجهة التي تستضيف مركزك على الشبكة لديها جدار ناري. فالمتلصصون يمكنهم الدخول عبر ثقوب في مخدّمك على الشبكة. بينما الجدار الناري سيراقب تدفق المعلومات بين مخدمك على الشبكة وبين الإنترنت، بعد ذلك أوقف أي اتصال

غير مرغوب فيه. إن شركة مايكروسوفت تقدم خدمة أمنية مملوءة بتوجيهات تتعلق بالأمن. ابحث عنها في موقع (www.microsoft.com/security) ومواقع أخرى ورد ذكرها تحت عنوان المصادر في نهاية هذا الكتاب.

- راقب مستخدميك مراقبة شديدة. إن المسح الذي سبق ذكره والذي أجرته مؤسسة (Price water house coopers) ومجلة (Information week) أظهر أن من بين الشركات التي شملها المسح باعتبارها تعرضت لخروقات في أمنها خلال العام ١٩٩٨، كانت نسبة ٥٨٪ من هذه الخروقات مصدرها المستخدمون.
- يجب إعداد بدائل جيدة لكل المعطيات بحيث إذا جرت سرقة شيء ما تكون لديك طريقة سريعة لاستعادة الخدمة.
- احرص على نسخ معلومات الائتمان وخزّنها في مكان آخر.
- بلّغ عن السرقة لكي يعرف المستخدمون وغيرهم أنك اتخذت إجراء بدلاً من السكوت عن السرقة واعتبارها فقط درساً تستفيد منه للمستقبل. لكي نبلّغ عن السرقة ابدأ بمركز الشرطة المحلي. وهذا المركز قد يحيلك إلى سلطات أعلى، وهذا يتوقف على الضرر ونوع الجريمة وطبيعة المعلومات التي سُرقت أو شُوهت.

ترخيص برامج الكمبيوتر: القرصنة غير شرعية

علاوة على معرفة كيفية استعمال برامج الكمبيوتر أحد أهم الأشياء التي يجب أن تعرفها عنها هي اتفاقية ترخيصها. فمن المخالف للقانون القرصنة ببرامج الكمبيوتر والمشاركة بها بين الذين يستعملونها في مكتبك. إن عدة شركات وجامعات كبرى في الولايات المتحدة تبين أنها مذنبة بجريمة نسخ البرامج بطريقة غير شرعية، وفرضت عليها غرامات قاسية.

ومع أنه لا توجد معايير عندما يتعلق الأمر باتفاقيات الترخيص (وهذا ما يعقد المشكلة)، هنالك بصورة عامة قاعدة شاملة يجب أن تتبعها: إنك لا

تحوز ملكية البرنامج الذي تشتريه، وإنما تملك فقط حق استعماله. وهذا يعني أنه يجب أن تلتزم حقوق الاستعمال وفق ما هو منصوص عليها في الاتفاقية وعندما تشتري برنامج كمبيوتر، يكون عادة موضوعاً في غلاف. وتوجد على الغلاف ملاحظة مطبوعة تنبهك إلى حقيقة أنك إذا فتحت الغلاف، فأنت موافق على ما ينص عليه الترخيص.

ما العمل؟

تعرف على أحكام اتفاقية ترخيصك. إنك تتسلمها مع كل برنامج تشتريه لأنها تبيّن أحكام الملكية والاستعمال. إن عدم التزامك الأحكام يشكل مثالاً سيئاً بالنسبة لمستخدميك. ومن الصعب أن تتوقع الصدق والنزاهة من عمالك إذا لم تمارسهما بنفسك.

كذلك، فإن أي مستخدم يتبين أنه يستخدم برامج وردت بواسطة القرصنة - سواء أكنت أنت من قدمها له أم لا - سيعرض شركتك لملاحقة قانونية محتملة. تأكد من أن مستخدميك يعرفون موقفك المنشود إزاء هذه المسألة. وهذا يعني أنك ما لم تسيّر الخيارات لمستعملي البرنامج المتعودين، يكون البرنامج مخصصاً لمستعمل فرد أو لمحطة تشغيل واحدة، وليس لمستعملين متعددين ولمحطات متعددة. ويجب أن تعلم مسبقاً أن عملية التركيب تحصي في أغلب الأحيان وتبلغ عن عدد عمليات التركيب. وإذا أردت الحصول على مساندة البائع، عليك أن تحترم اتفاقيات ترخيصك.

التقنية الحيوية قد تؤدي بك إلى المحكمة

هذه التقنية تُعرف أيضاً باسم الهندسة البشرية، وتعني تصميم معدات من أجل رفع إنتاج العامل إلى الحد الأقصى مع تخفيف التعب خلال استعمال المعدات. إن مشكلات جسدية من قبيل الصداع، وإعياء العنق والعين،

أو الآثار الجانبية للإشعاع، ومشكلات العضلات والأوتار، جميعها لها علاقة بالعمل على أنواع معينة من أجهزة الكمبيوتر وأجهزة الرصد، وخاصة نهائيات عرض صور الفيديو.

ما العمل؟

بصفتك مالك عمل تجاري قد لا تُلام بسبب أية عواقب سلبية ناجمة عن استعمال المعدات التي في مكتبك، ولكنك يمكن أن تعد مسؤولاً في المحكمة. احرص على أن يوفر مكتبك أفضل شروط التقنية الحيوية للمستخدمين: أي الإنارة الجيدة، والوضع الصحيح عند الجلوس، وأجهزة الرصد المعدلة بصورة صحيحة، ولوحات مفاتيح يمكن تحريكها من أجل راحة الذي يستعملها، الخ.. يجب أن تقوم بين حين وآخر بجولة تفتيشية على مواقع استعمال المعدات. تحدث إلى المستخدمين واطلب منهم أن يعبروا أمام الآخرين عن ارتياحهم إلى المعدات التي يستخدمونها وإلى بيئة العمل.

إلى جانب ذلك اتبع التشريعات المتعلقة بالتقنية الحيوية لكي تتأكد من أ نك تطبق دائماً القانون. خلال كتابتي لهذه السطور كانت إحدى وكالات الصحة (OSHA) منشغلة في إعداد سياسة للتقنية الحيوية تتعلق بالعمل داخل المنزل. وقد جاء في نشرة إخبارية أصدرتها مؤخراً أن المكاتب الموجودة في المنازل لن تخضع للتفتيش عن مخالفات قواعد السلامة والصحة الفدرالية. بيد أن هذه الوكالة، عندما سُئلت، أجابت بأنها ستحقق في الشكاوى المتعلقة بالعمل الخطر في المعامل إذا جرت تأدية هذا العمل في المنزل. الأمثلة على ذلك تتضمن تجميع مواد إلكترونية، واستخدام آلات دون حراسة، أو التعامل مع مواد خطرة دون حماية كافية.

تزوير البطاقة الائتمانية

إن تزوير البطاقة الائتمانية شائع في التجارة عبر الطرق الإلكترونية وهو مؤهل لأن يزداد سوءاً بسبب التوسع السريع باستخدام الإنترنت مستقبلاً. الأمر الذي يخشاه المستثمرون هو أنهم كتجار، مسؤولون عن كل تعامل يقبلونه بواسطة البطاقة الائتمانية. وبالتالي فإنهم إذا قبلوا عدداً كبيراً من الصفقات المزورة، يمكن أن يصل إلى ما يعد نسبة عالية من تكرار التزوير. والتجار الذين يتعاملون بواسطة الشبكة ووصل بهم الأمر إلى نسبة لا تتجاوز واحد بالمئة من المفروضة عليها سابقاً قد مُنعوا من قبل الشركات التي تصدر البطاقات من قبول بطاقات الائتمان نهائياً. إن الذي يفقد امتياز قبول البطاقات الائتمانية يمكن أن يؤدي به الأمر إلى خسارة عمله التجاري.

يقول (أودري لانفورد Audri Lanford) وهو خبير في سرقات الإنترنت ومحرر في النشرة الإخبارية المسماة (المتلصصون على الإنترنت): «إن تكرار الغرامات على الشركات التي تستخدم بطاقات الائتمان يوحي أن عملها التجاري غير قابل للحياة وغير شرعي، وسيُنظر إلى عملها التجاري بالتشكيك والسلبية إذا تبين أن مشكلاتها عديدة ومتكررة».

«إن الحد من تزوير بطاقات الائتمان يصون وقتك، وسمعتك وإيراداتك المالية». ويتابع (لانفورد): «حدثت زيادة هائلة في عدد التجار الذين تعرضوا لإساءات من قبل أشخاص منحرفين وضعوا طلبيات كبيرة مستخدمين معلومات عن بطاقات ائتمان مسروقة». ويوضح (لانفورد) هذا الأمر بقوله: بما أن التجار لا يحظون بنفس الحماية المتوفرة للمستهلكين عندما يتعلق الأمر بتزوير بطاقات ائتمان، فإنه يحسن بهم أن يتخذوا الخطوات الثماني المذكورة أدناه، وهي خطوات يمكن إيجادها في موقع (لانفورد) على الشبكة:

١ ـ اتخذ خطوات إضافية لتأكيد صحة كل طلبية. لا تقبل الطلبيات إلا إذا قُدمت لك معلومات كاملة، بما في ذلك عنوان كامل ورقم هاتف.

٢ ـ احذر الطلبيات التي تحمل عبارة «اشحن إلى» و«حصِّل القيمة من». اطلب من أي شخص يستخدم عنوان «اشحن إلى» أن يرسل فاكساً «بتوقيعه وبرقم بطاقة ائتمانه للتصديق على الصفقة».

٣ ـ كن حذراً بصورة خاصة من الطلبيات التي تردك من خدمات البريد الإلكتروني المجانية ـ فهناك نسبة عالية جداً من التزوير لأنه من السهل على من يريد الغش أن يفتح حساباً مجانياً ومجهول الاسم بالبريد الإلكتروني باسم شخص آخر، وأن يرسل من ثم إلى التاجر طلبية يستخدم فيها الحساب المزور في البريد الإلكتروني ورقم البطاقة الائتمانية المزور. إن أعمالاً تجارية كثيرة لا تقبل الطلبيات التي تأتي عبر هذه الحسابات المجانية بالبريد الإلكتروني، ومن الحكمة أن تحذو أنت حذوها. تُرى ما هي الاحتياطات التي يجب أن تتخذها إزاء الطلبيات التي تأتي من حسابات بالبريد الإلكتروني؟.

أرسل رسالة بالبريد الإلكتروني تطلب فيها معلومات إضافية قبل أن تعمل على إعداد الطلبية، وبصورة أخص اطلب عنوان بريد إلكتروني غير مجاني واسم ورقم هاتف المصرف الذي أصدر البطاقة الائتمانية، والاسم المذكور على البطاقة الائتمانية بدقة، والعنوان الدقيق للجهة المكلفة بدفع قيمة الطلبية. في أغلب الأحيان، كما يقول (لانفورد): لن تتلقى جواباً، أما إذا تلقيت، فيمكنك بسهولة أن تتحقق من المعلومات.

٤ ـ احذر الطلبيات التي هي أكبر من مقدار الطلبيات التي تتلقاها عادة، واحذر أيضاً الطلبيات التي يجب تسليمها بعد يوم واحد. إن الغشاشين لا يهتمون بالكلفة لأنهم لا ينوون الدفع في أي حال من الأحوال.

٥ ـ وجّه مزيداً من الانتباه إلى الطلبات الدولية. افعل كل ما تستطيع للتأكد من قانونية الطلبية قبل أن تشحن منتجاتك إلى بلد آخر.

٦ ـ إذا كنت مرتاباً الجأ إلى الهاتف واطلب الزبون لكي يثبت الطلبية مستخدماً رقم الهاتف المذكور على عنوان صاحب البطاقة الائتمانية.

٧ ـ فكر في استخدام برامج الكمبيوتر (أون لاين online) لمكافحة تزوير البطاقة الائتمانية.

٨ ـ إذا جانبك الحظ كتاجر فتعرضت لإساءة من قبل لص بطاقات ائتمانية اتصل فوراً بمصرفك وبالشرطة. وقد تتبلغ الشرطة الشكوى ولكنها لن تفعل المزيد إلا بعد معرفة قيمة التزوير بالدولارات.

خُذ نفساً عميقاً

بلا شك أنه عندما يتعلق الأمر بشبكة الكمبيوتر عندك، هنالك عدة حقائق بارزة: معدات الكمبيوتر ووصلاته إلى العالم الخارجي ضرورية، والخطر الأمني كبير، وشيء ما سيتعطل لا محالة، والأعمال التجارية الصغيرة هي الأشد معاناة عند طلب المساعدة، والصعوبات لابد أن تكثر في المستقبل. ولا مجال لإنكار هذه الحقائق: فنمو تكنولوجيا الكمبيوتر قد خلق صناعة جديدة تماماً هي صناعة الجريمة. ولكن، وكما يبين هذا الفصل من الكتاب، فإن القليل من الدواء الوقائي يمكن أن يفعل فعلاً كبيراً في مساعدتك للحصول على نوم أهدأ قليلاً خلال الليل.

أمّن سجلاتك الحيوية

إن شركتك تحتفظ بالعديد من الأعمال الورقية والسجلات الضرورية لاستمرارية عملك التجاري بعد حدوث أزمة. احرص على نسخ وتأمين السجلات الهامة التالي ذكرها:

- الصكوك/ عقود الآجار.
- الأذونات.
- حقوق التأليف.
- العقود الموقعة مع البائعين والعملاء.
- سجلات الضريبة.
- ملفات الأشخاص العاملين في الشركة.
- الرسوم الهندسية.
- صفحات سلامة المواد.
- توثيق الالتزام بالأنظمة الحكومية.
- أية وثيقة لابد من الاحتفاظ بها قانونياً لمدة من الزمن.
- العمل المستمر الذي لا يمكن إعداد نسخة عنه لأنه لم يكتمل.
- ملفات الادعاء لدى المحاكم وملفات التقاضي.
- المعلومات المالية والمعلومات عن الأسهم ومالكيها.
- دليل العمل الخاص بسياسة الشركة.
- ميثاق الشركة.
- دليل عمل المستخدمين.
- نسخة مكتملة تحتوي على أرقام الهواتف وشيفرات الكمبيوتر والإنترنت وكلمات المرور، وأرقام هواتف المستخدمين، وأرقام بطاقات الائتمان لدى الشركة.
- نظام التشغيل الأساسي لدى الشركة والملفات وبرامج الكمبيوتر الحساسة.
- الفواتير وقوائم الشحن وغيرها من الوثائق في نظام كمبيوتر شركتك.

الآن، احبس نفسك، لأننا سننتقل إلى الفصل السادس الذي ستتعلم منه كيف تضيف مزيداً من التأمين لجهودك الرامية لتوفير الأمن لعملك.