
Internet Explorer 8

الفصل الأول السلامة الالكترونية

- على الرغم من الآفاق الواسعة التي فتحتها شبكة الإنترنت، وعلى الرغم من المتعة التي يعيشها المستخدم عند استخدامه لخدماتها أو حين إبحاره في صفحاتها، تبقى المشكلة العالقة هي كيفية تأمين الحماية الشخصية التي باتت هاجساً يشغل بال المستخدمين ومطوري صناعة خدمات الإنترنت على حد السواء.
- تنقسم الحماية الشخصية على شبكة الإنترنت إلى قسمين هما:
  - 1. السلامة.
  - 2. الأمن.
- فالسلامة هي توفير الحماية لضمان سلامة المستخدم نفسه من العرض للاستغلال أو الابتزاز أو الانتهاك أو الإساءة. علاوة على أنها اصطلاح يستخدم للإشارة إلى حماية الأطفال أثناء استخدامهم لشبكة الإنترنت. أما الأمن فهو توفير الحماية لضمان أمن المعلومات والبيانات والخصوصية الشخصية. وهي بذلك تشمل حماية الملفات والعتاد.

- **مخاطر شبكة الإنترنت:**
- لقد أصبح الاعتماد على شبكة الإنترنت كبيراً كواحدة من وسائل الاتصال الهامة في مختلف حقول الاستخدام بشكل أبرز أهمية التركيز على المخاطر التي قد تنتج جراء ذلك الاستخدام. فما هي مخاطر شبكة الإنترنت؟ هناك العديد من المخاطر بعضها جدي والبعض الآخر أقل جدية. وتتراوح تلك المخاطر بين الإصابة بالفيروسات المدمرة للبيانات والمعلومات المخزنة على الحاسوب والاختراق للعبث بملفات المستخدم. أو استغلال حاسوبه بقصد الإساءة إلى آخرين. إلى سرقة البيانات الشخصية بقصد الانتحال أو الابتزاز. وسرقة بطاقات الائتمان. وعلى الرقم من أنه ليست هناك ضمانات كاملة للحماية من المخاطر إلا أن هناك خطوات وقائية تحمي المستخدم من خطر الإصابة.

- **السلامة على الإنترنت:**
- اعرف جيداً مع من تتعامل قبل الكشف عن أية معلومات.
- تجنب الإفصاح عن أية معلومات شخصية في خدمات المشاركة الحية كغرف المحادثة والمنتديات.
- احرص على استخدام اسم الأول فقط عند المشاركة في المحادثات أو المنتديات.
- احرص على عدم إرسال أية معلومات حساسة ككلمات السر وأرقام بطاقات الائتمان عبر البريد الالكتروني، واعلم أن الجهات الرسمية لا تطلب تلك المعلومات عبر البريد الإلكتروني.
- استخدم كلمات سر صعبة التخمين وتجنب المعلومات العامة كتواريخ الميلاد وأرقام السيارات أو الهواتف وأسماء الأبناء، وحاول المزج بين الأحرف الصغيرة والكبيرة والأرقام والرموز.
- تجنب المنتديات المشبوهة والمعروفة بالمنتديات السفلية والتي عادة ما يجتمع فيها مخترقوها الأنظمة.
- تجنب خاصية التخزين التلقائي للمعلومات الشخصية على الحواسيب التي لا تخصك في حال استخدامها.
- قم بعملية مسح ملفات (cookies) بين فترة وأخرى.
- تجنب الاحتفاظ بالصور والمعومات الشخصية على جهاز الحاسوب، واستخدم عوضاً لذلك ذاكرة التخزين المحمولة.
- قم بفصل كاميرا الويب في حال عدم استخدامها.
- استخدم كلمات سر للملفات الحساسة.
- تجنب الرد على رسائل البريد الإلكتروني المشبوهة.
-

- **سلامة التعاملات التجارية:**
- عند القيام بعملية الشراء الإلكتروني عبر مواقع الويب، تأكد من الآتي:
- استخدم المواقع التجارية المعروفة.
- تأكد من أن الموقع يمتلك عنواناً فعلياً وأرقام اتصال.
- اطلع على سياسة الموقع التجاري وشروط الخدمة.
- عند الشروع في علمية الدفع بواسطة بطاقة الائتمان، تأكد من ظهور صورة القفل (padlock) في أسفل الصفحة أو نافذة العنوان.
- اضغط على القفل لتظهر لك معلومات الشهادة الإلكترونية، وتأكد أن الشهادة منحت لنفس عنوان الموقع.
- تأكد من أن بادئة عنوان الموقع قد تغيرت من (http) إلى (https.).
- تجنب العروض الترويجية غير المعروفة الواردة عبر البريد الإلكتروني.
- يمكنك الاستعانة بميزة الدفع عن طريق طرف ثالث، كتلك التي توفرها شركات مثل (PayPal) و(money bookers.).
- استخدم بطاقات الائتمان الافتراضية التي تصدرها بعض المؤسسات المصرفية بدلاً من استخدام البطاقات التقليدية.
-

- **سلامة التعاملات التجارية:**
- عند القيام بعملية الشراء الإلكتروني عبر مواقع الويب، تأكد من الآتي:
- استخدم المواقع التجارية المعروفة.
- تاكد من أن الموقع يمتلك عنواناً فعلياً وأرقام إتصال.
- اطلع على سياسة الموقع التجاري وشروط الخدمة.
- عند الشروع في علمية الدفع بواسطة بطاقة الإئتمان، تأكد من ظهور صورة القفل (padlock) في أسفل الصفحة أو نافذة العنوان.
- اضغط على القفل لتظهر لك معلومات الشهادة الإلكترونية، وتأكد أن الشهادة منحت لنفس عنوان الموقع.
- تأكد من أن بادئة عنوان الموقع قد تغيرت من (http الى https).
- تجنب العروض الترويجية غير المعروفة الواردة عبر البريد الإلكتروني.
- يمكنك الاستعانة بميزة الدفع عن طريق طرف ثالث، كتلك التي توفرها شركات مثل (paypal و money bookers).
- استخدم بطاقات الإئتمان الإفتراضية التي تصدرها بعض المؤسسات المصرفية بدلاً من استخدام البطاقات التقليدية.

الأمن الإلكتروني

- **أمن الإنترنت:**
- استخدم برامج مكافحة الفيروسات والجدران النارية (firewalls)لتأمين جهاز الحاسوب واعمل على تحديثها باستمرار.
- استخدم برامج الكشف عن الملفات الخبيثة كملفات التجسس والملفات الدعائية والملفات التي تسيطر على متصفح الإنترنت.
- افحص الملفات المنزلة من المواقع غير المعروفة أو خدمات مشاركة الملفات أو الواردة عن طريق البريد الإلكتروني.
- لا تفتح الملفات المرفقة بالبريد الإلكتروني المجهولة المصدر.
- استخدم برامج تشفير الملفات (.files encryption)
- استخدم مرشحات رسائل البريد الالكتروني (filtersوخدمات مكافحة البريد غير المرغوب فيه anti-spam).)
- قم بعمل نسخ احتياطية للملفات بشكل دوري.
- كن حذراً أثناء استخدام برامج المحادثة الفورية، وافحص الملفات التي تردك بواسطتها قبل فتحها.
- استخدم مواقع فحص المنافذ (portsللتأكد من عدم وجود منافذ مفتوحة للمخترقين، وتعرف تلك المواقع باسم (.online port scanners)
- قم بعمليات التحديث الضرورية والدورية لبيئة التشغيل المستخدمة لسد الثغرات الأمنية.
- تجنب فتح حساباتك المصرفية على الشبكة أو ارسال أرقام بطاقات الإئتمان عبر الشبكات اللاسلكية (wi-fiغير الآمنة كالموجودة في المطارات والمقاهي على سبيل المثال.

مصادر تهديد الخصوصية والإزعاج

أولا: المتطفلون والمتجسسون على بريدك الإلكتروني:

كثير من الناس مصابون بإدمان التجسس على الغير. وينشأ معهم حب التتبع لخصوصيات الناس. ويتمكنون من تحقيق ذلك بعدة طرق منها:

برامج التجسس وهي كثيرة ومتنوعة ومتوفرة بالأسواق أو عن طريق الإنترنت.

تخمين كلمات العبور السهلة التي قد يستخدمها الأصدقاء كاسم الدولة والمدينة التي ولدت بها أو اسم المدرسة أو تاريخ الميلاد.

استخدام برامج مخصصة للوصول الى كلمات العبور.

وهي عبارة عن برامج تمكن مستخدمها من تجريب عدة آلاف من الكلمات السرية المنطقية والشائعة لدى الناس. وبذلك يمكن لها أن تصيب في بعض الأحيان.

كما يمكن لكل من يستطيع الوصول إلى جهازك في المكتب أو المنزل من الزملاء أو الأهل أو الأصدقاء من التطفل على رسائلك باستخدام بعض الخصائص المتوفرة في متصفحك ومنها: خاصية الرجوع للخلف في المتصفح. واستخدام خاصية تذكر اسم المستخدم وكلمة العبور. واستخدام خاصية الإكمال التلقائي للاسم وفراغات النماذج. واستخدام خاصية تذكر الصفحات التي تقوم بزيارتها.

ثانيا: المزعجون:
وهي عادة الشركات والمواقع التي تحصل على عنوان بريدك الإلكتروني وتقوم بتبادل هذه العناوين فيما بينها أو تقوم ببيع هذه العناوين وكذلك يقوم بعض الأفراد بجمع هذه العناوين للقيام بإزعاج الآخرين أو لغرض بيعها لإحدى الشركات. وقد انتشرت مؤخرا رسائل باللغة العربية تحكي قصص محزنة لأطفال أو كبار تعرضوا لحوادث شخصية أو حوادث سير (طبعا كلها من نسج الخيال) ويطلب منك صاحب الرسالة بأن تساعد ذلك الطفل المسكين بارسال الرسالة الى كل من تعرف ومن لا تعرف!! وطبعا أنت من ذوي القلوب الرحيمة والطيبة فتقوم بالعمل نيابة عنه بينما يقوم هو بجمع العناوين وتكوين ثروة من العناوين يقوم ببيعها أو يكون قد أرسل معها فيروسا أو برنامج تجسس أو برنامج للتحكم وتعطيل المواقع وأنت لأتعلم عنها.
كما انتشرت في الآونة الأخيرة رسالة تحتوي على معلومات عن أحد مكونات الشامبو وأنها تسبب السرطان.
ويذكر فيها منتجا معينا ويمدح فيه بينما يذم في بقية الأنواع. ويطلب منك إخبار كل الأصدقاء والمعارف عن طريق تحويل الرسالة. وطبعا كل هذا الكلام ليس له أساس من الصحة والهدف منه جمع العناوين أو التسويق للشامبو الخاص بهم.
سبل الوقاية

*لتفاصيل أكثر عن هذا الموضوع، انظر **فيض الدارئ**.*

- وتجاوز سعة المخزن المؤقت هو هجوم يمكن أن تستخدم من جانب القراصنة للحصول من خلال طرق مختلفة على كامل النظام. أنها تشبه "اجبار الغاشمة" كمبيوتر يرسل هجوم هائل للكمبيوتر الضحية حتى الكراكس. معظم الحلول الأمنية الإنترنت اليوم لا توفر الحماية الكافية ضد هذه الأنواع من الهج.