

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

وَالسَّلَامُ عَلَيْكُمْ وَرَحْمَةُ اللَّهِ وَبَرَكَاتُهُ



**

العنوان:

السلامة الإلكترونية



الأمن والسلامة على الإنترنت

- على الرغم من الآفاق الواسعة التي فتحتها شبكة الإنترنت، وعلى الرغم من المتعة التي يعيشها المستخدم عند استخدامه لخدماتها أو حين ابجاره 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 للإستغلال أو الإبتزاز أو الإتهاك أو الأساءة. 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 الاساءة إلى اخرين. إلى سرقة البيانات الشخصية بقصد الإلتحال أو الإبتزاز. وسرقة بطاقات الإئتمان. وعلى الرغم من أنه ليست هناك ضمانات كاملة للحماية من المخاطر إلا ان هناك خطوات وقائية تحمي المستخدم من خط الإصابة.



السلامة على الإنترنت:

- اعرف جيداً مع من تتعامل قبل الكشف عن أية معلومات .
- تجنب الافصاح عن أية معلومات شخصية في خدمات المشاركة الحية كغرف المحادثة والمنتديات .
- احرص على استخدام اسم الاول فقط عند المشاركة في المحادثات أو المنتديات .
- احرص على عدم ارسال أية معلومات حساسة ككلمات السر وأرقام بطاقات الإئتمان عبر البريد الإلكتروني، واعلم ان 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 مخترقوا 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 والمعلومات 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 إتصال.
- اطلع على سياسة الموقع التجاري وشروط الخدمة.
- عند الشروع في عملية 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 الى https).
- تجنب العروض الترويجية غير المعروفة الواردة عبر البريد الإلكتروني.
- يمكنك الاستعانة بميزة الدفع عن طريق طرف ثالث، كتلك التي توفرها شركات مثل (money bookers).
- استخدم بطاقات الائتمان الافتراضية التي تصدرها بعض المؤسسات المصرفية بدلاً البطاقات التقليدية.



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
- استخدم برامج تشفير الملفات (files encryption).



- استخدم مرشحات رسائل البريد الإلكتروني (filters) وخدمات 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 بواسطة قبل فتحها .
- استخدم مواقع فحص المنافذ (ports) للتأكد 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 إرسال أرقام بطاقات الإئتمان عبر الشبكات اللاسلكية (wi-fi) غير الآمنة كالموجودة في المطارات والمقاهي على سبيل المثال



أمن وسلامة الأطفال:

- شارك الأطفال متعة تصفح واستخدام خدمات الإنترنت لكي تكون قريباً من تصرفاتهم.
- ضح جهاز الحاسوب المتصل بالإنترنت في غرفة العائلة.
- ناقش عملية الاستخدام وضع ضوابط وشروط لها حتى يشعر الطفل بأهميتها.
- تأكد من وجود برامج الحماية من الفيروسات وملفات التجسس والملفات الخبيثة على أجهزة الحاسوب التي يستخدمها الأطفال.
- درب الأطفال على عدم البوح بمعلوماتهم اا
- اعرف أصدقاء أطفالك على الشبكة، وراقب



- استخدم برامج التحكم ومراقبة التصفح والتي تعرف باسم (parental control) والتي تقوم بحظر ومنع المواد المسيئة والخطرة.
- استخدم ميزة الخصوصية (privacy) في المتصفح لحظر المواقع غير المرغوبة والموجودة في خيارات الإنترنت (internet options) في قائمة الأدوات (tools).
- استخدم جهازاً منفصلاً لاستخدام الأطفال، وفي حال تعذر ذلك، قم باستخدام حساباً منفصلاً لهم على نفس الجهاز.









من عمل الطالبة:
رفعة علي ظرمان المري
الصف:
العاشر



*** ●