" السلامة الالكترونية "

قد 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 الاصابة بالفيروسات المدمرة للبيانات والمعلومات المخزنة على الحاسوب. والاختراق للعبث بملفات المستخدم. أو استغلال حاسوبه بقصد الاساءة إلى آخرين. إلى سرقة البيانات الشخصية بقصد الانتحال أو الإبتزاز. 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

:

- تجاعرف جيداً مع من تتعامل قبل الكشف عن أية معلومات.
- نب 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 أية معلومات حساسة ككلمات السر وأرقام بطاقات الإئتمان 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 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 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.

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 (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 بواسطتها 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 الائتمان عبر الشبكات اللاسلكية (Wi-Fi) غير الآمنة كالموجودة في المطارات والمقاهي على سبيل المثال.

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 الشخصية على الشبكة.
- اعرف أصدقاء أطفالك على الشبكة، وراقب محادثاتهم ورسائلهم.
- 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).

نصائح لتجنب المخترقين:-

- استخدم برامج مكافحة الفيروسات والجدران النارية (firewalls) لتأمين جهاز الحاسوب واعمل على تحديثها باس

- استخدم برامج مكافحة الفيروسات والجدران النارية (firewalls) لتأمين جهاز الحاسوب واعمل على تحديثها باستمرار.

•قم بعمل نسخ احتياطية للملفات بشكل دوري.

•تجنب فتح حساباتك المصرفية على الشبكة أو ارسال أرقام بطاقات الائتمان عبر الشبكات اللاسلكية (Wi-Fi) غير الآمنة كالموجودة في المطارات والمقاهي على سبيل المثال.

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 (filters) وخدمات مكافحة البريد غير المرغوب فيه (anti-spam).
•قم بعمل نسخ احتياطية للملفات بشكل دوري.

عيوبها:

-تحتاج للبطاريات أو مصدر كهربائي وفي أي وقت.

-السيجارة نفسها أو مستلزماتها مثل شرائط النيكوتين قد لا تتوفر في الأماكن النائية بعكس السجائر.

-قد تساعد في علاج الإدمان لكنها تعزز العادة الموجودة في التدخين بل وقد تحببها لغير المدخنين خاصة المراهقين.

-لا زالت في طور الحاجة لدراسات علمية مكثفة حتى يعترف بها عالميا من قبل الكثير من منظمات الصحة وخاصة حول تأثيرها على المدى البعيد على الجسم أو احتوائها على سموم غير معروفة لحد الآن.

شبكه الانترنت

على الرغم من الآفاق الواسعة التي فتحتها شبكة الإنترنت، وعلى الرغم من المتعة التي يعيشها المستخدم عند استخدامه لخدماتها أو حين ابحاره 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 الإنتهاك أو الاساءة. علاوة على أنها اصطلاح يستخدم للإشارة إلى حماية الأطفال أثناء استخدامهم لشبكة الإنترنت. أما الأمن فهو توفير الحمابة لضمان أمن المعلومات والبيانات والخصوصية الشخصية. وهي بذلك تشمل حماية الملفات والعتاد.

بطاقة إضافية على الموضوع الرابع

الاسم طالبتان: حليوه محمد ناصر
دلموك،مها صالح الغيثاني
الصف:الثامن
إشراف المعلمة :عواطف كرار
مشروع :الحاسوب عن سلامه الكترونيه