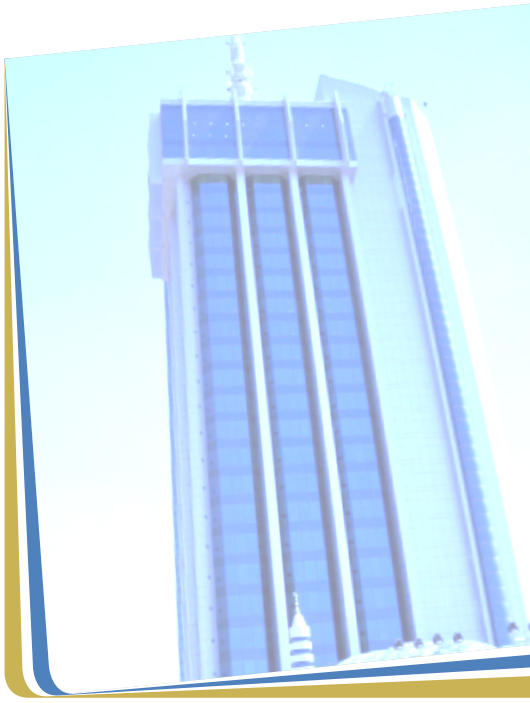
المحتويات



إعـــداد :

م . محمد محمد خير المبارك

م . منى محمد الحسن حـران

م . معتز الصـــــادق اسحاق

راجعـــه :

د . يحي عبد الله

تصميم :

أيمن محمد حمد عبد الباقي (سرمد)

الخرطوم – برج الاتصالات

بري – شمال كبري المنشية

ص . ب : ٢٨٦٩ رمز : ١١١١١

هاتف : ٠٠٢٤٩١٨٧١٧١٢٤٧

فاكس : ٠٠٢٤٩١٨٧١٧١٤٤٤

بريد الكتروني : contact@cert.sd

الخرطوم – السودان

للتواصل معنا : www.facebook.com/SudanCERT

للتبليغ عن جريمة الكترونية : incident@cert.sd

للتبليغ عن رسائل ضارة : spam@cert.sd

للتبليغ عن موقع انترنت ضار : filtering@ntc.gov.sd

شكر وعرفان

تتقدم الهيئة القومية للاتصالات ممثلة في المركز السوداني لأمن المعلومات بأسمى آيات الشكر والتقدير والامتنان لكل من ساهم في إعداد هذا الكتيب ونخص بالشكر المركز الوطني للسلامة المعلوماتية بسلطنة عمان ووزارة الاتصالات وتكنولوجيا المعلومات بجمهورية مصر العربية الذين ساهموا في إعداد هذا المنهج من خلال مدنا بعصارة جهدهم .

مقدمة:

أصبحت المجتمعات أكثر إعتماداً من أي وقت مضى على تكنولوجيا الاتصالات والمعلومات (ICT) بصورة عامة وعلى خدمة الإنترنت بصورة خاصة، هذه الاعتمادية المتزايدة تؤدي إلى كثير من المخاطر التي يجب التحكم فيها من خلال المزج بين الحلول التقنية وتطبيق السياسات الأمنية المناسبة بالإضافة إلى تدريب وتوعية مستخدم الانترنت الذي يمثل الحلقة الأضعف في منظومة أمن المعلومات والشبكات.

المادة التي بين يدي القارئ الكريم تمثل مرجعاً متكاملاً لكيفية استخدام الإنترنت بصورة آمنة والإستفادة من خدماتها المتعددة وفوائدها الكبيرة، فالإنترنت أتاحت قدر كبير من المعرفة والتواصل والاتصال والتسلية ووفرت فرصاً للعمل والتعلم والتدريب والعلاج وغيرها.

يهدف هذا الكتيب لخلق جيل من مستخدمي الإنترنت على قدر من الوعي والإدراك والمعرفة والثقة في التعامل مع شبكة الإنترنت وخدماتها المختلفة.

ملحوظة هامة : يستهدف هذا الكتيب تلاميذ المدارس في مرحلتي الثانوي والأساس، ويجب أن يتم تدريس وتدريب هذا المنهج من قبل معلم حاسوب متخصص بعد تلقي دورة تدريبية قصيرة في الاستخدام الآمن للانترنت.


أمن المعلومات

تعريف

أمن المعلومات هو حماية المعلومات ونظم المعلومات من كل تصرف غير مشروع مثل الدخول لأنظمة الغير أو الإستخدام أو الإفشاء أو العبث أو التعديل أو التدمير .

أركان أمن المعلومات

يقوم أمن المعلومات على ثلاث أركان أساسية وهي :

1. التكامل : ويعني ضمان أن محتوى المعلومات صحيح ومكتمل ولم يتم تعديله دون إذن، وأن الأجهزة التي تحتويه سليمة ؛
2. السرية : وتعني ضمان أن المعلومات لا يمكن الوصول اليها الا للشخص المخول له ؛
3. الإتاحة : بما يعنى ضمان إمكانية وصول المعنيين إلى المعلومات عند الحاجة إليها.

أهداف أمن المعلومات الرئيسية هي التكامل – السرية - الإتاحة وهو ما يرمز له اختصاراً ب (CIA) وهي الحروف الأولى من الكلمات : Confidentiality – Integrity - Availability

يتزايد الاهتمام العالمي بأمن المعلومات بصورة يومية وذلك لعدة أسباب :

- زيادة الاعتمادية على أنظمة المعلومات والاتصالات مثل انظمة التجارة الالكترونية والحكومة الالكترونية ؛
- انتشار استخدام شبكات الحاسوب واستخدام الإنترنت لأداء الأعمال ؛

- سرعة التطوير في مجال تقنية المعلومات وبالتالي زيادة عدد الثغرات الأمنية ؛
- تزايد عدد المخترقين وتعدد أساليبهم .

نظم المعلومات

نظم المعلومات هي مجموعة من العناصر التي تقوم بجمع ومعالجة وتخزين واسترجاع وبث المعلومات داخل المؤسسة أو أية جهة أخرى .

أهم التهديدات لنظم المعلومات :

تحديات أمن المعلومات تتسم بالشمول والاتساع، فيما يلي أهم مصادر التهديدات الأمنية لنظم المعلومات :

- المخترقون (الهـــاكرز) ؛
- الموظفون المستـــاؤون ؛
- المؤسسات المنـافسة ؛
- الكـــــوارث الطبيعيـة ؛
- الأخطاء غير المقصودة ؛
- المستخـــــدم نفسه.

في إحدى عمليات المسح لتحديد أهم المهددات لنظم المعلومات ونسب التهديد، ظهر أن أكبر تهديد يكمن في المستخدم نفسه، فهو يشكل ما يزيد على نصف التهديد الإجمالي، بينما لا يشكل الاختراق سوى نسبة ضئيلة جداً، كما أن أخطاء المستخدمين تمثل ضرراً أكثر من العوامل الأخرى مجتمعة.

أخطاء المستخدمين الأكثر شيوعاً

أكثر الأخطاء شيوعاً تتمثل في :

- اختيار كلمة مرور ضعيفة وعدم تجديدها؛
- استخدام نفس كلمة المرور لجميع الحسابات؛
- ترك أجهزة الحاسوب المحمولة دون حماية؛
- ترك جهاز الحاسوب مفتوحاً دون أية مراقبة؛
- فتح مرفقات البريد الإلكتروني المرسلة من أشخاص مجهولين؛
- الأخطاء البشرية (إدخال أو تخزين البيانات بصورة غير صحيحة)؛
- الثرثرة بمعلومات هامة؛
- نشر الفيروسات بوسائل التخزين المتنقلة؛
- عدم تحديث برنامج مضاد الفيروسات ونظام التشغيل.

كلمة المرور

(Password)

مدخل

تعد كلمات المرور (password) واحدة من أكثر الطرق المستخدمة شيوعاً لحماية المعلومات والدخول إلى الأنظمة المشغلة لها ، ورغم أن كلمات المرور تمثل إحدى أضعف الحلقات في منظومة أمن المعلومات بسبب كثرة الأخطاء في استخدامها، إلا أنه يمكن اعتبارها أداة حماية فعالة عند استخدامها بالشكل الصحيح. وبالتالي يمكن اعتبار كلمة المرور خط الدفاع الأول والذي يصبح لا قيمة له عند ممارسة بعض العادات الخاطئة مثل استخدام كلمات مرور ضعيفة أو تدوينها ، هذه العادات تضعف من فعالية كلمات المرور كخط دفاع أول .

صفات كلمات المرور القوية

كلمة المرور القوية هي التي يصعب تخمينها أو الوصول لها باستخدام البرامج المختلفة، فالعناصر التي تجعل كلمة المرور أكثر قوة ومناعة كثيرة منها:

- طولها أي زيادة عدد الحروف والرموز فيها.
- تعقيدها بزيادة الترتيب العشوائي فيها. فكلما زادت الحروف والرموز والأرقام العشوائية، كلما أصبحت الكلمة فريدة أكثر بحيث لا يظهر أي جزء منها في أي قاموس أو غيره من كتب المفردات .

إرشادات كلمة المرور

أجعل كلمة المرور طويلة

- عن طريق زيادة حرف أو رقم أو رمز ؛
- يجب أن لا يقل طول الكلمة عن ٨ حروف/رموز /أرقام ؛

غيِّر كلمة المرور باستمرار

- استخدام كلمة المرور لفترة طويلة يعطي فرصة للمخترق لتجريب جميع الخيارات ؛
- لا تستخدم نفس كلمة المرور السابقة مره أخرى إلا بعد فترة طويلة ؛

أضف بعض التعقيدات

- اجمع بين الأحرف والأرقام والرموز ؛
- يفضل كذلك استخدام الأحرف الكبير والصغيرة معاً ؛

لا تجعل المتصفح يحتفظ بكلمة المرور

- هنالك بعض البرامج التى تقوم بتخزين كلمات المرور فى الحاسوب بحيث يتم استخدامها تلقائيا عند السؤال عنها فى المرات القادمة (تجنب استخدام هذه الخاصية قدر الامكان) ؛

يجب ألا تستخدم معلومات شخصية

- يتوقع المخترقون معلومات مثل اسمك، تاريخ ميلادك ، رقم الهاتف وغيرها ؛
- كذلك يجب تجنب الأسماء المشهورة مثل أسماء المناطق ؛

تجنب الترتيب والتكرار

مـن السهـل اكتشـاف كلمـة مـرور على شـاكلة (٢٢٢٢٢٢) أو (١٣٥٧٩) أو (asdfgh)

لا تستخدم كلمات المعاجم

كلمات المعجم يمكن الوصول إليها من خلال برامج سهلة الاستخدام (حتى ولو كانت باللغة العربية)

نواهـــــــي

- لا تستخدم نفس كلمة المرور في أكثر من نظام ؛
- لا تترك أحداً ينظر إليك وقت إدخال كلمة المرور ؛
- لا تعط كلمة المرور لأحد ولا تشارك بها أحداً ؛
- لا تكتب كلمة المرور ولا ترسلها بالبريد ؛
- لا تختر (تذكر كلمة مروري) على الحواسيب المشتركة؛
- لا تعد استخدام كلمات المرور القديمة ؛
- تجنب استخدام كلمة مرور فارغة .

اختيار كلمة المرور

من الطبيعي أن يجد الناس صعوبة في حفظ كلمة المرور القوية فَقَلَّ من يحفظ ثمانية أحرف عشوائية تتغير باستمرار. لذلك ووفقاً للدراسات فإن قرابة نصف مستخدمي الحاسوب لا يغيرون كلمات المرور دورياً، بل يتركونها في الوضع التلقائي، بينما يستخدم معظم المستخدمين كلمة المرور ذاتها لأكثر من حساب إلكتروني.

كيف نستخدم كلمة مرور قوية

فيما يلي طريقة سهلة لإنشاء كلمة مرور قوية يسهل حفظها:

فمثلا يمكن استخدام مقولة من كتاب ما، مقطع من قصيدة، أو نشيد، مثل:

easy come easy go

بالتأكيد أنك ستطبعها دون فراغات بين كل كلمة والأخرى ولإضفاء مزيد من التعقيد يمكنك استبدال أحد الحروف المتكررة برقم ، أي كما يلي:

E7sycomee7sygo

وباختبار قوة هذه الكلمة ستجد أنها تحقق أعلى مراتب التقويم.

طرق اختراق كلمة المرور

- الطريقة السهلة لكسر كلمات المرور هي أن يقوم المخترق بتخمينها، لأن الكثير من الناس يستخدمون معلومات شخصية كالأسماء العائلية وتواريخ الميلاد وغيره ؛
- والطريقة الثانية باستخدام برامج تستطيع فك تشفير كلمات المرور معجمياً بلغات مختلفة، وحساب الاحتمالات الممكنة لكلمة المرور بخلط الأحرف والأرقام والرموز ؛
- قد يتبين من هذا بأنه من المستحيل إيجاد كلمة مرور لا تكسر وهذا صحيح إلا أن الصحيح أيضاً أن كلمة المرور القوية تجعل عملية تخمينها أو فك تشفيرها عملية طويلة ومملة إلى درجة قد تؤدي بالمخترق إلى الإحجام عن العملية والتركيز على غيرها.

تذكر : كثير من حالات اختراق كلمات المرور لا تتم بالبرامج المعقدة بل بسبب الإهمال واختيار كلمات سهلة التوقع .


أمن الحاسب الشخصي

مدخل

إستخدام الحاسوب من غير حماية يجعله عرضة لهجمات من قبل أشخاص غير مصرح لهم لذلك يتوجب علينا استخدام وسائل تقنية مثل الجدار الناري ومضاد الفيروسات بالإضافة للتعامل بحذر ووعي .

الجدار الناري (Firewall)

هو جهاز يتم تركيبه عند مدخل الشبكة أو برنامج حاسوبي يتم تنصيبه في جهاز الحاسوب للتحكم في البيانات الواردة للجهاز (أو الشبكة) والصادرة منه.

فيما يلي بعض الارشادات الهامة لتفعيل الجدار الناري :

- حصن جهازك باستعمال برنامج جدار ناري Firewall
- هيئ الجدار الناري لمنع المستخدمين غير المخول لهم من الوصول إلى جهازك ؛
- تحكم في إعدادات الجدار الناري وأغلق المنافذ (Ports) غير المستغلة ؛
- لا تسمح للبرامج غير المعروفة بالاتصال بالانترنت ؛
- لا تتجاهل تنبيهات الجدار الناري .

الفيروسات (Viruses)

الفيروس هو برنامج مستقل صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها وذلك لتقوم بتنفيذ بعض الأوامر التي غالباً ما تؤدي إلى إلحاق الضرر بالحاسوب المصاب أو السيطرة عليه .

الفيروس هو برنامج مستنسخ لنفسه، عادة ما يكون قادراً على إحداث ضرر كبير بالملفات والبرامج على نفس الحاسوب. الفيروس عادة لا يستطيع الانتقال إلى حاسوب آخر بدون مساعدة بشرية ولذلك ينتشر عادة عبر البريد الإلكتروني أو عبر وسائط التخزين الخارجية أو

عبر اخفاء نفسه في الملفات التي يتم انزالها من الانترنت .

أضرار الفيروسات

تتفاوت آثار الفيروسات تفاوتاً واسعاً اعتماداً على ما تهدف إلى القيام به. كما أن الفيروسات يمكنها القيام بأعمال كثيرة ومختلفة حسب رغبة مصممها، من ذلك :

- تدمير البيانات وبرامج التشغيل ؛
- إنشاء رسائل مزعجة ؛
- تشغيل برامج غير مطلوبة ؛
- ابطاء سرعة عمل الجهاز ؛
- سرقة البيانات مثل أرقام الحسابات وكلمات المرور أو أرقام بطاقات الائتمان .

الديدان (Worms)

تتشابه الدودة مع الفيروس حيث أنها برنامج مستنسخ لنفسه، لكنها تستخدم الشبكة لإرسال نسخ منها إلى حواسيب على الشبكة ويمكنها الانتقال دون تدخل المستخدم. تؤدي الدودة إلى شغل موارد الجهاز والشبكة بشكل كبير.

أحصنة طروادة (Trojan Hourse)

حصان طروادة هو برنامج تخريبي يلبس زى البرامج الصالحة لكنه خبيث. يسمى هكذا لأنه لا يتناسخ كالفيروس بل يفتح باباً خلفياً ببرنامج تقوم بإنزاله، كلعبة مثلاً، ليدخل المخترق من هذا الباب فيسيطر على حاسوبك أو يتجسس عليك.

برامج التجسس (Spyware)

برامج التجسس هي برامج تقوم بجمع معلومات عن حاسبك بغير علمك وتنتشر عادة عند إنزال برامج من الإنترنت.

أعراض الإصابة بالفيروسات

أعراض الإصابة بالفيروسات تتفاوت تبعاً للفيروس فهي قد تؤدي إلى :

- مشاكل في العرض على الشاشة ؛
- فشل الحاسب في الإقلاع أو بطء غير طبيعي أثناء ذلك ؛
- توقف النظام ؛
- نشاط غير مألوف في مشغل الأقراص ؛
- تكرار ظهور رسائل الخطأ في أكثر من برنامج ؛
- توقف بعض البرامج عن الاستجابة ؛
- حدوث بطء شديد عند تشغيل الجهاز أو عند تنفيذ بعض التطبيقات ؛
- مسح الملفات أو تدميرها ؛
- تخريب القرص الصلب.

تنتشر الفيروسات والديدان وبرامج التجسس عادة بإحدى الطرق التالية :

- وسائط تخزين خارجية كالأقراص المدمجة وذاكرة الفلاش .
- تنزيلات الإنترنت .
- مرفقات البريد الإلكتروني .

كيفية حماية الجهاز من الفيروسات

- تأكد من تنصيب برنامج موثوق مضاد للفيروسات ؛
- تأكد من تحديث برنامج مضاد الفيروسات بصورة دائمة ؛
- قم بعمل مسح دوري لجهازك ؛
- احذر من عمل مسح لجهازك بالبرامج المجانية التي تظهر لك خلال تصفحك أحياناً؛
- تأكد من استخدام برامج مكافحة التجسس (Anti spyware) ؛
- أحفظ بياناتك احتياطياً على وسائط خارجية بشكل دوري ؛
- افحص كل مرفقات البريد الإلكتروني بمضاد الفيروسات قبل فتحها، واعتنِ عناية خاصة بملفات التنفيذ ؛
- لا تفتح مرفقات بريد لا تعرف مرسله حتى لو كان العنوان ملفتاً مثل (ربحت مليون دولار) ؛
- إن كنت تستخدم حاسباً مشتركاً مع غيرك فاتفقوا على أسلوب واضح لاتخاذ الحيطة عند إدخال وسائط التخزين الخارجية ؛
- قم بتحميل البرامج من مواقع تثق فيها فقط وافحصها قبل الفتح .

من الخطأ الاعتقاد أن الجدار الناري أو مضاد الفيروسات أو الاثنان معاً سيمنحان شبكتك أو حاسوبك تاميناً كاملاً ولكنهما بالضرورة يمنعان كم هائل من الاضرار على أنظمتك.

برامج الحاسوب

إن البرامج المنتشرة على الانترنت منها المفيد ومنها الضار لذلك يجب علينا التحقق منها، وأسلم الطرق للتحقق هي تحميل البرامج من مصادر موثوق منها (قبل أن تقوم بتحميل أي برنامج لابد أن يكون جهازك مزود بمضاد الفيروسات حتى لا تقع فريسة للبرامج الخبيثة والتي في أحيان كثيرة تدمر نظام حاسوبك) .

هنالك بعض الأمور التي يجب عليك التقيد بها دائماً لحماية الحاسوب والمعلومات الخاصة بك ، مثل :

- ينصح بعدم الدخول على حاسوبك باستخدام حساب مدير النظام (Administrator) والذي تكون له صلاحيات كاملة على نظام التشغيل ؛
- استخدم كلمة مرور قوية للدخول (راجع إرشادات " كلمة المرور") ؛
- حدِّث نظام التشغيل باستمرار عن طريق موقع الشركة مثل "مايكروسوفت Microsoft " أما في حال علمك بوجود ثغرة ما في نظام التشغيل قم بتحميل التحديث بشكل يدوي من موقع الشركة ؛
- استخدم برنامج مكافحة فيروسات على أن يكون محدثاً ومفعلاً ؛
- استخدم برنامجا لمكافحة برامج التجسس على أن يكون محدثاً ومفعلاً ؛
- ينصح بانزال برامج وتطبيقات من المواقع الموثوقة فقط؛
- اقرأ النصوص التي تظهر أمامك جيداً قبل الاختيار .


الهندسة الإجتماعية
(Social Engineering)

مدخل

تعرف الهندسة الاجتماعية – في علم الحاسوب – على أنها فن التواصل مع الناس اجتماعياً ثم خداعهم وجعلهم يقدمون على تنفيذ أعمال أو البوح بمعلومات تساعد في الوصول لأنظمتهم الخاصة. يتضح من التعريف السابق أن الهندسة الاجتماعية هي اختراق غير تقني بل يعتمد بالشكل الأساسي على التصرفات العفوية للمستخدمين، أي استخدام الخداع للحصول على معلومات بالاستفادة من مهارات التعامل.

طرق الهندسة الاجتماعية

غالباً ما يعتمد المخترق إلى حيلة سهلة وذلك بأن يسأل أسئلة بسيطة عن طريق الهاتف أو البريد الإلكتروني أو مباشرة منتحلاً شخصية يمكن الوثوق بها مثل مهندس دعم فني أو رجل قانون.

كما يعتبر التصيّد وجها آخر للهندسة الاجتماعية، فقد يرسل المخترق لك بالبريد تنبيها بأن عليك تغيير كلمة المرور لسبب ما ويعطيك وصلة مزيفة، وعند النقر على الوصلة تجد أن الواجهة هي نفس الواجهة التي تتعامل معها تماماً لكن الذي تجهله أن العنوان مزيف.

إحدى الطرق المستخدمة لجمع معلومات عن الشركات هي استخدام صناديق القمامة بحثاً عن فواتير أو أي مستندات أو معلومات شخصية أو مصرفية مفيدة.

عملية الاختراق لا تتم بالضرورة باستغلال ثغرات تقنية في نظامك، بل قد تكون باستغلال ثغرات بشرية.

وسائل الحماية من الهندسة الاجتماعية

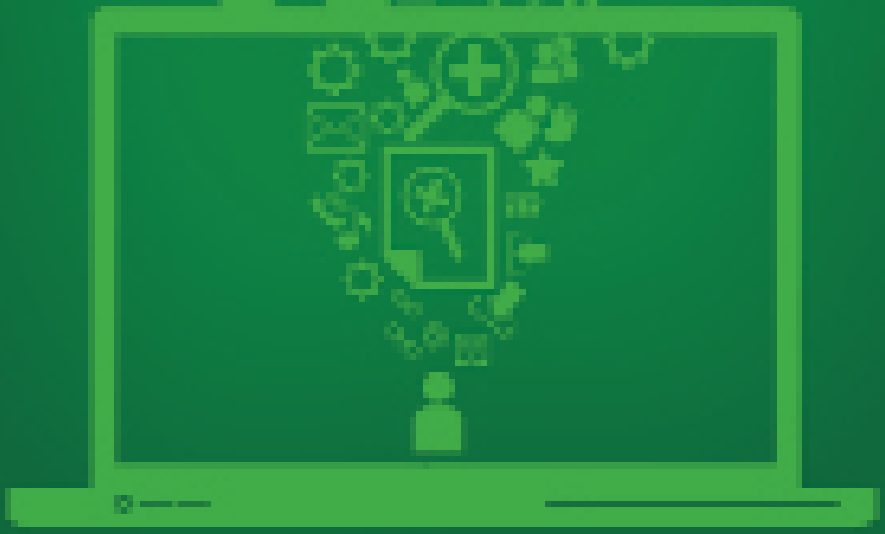
هذه بعض الطرق التي ينصح بإتباعها للوقاية من خطر الهندسة الاجتماعية :

- لا تتحدث بشكل صريح مع أي شخص لا تعرفه حق المعرفة عن الأنظمة و الإعدادات المستخدمة لديك ؛
- على الشخص عدم التردد أبداً بالسؤال عن هوية طالب المعلومة ؛
- عدم الإفصاح عن المعلومات الشخصية أو المالية من خلال البريد الالكتروني إلا عند التأكد من سلامة الأمر (بالتشفير مثلاً) ؛
- عدم الضغط على أي رابط بالبريد الالكتروني بقصد تحديث بيانات شخصية لأن هذه الروابط قد تؤدي إلى صفحات مزيفة ؛
- التخلص من الأوراق فور الانتهاء منها باستخدام آلة تقطيع الورق ؛
- يجب تدريب الموظفين على كيفية التعامل مع الهندسة الاجتماعية .

تذكـــر

لا تحاول استخدام الهندسة الاجتماعية لأنها تمثل نوع من أنواع الاختراق وقد تتعرض للمسائلة القانونية بسببها.

أمن البريد الإلكتروني



مدخل

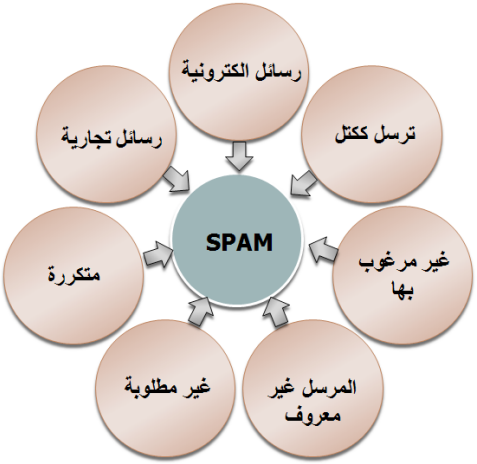
يعتبر البريد الإلكتروني وسيلة لتبادل الرسائل الالكترونية عبر الإنترنت. كما أنه واحد من أكثر الوسائل لانتشار الفيروسات وهو وسيلة سهلة لترويج الإعلانات ويستخدم أيضاً للاحتيال (phishing).

مصادر التهديد الأمني في الرسائل الإلكترونية

1. الملفات المرفقة : ينصح بعدم فتح المرفقات لرسائل من مصادر غير موثوقة ؛
2. الوصلات المضمنة داخل الرسالة : كثير من الروابط داخل الرسائل الالكترونية تؤدي الى انزال برامج خبيثة ؛
3. الرسائل الاقتحامية (SPAM) : رسائل غير مرغوبة وغير مطلوبة وغالباً ما يكون مصدرها شركات ومواقع تحصل على عنوان بريدك الإلكتروني فتقوم بتبادل هذه العناوين فيما بينها أو تقوم ببيع هذه العناوين لغرض التسويق .
4. التصيّد (Phishing) : التصيّد هو استدراج مستخدمي شبكة الإنترنت إلى مواقع وهمية باستخدام البريد الإلكتروني في محاولة لسرقة كلمات مرور أو معلومات حسابات مصرفية أو غيرها من البيانات الهامة.

   يتم اصطياد الضحايا عن طريق إرسال رسائل مزيفة تشبه الرسائل الرسمية من مؤسسة أو شخص يثق به المستلم. ويكون الغرض من هذه الرسائل المزيفة هو خداع المستقبل لتقديم معلومات شخصية أساسية عن أنفسهم وذلك بالطلب منهم تحديث بياناتهم بالضغط على وصلة تأخذهم مباشرة لموقع مزيف.
5. الرسائل المتسلسلة : انتشرت مؤخراً رسائل تحكي قصصاً محزنة لأطفال أو كبار تعرضوا لحوادث شخصية ويطلب منك القيام بإرسال الرسالة إلى من تعرف، وتقوم أنت بالعمل نيابة عنه بينما يقوم هو بجمع العناوين وبيعها أو يكون قد أرسل معها فيروساً أو برنامج تجسس. عادة ما تهدف مثل هذه الرسائل لجمع العناوين أو التسويق لمنتج ما.

خصائص الرسائل الاقتحامية (SPAM)



تذكر .. يمكن استخدام البريد الإلكتروني بينة أمام القضاء.

أضرار الرسائل غير المرغوب فيها

الرسائل الاقتحامية أو المتسلسلة تشكل عبئاً على نظام البريد الإلكتروني فهي تهدر الموارد عن طريق تأثيرها السلبي في سرعة حركة مرور البيانات واستنزاف سعات التخزين، كذلك يستغرق مستخدم البريد وقتا طويلاً في الإطلاع على هذه الرسائل ومسحها بالإضافة لما تحتويه في كثير من الأحيان لفيروسات ومواد ضاره.

لاستخدام البريد الالكتروني بأمان ينصح بـ :

- استخدم أكثر من بريد الكتروني ؛
- لاتفتح مرفقات دون التأكد من محتواها؛
- لاتفتح رسائل من مصادر غير معروفة لديك؛
- لاتستجيب للرسائل المغرية مثلا (ربحت مليون دولار)؛
- لاترسل معلومات شخصية عبر البريد الالكتروني؛
- احفظ نسخ احتياطية للبريد الهام؛
- احرص على قراءة النصوص التي تظهر أمامك جيدا قبل الاختيار؛
- استخدم كلمات مرور (passwords) صعبة ومعقدة ؛
- لاتستخدم كلمات مرور يسهل توقعها (مثل اسمك أو رقم هاتفك)؛
- أغلق الايميل عند الانتهاء من استخدامه (logout)؛
- لاتستخدم المفتاح reply all الا بعد مراجعة جميع الايميلات المرسلة لها الرسالة؛
- لاتستخدم مفتاح forward الا اذا تأكدت من انك ترغب في ارسال المرفقات أيضاً؛
- لاتثق في اصدقاء الانترنت ؛
- إحرص على استخدام بريد إلكتروني رسمي (إن وجد) بدلاً عن البريد المجاني مثل (hotmail, yahoo) في الأعمال الرسمية؛
- إحرص على إضافة بريد إلكتروني آخر لإستخدامه في إسترجاع البريد الإلكتروني الرئيسي في حال فقدانه أو أختراقه؛
- راجع إعدادات الخصوصية والحماية لديك؛
- لا تستخدم نفس كلمة المرور للحسابات الإلكترونية المختلفة.

أمن شبكة الانترنت

مدخل

تعتبر شبكة الإنترنت التي تضم مجموعة كبيرة من الشبكات المترابطة حول العالم وسيلة هامة تتيح لملايين المستخدمين الولوج إلى كم هائل من المعلومات إضافة إلى التواصل والاتصال وتبادل المعلومات والرسائل وغيرها.

إعتبارات أمنية

عند زيارة موقع ما فإن متصفح الإنترنت يترك أثراً لأنشطة الزائر عند مزود خدمة الإنترنت وفي جهازه، وذلك عن طريق الكتابة في ملفات التسجيل وتخزين الملفات المؤقتة وملفات الكوكيز في القرص الصلب.

إعداد المتصفح

يمكن تهيئة متصفحات الويب بدرجات أمن مختلفة تناسب احتياجاتك الأمنية، ويتم ذلك عن طريق تغيير إعداد مستوى الأمن بالمتصفح .

يختلف إعداد مستوى الأمن باختلاف نوع المتصفح، إلا أن الثابت هو وجود علاقة عكسية بين المرونة الوظيفية ودرجة الأمن في إعدادات المتصفح، فكلما زادت درجة الأمان قلت قدرتك على دخول المواقع وتنفيذ بعض العمليات إلا أن احتمال تعرضك للتهديدات يكون أقل والعكس صحيح .

للأسف، في الكثير من الأحيان يتطلب أن يكون مستوى الأمن منخفضاً من أجل الاستفادة من مواقع الإنترنت التفاعلية، ومع ذلك يحسن أن تعلم بأن لديك الخيار في تحديد درجة الأمن التي تناسب النشاط الذي تقوم به .

قواعد إستخدام الإنترنت الآمن

من القواعد الأساسية لاستخدام الإنترنت بأمان :

- لا تقدم أي معلومات شخصية لأصدقاء الإنترنت؛
- التفاصيل الخاصة بك يمكن استخدامها لخداعك أو بيعها لآخرين؛
- استخدم دائماً المواقع الموثوق بها فقط؛
- تأكد من إغلاق متصفح الإنترنت بعد الانتهاء من استخدامه؛
- لا تقم بإنزال أي ملفات من الإنترنت ما لم تكن من مصادر موثوقة؛
- إستخدم البرامج المضادة للفيروسات وحدثها باستمرار؛
- توخى الحذر أثناء التصفح ولا تقم بزيارة المواقع غير المشروعة؛
- تعامل بحرص مع النوافذ المنبثقة فالبرمجيات المضادة للفيروسات قد تستخدم النوافذ المنبثقة لإيصال الرسائل المهمة إليك وهذه النوافذ يجب ألا تتجاهلها؛
- لا تحاول التخلص من النوافذ المنبثقة عند ظهورها بالضغط على زر «موافق» بل أغلقها فوراً؛
- قم بتحديث متصفح الانترنت باستمرار؛
- أضبط إعدادات المتصفح لتحديد المواقع التي يُسمح لها باستخدام ملفات الكوكيز (cookies) ؛
- تأكد من ضبط إعدادات الأمان والخصوصية والمحتوى لمتصفح الإنترنت.

مدخل :

يدل مفهوم التواصل على عملية نقل الأفكار والتجارب وتبادل الخبرات و المعارف والمشاعر بين الأفراد والجماعات، فهو جوهر العلاقات الإنسانية والمتحكم في تطورها.

حديثاً اجتاحت مواقع التواصل الاجتماعي أو ما يعرف بالشبكات الاجتماعية على الانترنت مثل «فيسبوك» و«تويتر» و «الواتساب» العالم بأسره، وبات الجميع من مختلف الأجيال يستخدمونها.

تعريف :

هي عبارة عن مواقع انترنت او برامج تقدم مجموعة من الخدمات للمستخدمين مثل المحادثة الفورية والرسائل الخاصة والبريد الإلكتروني والفيديو والتدوين ومشاركة الملفات وغيرها من الخدمات التي تسهل عملية التواصل والاتصال بين مستخدمي تلك الخدمات.

لاستخدام شبكات التواصل الاجتماعي بأمان ينصح بـ:

- تجنب استخدام كلمة مرور ضعيفة؛
- تجنب استخدام نفس كلمة مرور البريد الالكتروني في المواقع الاجتماعية؛
- اختر أصدقائك بعناية؛
- تجنب كتابة معلومات شخصية عنك وعن أسرتك؛
- تأكد من قيود الخصوصية لديك؛
- كن حذراً عند فتح التطبيقات المجهولة وتجنب فتح الروابط غير الموثوق بها؛
- لا تستقبل ملفات من أشخاص لا تعرفهم جيداً؛
- لا تشارك في أعمال ضارة على الانترنت مثل (إشانة السمعة والتحريض والابتزاز وغيرها)؛
- لا تستجيب لمواقع وروابط الاستدراج.

أمن الشبكات اللاسلكية

مدخل

مع تزايد استخدام الشبكات اللاسلكية في العمل والمنازل والأماكن العامة تبرز مخاوف كثيرة من هذه التسهيلات التقنية في الاتصال. يتم الدخول للشبكات اللاسلكية عبر نقطة وصول (access point) وهي عبارة عن جهاز متصل بالانترنت ويتم الدخول على هذا الجهاز لاسلكياً للوصول لشبكة الانترنت.

مصادر تهديد الشبكات اللاسلكية

نقاط ضعف الشبكات اللاسلكية متعددة، أهمها:

- تسمية جهاز المخترق باسم نقطة التغطية اللاسلكية المتوفرة لإيهام المتصلين بأنها حقيقية ؛
- التقاط مسمى الموزع عن طريق برامج خاصة للكشف وتخمين كلمة مرور الشبكات اللاسلكية ؛
- بسبب اعتمادها على الطيف الكهرومغناطيسي فإنها عرضة للتصنت ؛
- عدم إلمام المستخدمين بتفعيل إجراءات الحماية، ومن أمثلة ذلك ترك مسمى الموزع الأصلي دون تغيير مما يسهل على المهاجم الاشتراك في الشبكة اللاسلكية ؛
- الاعتماد على المعلومات الافتراضية للأجهزة (Default settings).

خطوات لحماية الشبكات اللاسلكية

تتطلب حماية الشبكات اللاسلكية اتخاذ عدد من الخطوات الاحترازية، مثل:

- أعط اسماً مختلفاً لشبكتك اللاسلكية غير الذي وضعه موزع الشبكة؛
- عند العمل دون اتصال اقفل الاتصال اللاسلكي في بطاقة الحاسوب؛

- استخدم أجهزة المودم المعروفة ذات السمعة الأمنية الجيدة ؛
- غيِّر القيم الافتراضية التي تأتي مع جهاز المودم مثل (admin) ؛
- فعِّل خاصية التشفير وذلك من خلال استخدام التقنيات الحديثة مثل WPA؛
- أوقف نظام إل (DHCP) واستخدام عنوان انترنت (IP) ثابت؛
- حدِّث برامج التشغيل الخاصة بجهاز المودم (Modem) وذلك من خلال الزيارات الدورية للموقع الخاص بالشركة المصنعة ؛
- عطِّل خاصية "التشغيل عن بعد" لجهاز المودم الخاص بك ؛
- فعِّل خاصية "إخفاء" إذا كان جهازك يدعم تلك الخاصية ؛
- فعِّل خصائص التحكم بالدخول مثل استخدام كلمات المرور أو استخدام العناوين الفيزيائية لأجهزتك .

تأمين الهواتف الذكية

مدخل

يوماً بعد يوم تزداد أهمية الهواتف الذكية لكافة فئات المجتمع فبالإضافة لفوائدها الأولية المتمثلة في الاتصال هاتفياً وعبر الفيديو والرسائل النصية القصيرة ورسائل البيانات فقد أصبحت الهواتف الذكية تقدم معظم أو كل الخدمات التي يقدمها الحاسب الآلي خاصة في بيئة الانترنت التي أتاحت عدد كبير جداً من التطبيقات والبرامج سهلة الانزال والاستعمال. لما سبق فان هذه الهواتف أصبحت معرضة لعدد غير محدود من المخاطر مثل الفيروسات والديدان وبرامج التجسس والسرقة وغيرها.

للحد من هذه المخاطر فإننا ننصح مستخدمي الهواتف الذكية بالتالي :

- الحفاظ على الهاتف وعدم تركه في الأماكن العامة ولو لفترة قصيرة؛
- ضع كلمة مرور صعبة التخمين على الهاتف؛
- يجب تحميل برامج الحماية المضادة للفيروسات؛
- يجب عمل نسخة احتياطية بشكل دوري للحد من الخسائر؛
- عدم تحميل البرامج أو الملفات من المواقع المشبوهة؛
- عدم فتح البريد الالكتروني من الأشخاص غير المعروفين؛
- إبقاء البلوتوث بوضع عدم التشغيل في حالة عدم الحاجة إليه؛
- تجنب حفظ أي معلومات حساسة على الهواتف ككلمات المرور أو معلومات عن الحسابات البنكية فإن كان لابد من ذلك فيجب وضع كلمة مرور قوية لا يمكن تخمينها وتشفير البيانات المهمة؛
- تجنب تخزين الصور الخاصة في هاتفك؛
- يجب تحميل البرامج التي تمكن المستخدم من إقفال الجهاز و مسح البيانات و تحديد موقعه عن بعد في حالة ضياعه أو سرقته؛

حماية الهواتف الذكية من الفيروسات

يمكن للهواتف الذكية أن تتعرض للفيروسات عن طريق تحميل الملفات من مواقع الانترنت غير الموثوق بها أو عن طريق البريد الالكتروني أو عن طريق الوسائل التخزينية المتحركة ثم تقوم باستغلال نقاط الضعف في نظام التشغيل إما بتدمير الجهاز أو سرقة المعلومات منه.

وللحد من خطورة الفيروسات والبرامج الضارة ينصح بتحميل البرامج المضادة للفيروسات والتي تعمل على البحث عن هذه الفيروسات وتدميرها أو منعها، ويجب الالتزام بتحديث هذه البرامج بشكل مستمر لتستطيع التعرف على الفيروسات الجديدة. كذلك يجب عدم تحميل أو فتح البرامج من المواقع أو الأشخاص غير الموثوق بهم أو غير المعروفين.

حماية الهواتف الذكية من برامج التجسس

برامج التجسس هي تلك البرامج التي تقوم بمراقبة سلوك المستخدم دون علمه وتقوم كذلك بجمع المعلومات الشخصية عنه، مراقبة المواقع التي يزورها؛ التنصت على مكالماته، أو تغيير في إعدادات الجهاز بدون علمه أو موافقته على ذلك.
يمكن للهواتف الذكية أن تصاب ببرامج التجسس عن طريق تثبيت البرنامج بشكل خفي خلال تثبيت برنامج آخر يرغب المستخدم فيه أو عن طريق البرامج الانبثاقية التي تفاجئ المستخدم بالظهور كإعلانات أثناء تصفح الإنترنت ومحاولة تحميل نفسها على الهاتف أو عن طريق خداع المستخدم بإظهار تنبيهات زائفة تخص نظام التشغيل أو الإضافات التي تكون علي المتصفح مثل شريط أدوات إضافي وصناديق البحث الإضافية.

كما تعتبر البرامج التي تظهر بشكل برامج مضادة للتجسس من أخطر الحيل المستخدمة لتحميل البرامج التجسسية حيث تقوم بالتخفي وإقناع المستخدم بأنها أداة تساعد على كشف وإزالة البرامج التجسسية.

لحماية الأجهزة من هذا الخطر ينصح بإتباع الإرشادات التالية:

- استخدام البرامج التي تعمل على اكتشاف وإزالة البرامج التجسسية (anti spyware)؛
- يجب على المستخدم أن يقرأ اتفاقية الترخيص بشكل كامل قبل تثبيت أي برنامج، لأن بعضها تنص بوضوح بأن البرنامج سيقوم بمراقبة سلوكك وإرسال بيانات لجهة خارجية؛
- تحديث نظام التشغيل والبرامج المهمة بشكل دوري ومستمر؛
- تثبيت برامج لمكافحة الفيروسات وجدار الحماية؛
- عدم تحميل أو فتح البرامج من المواقع أو الأشخاص غير الموثوق فيهم أو غير المعروفين؛
- يجب توخي الحذر عند تثبيت البرامج المجانية ، لأن عدداً كبيراً منها يقوم بتثبيت بعض البرامج التجسسية أو الدعائية .


دليل إرشادي لأولياء الأمور

مدخل

الانترنت هي شبكة تتكون من ملايين الشبكات الأصغر حجماً والمرتبطة مع بعضها البعض والتي تضم بدورها أعداداً متزايدة ومتطورة من الحواسيب والهواتف السيّارة والأجهزة اللوحية. هذه الحواسيب تقوم بتبادل البيانات فيما بينها باستخدام بروتوكول الانترنت وتتيح عدد مقدر من الخدمات للمستخدمين .

تطورت الانترنت بصورة متسارعة وزادت الخدمات المقدمة من خلالها وأصبحت أكثر أهمية لفئات المجتمع المختلفة فهي تتيح قدر كبير من المعرفة وفرص لا حصر لها للتطور والتعلم والتدرب وتبادل الأفكار وإظهار المواهب كما تخلق فرص مقدرة للعمل والتواصل مع المجتمعات المختلفة والاتصال السهل والتسلية وغيرها من الفوائد الكبيرة .

هذه الاعتمادية المتزايدة على الانترنت أدت لكثير من المخاطر التي يجب علينا جميعاً الانتباه لها والتحكم في أثرها حتى نستطيع أن نصل للمعادلة الأمثل وهي الاستفادة بأكبر قدر من الانترنت مع تضييق احتمالية التضرر منها لأقل قدر ممكن .

يعد الأطفال من أكثر الفئات العمرية استخداماً للانترنت خاصة في ممارسة الألعاب والتواصل عبر الشبكات الاجتماعية وتبادل المعلومات الشخصية. وهذا يتيح فرصاً إيجابية للمشاركة، والابتكار والاستفادة، كما أنه يسمح بالتواصل بين الأطفال ولكنه أيضاً يعرض الأطفال لكثير من المخاطر .

هذا المرشد يهدف لرفع وعي أولياء الأمر وتجهيزهم ليتولوا دورهم الهام في توجيه أطفالهم لاستخدام الانترنت بطريقة ذكية وآمنة كذلك يساعد أولياء الأمر في تعزيز الثقة لدى أبنائهم في استخدام الانترنت والاستفادة من خدماتها المختلفة .

الأمان يمنحك السلامة

1. حماية حاسوب المنزل

وجود حاسوب في المنزل يعني توفر وسيلة تعليمية وترفيهية رائعة للأسرة. إلا أن وضع الحاسوب في مكان عام في البيت ووضع قواعد محددة تتعلق بشروط الاستخدام والوقت الذي يمكن قضاؤه أمام الشاشة يساعد أفراد الأسرة علي أن يظلوا في أمان .

2. تأمين الحاسوب بصورة عامة

يمكن تحقيق الأمان من خلال الفهم الأساسي للمخاطر المحتملة ومعرفة الحلول السهلة. وتشمل هذه الحلول الأدوات التكنولوجية البسيطة ومدى فطنة المستخدم ومعرفته، علماً بأن الفطنة تنمو بالتقدم في العمر والممارسة شأنها شأن أي شيء آخر .

إن الأشياء التي يرجح أن تقوم أنت أو أبناؤك بها علي الحاسوب كاستخدام بطاقات الذاكرة أو الاسطوانات، وفتح المرفقات، قد تنطوي جميعها علي المخاطر، وهي مخاطر تتعلق بالدرجة الأولي ببرامج الحاسوب الضارة أو ما يعرف بالبرمجيات الخبيثة، التي تم تصميمها لإلحاق الضرر بالحاسوب وسرقة المعلومات الشخصية أو ملاحقتك بالدعاية غير المرغوب فيها.

3. مقاومة الرسائل المزعجة والضارة

تمثل الرسائل المزعجة نحو ٨٠٪ من رسائل البريد الإلكتروني المتداولة علي شبكة الانترنت (رسائل غير مرغوب فيها وغير معروفة المصدر ومتكررة). فنشر عنوان البريد الالكتروني دون قصد على الشبكة عند استخدام مجموعة إخبارية أو موقع للدردشة أو منتدى عام أو موقع للتعارف الاجتماعي أو نموذج استمارة علي الانترنت يمكن أن تنتج عنه رسائل مزعجة, وهناك برمجيات معينة تستطيع جمع عناوين البريد الإلكتروني من شبكة الانترنت لتكوين

قوائم بريدية تستغل بعدها في توزيع الرسائل المزعجة بأعداد هائلة .

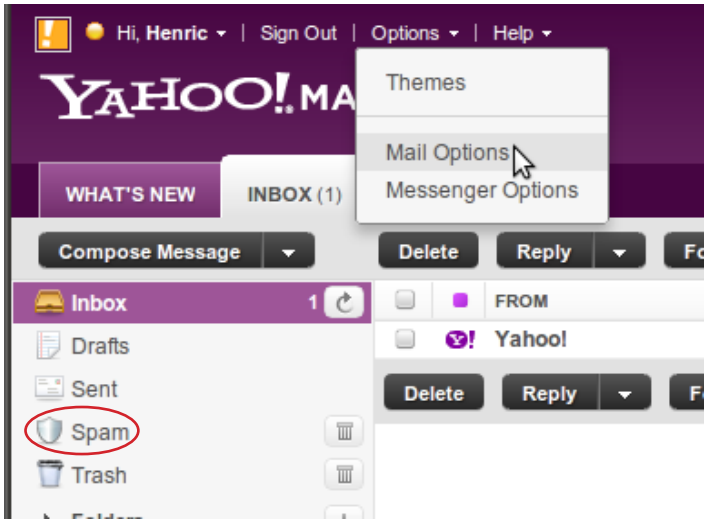
يتعلق هذا النوع من الرسائل في المعتاد بالمواد الإباحية والمستحضرات الطبية والصفقات المالية المشبوهة وغيرها. و قد تكون الرسائل المزعجة مصدراً للبرامج الخبيثة وفي أغلب الحالات توزع هذه الرسائل لأغراض الاحتيال .

إليك بعض النصائح لمساعدتك علي حماية أسرتك من الرسائل المزعجة :

- راجع إعدادات الرسائل المزعجة: يقدم بعض مقدمي خدمة البريد الالكتروني خيارات مقاومة الرسائل المزعجة التي يمكنها أن تنشط داخل برنامج البريد الالكتروني الخاص بك. لكن عليك أيضاً تفقد مجلد الرسائل المزعجة للتأكد من عدم دخول رسائل مطلوبة بطريق الخطأ (انظر الصورة) .

- علم أبناءك ألا يقدموا علي فتح رسائل البريد الالكتروني القادمة من أشخاص مجهولين، فالرسائل المزعجة تحتوي دائماً علي عروض ومرفقات جذابة .

- لا يكفي مسح الرسائل المزعجة بل يجب التبليغ عنها. هنالك جهات كثيرة يمكن التبليغ فيها، منها spam@cert.sd



4. تصفح شبكة الانترنت

حققت الإنترنت منافع لا حصر لها للأطفال في أنحاء العالم، حيث يستفيد الأطفال من تصفح الانترنت في الترفيه وزيارة المواقع التعليمية والتواصل مع أقرانهم وغيرها، ولكن مع كل ما تحتويه الشبكة من مواد مفيدة ومسلية إلا أنها تعرض الأطفال لكثير من المخاطر أبرزها المحتوى غير الأخلاقي والضار مثل المواد الإباحية والعارية والقمار والإساءة إلى الأديان وغير ذلك من أنواع المحتوى غير الملائم .

كما تعتبر محركات البحث وسيلة سهلة ومباشرة للعثور على المحتوى على شبكة الانترنت، ولكن نظراً لأن البحث يعتمد على اختيار الكلمة الدالة، فمن السهل العثور على محتوى غير مطلوب (في الفقرات التالية ستجد نصائح سهلة لتصفح الانترنت بأمان) .

لماذا يدخل أطفالنا على الانترنت

يجب على أولياء الأمر أن يكونوا ملمّين بتفاصيل التجارب التي قد يمر بها أبنائهم أثناء تصفحهم للإنترنت والمخاطر وجوانب الضعف المتصلة بالأنشطة المختلفة على الإنترنت.

يدخل الأطفال إلى الإنترنت لأسباب مختلفة من بينها :

- إنشاء معلومات شخصية ، إدخال معلومات عن أنفسهم ؛
- التواصل مع الآخرين وتقاسم معلومات أو أفكار مع مستخدمين آخرين من خلال الدردشة، ومواقع التدوين، والرسائل الفورية، ومنتديات المناقشة، وخاصية نقل الصوت من خلال بروتوكول الإنترنت ؛
- خلق شخصية افتراضية اختيار صورة مرسومة تمثلهم وتحدد هويتهم في موقع من مواقع الإنترنت ؛
- ممارسة ألعاب تحدي عقولهم والقيام بأنشطة تمكنهم من المشاركة علي الانترنت .
- الرد على الأسئلة يتحدى الأطفال أنفسهم وأقرانهم بالدخول لمواقع تتيح قدر من التحدي؛
- رسم صور، ورسوم متحركة، ورسوم هزلية وتصميم ألعاب كثير من الأطفال يستمتعون بإنشاء محتوى خاص بهم و مشاركته مع أقرانهم، وتنشط مواهبهم عندما يتعاونون مع آخرين من نفس المجتمع الافتراضي ؛
- شراء منتجات بعض المواقع قد تسمح للمستخدمين بشراء منتجات أو خدمات باستخدام أموال حقيقية .

المخاطر وجوانب الضعف المتصلة باستخدام الأطفال للإنترنت

للتواصل عبر الانترنت ميزات كثيرة كما ذكرنا سابقاً, ولكن الواقع قد يأتي بخلاف ذلك أحيانا، فقد يتعرض الأطفال لتجارب تؤثر سلباً على حياتهم، لذا من المهم أن نتعرف علي بعض المخاطر وجوانب الضعف المتصلة باستخدام الانترنت. فمن بين ذلك :

- الاتصال بأشخاص لا يعرفهم ..
  - كثيراً ما يفضل الأطفال أصدقاء الانترنت على أصدقاء الواقع .
- الاطلاع على محتوى غير مناسب ..
  - خاصة المواد الإباحية فهي لا تتناسب وسنهم .
  - أو محتوى ضار آخر مثل المخدرات أو المواد التي تدعو للكراهية أو تساعد في صنع القنابل وغيرها .
- مشاهدة الإعلانات غير الملائمة ..
  - كثير من الإعلانات موجهة للراشدين ولا تناسب الأطفال؛
- الإغراء والاستدراج عبر غرف الدردشة والبريد الالكتروني ..
  - هنالك جهات محترفة تعرف كيف تستدرج الأطفال بمغريات يصعب مقاومتها وبذلك يتحصلون على ما يريدون؛
- المضايقة والإزعاج والتخويف والتهديد وتشويه السمعة وغيرها
  - الانترنت متاح للأشرار كما هو متاح للأخيار لذلك لا تتوقع أن يتعامل طفلك مع أمثاله فقط.

- كشف المعلومات الشخصية
  - يستطيع أي محتال وبسهولة استخراج معلومات شخصية عن الطفل والأسرة.
- الوصول أو إنزال مواد تخص الغير
  - قانون مكافحة جرائم المعلوماتية السوداني يعاقب بشدة على تخريب مواد تخص الغير أو إنزال مواد تخص الغير دون أخذ إذن منهم .
- التعرض لبرامج التجسس والفيروسات .
  - تأتى نتيجة لعدم حماية حاسوبك بأحد مضادات الفيروسات وتحميل البرامج من المواقع غير الموثوقة أو فتح مرفقات من مصادر غير معروفة.
- إدمان الألعاب .
- ممارسة بعض الأشياء الممنوعة في الواقع (مثل القمار والغش).
- إدمان الانترنت .
  - إدمان الانترنت يعرض الأطفال للعزلة الاجتماعية وأمراض مثل التوحد والسمنة.

كيف يمكن للأسر أن تواجه مخاطر استخدام الانترنت ..

- يجب أن تتدخل.
  - ساعد طفلك في أعماله وشاركه في الرأي.
  - لا تستحي بأن تتعلم من طفلك.
  - ناقشه في نشاطاته حتى في الأوقات التي لا يعمل فيها.
- اجعل الحاسوب في مكان مفتوح وواضح .

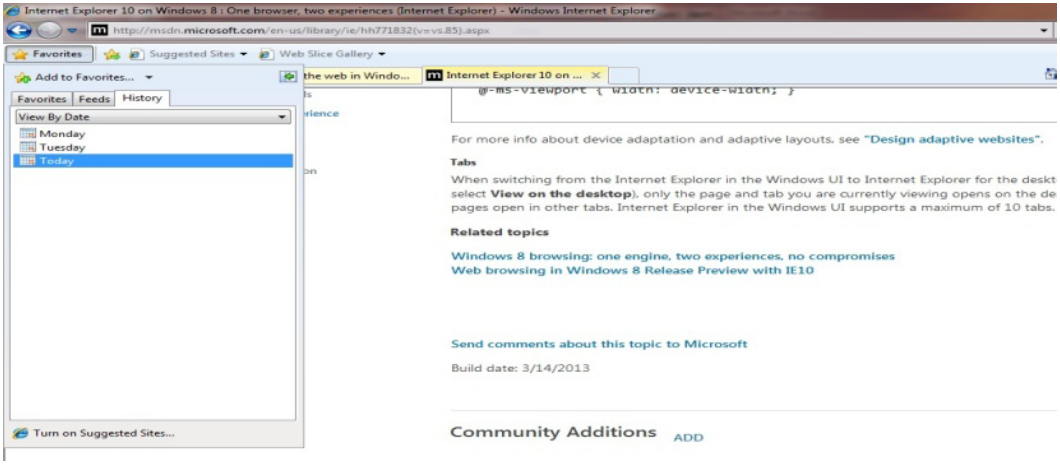
- سيحد طفلك من القيام بممارسات خاطئة.
- ويسمح لك بالتدخل في الوقت المناسب.

• ضع قواعد .. وحذر الأطفال من المخاطر.

- حدثه عن المخاطر المختلفة وكيفية التعامل معها.
- لا تخوف طفلك بل وعيه.
- علم طفلك ضرورة الاحتفاظ بكلمة مروره وعدم تقاسمها مع الآخرين.

• قسم الحاسوب إلى حسابات (accounts).

- واجعل طفلك يستخدم حساب معين بصلاحيات محدودة.
- لاحقا راجع المواقع التي يدخل عليها طفلك (انظر الصورة أدناه)



- راجع إعدادات جهازك خاصة الإعدادات الأمنية.
  - مثل برامج مكافحة الفيروسات والجدار الناري.
  - لا تجعل المتصفح يتذكر كلمة المرور.
  - راجع إعدادات متصفح الانترنت .
- قم بتشغيل برامج وأدوات التحكم الأسرية (راجع دليل استخدام أمان العائلة).
- لا تجعل طفلك يتصفح المواقع الإباحية.
  - لمواقع الإباحية ضارة جداً ولا تتناسب مع أعمار الأطفال فهي تساعد على التفكك الأسري والشذوذ (يمكنك التبليغ عن موقع اباحي في filtering@ntc.gov.sd).
  - المواقع الإباحية غالباً ما تحمل معها برامج ضارة للحاسوب.
- بيّن أهمية الانترنت لأسرتك.
- طوّر معلومات أسرتك عن الانترنت.
- حدد لأطفالك قائمة بالمواقع الجيدة والمتناسبة مع أعمارهم.
- علم طفلك ألا ينساق للإعلانات والمسابقات والجوائز الوهمية.
- حذر طفلك من مخاطر الإدلاء بمعلومات شخصية على الانترنت.
- عود طفلك إلا يقوم بفتح رسائل و مرفقات في البريد الالكتروني من مصادر غير معروفة.
- شارك طفلك في نشاطه على الانترنت.
- كن مدركاً أن ابنك قد يتصرف بشكل مختلف تماماً على الإنترنت عما هو وهو بعيد عن الإنترنت.
- تعلم الثقافة المتداولة على الانترنت.

هـــــــام:

وقِّع عقد أخلاقي بينك وبين طفلك تضع فيه كل ماتعلمته هنا بالاضافة لخبراتك الحياتية لابعد طفلك من مخاطر الانترنت ، اجعل طفلك يشارك في اعداد العقد وحتماً سيلتزم به.

في الملحق رقم ٢ تجد نموذج لعقد يمكن أن يشكل مسودة جيدة تبدأ منها.

ملحق رقم (١)
قاموس لغة الدردشة

الاختصار	المعنى المقصود	الاختصار	المعنى المقصود
Asl	Age, sex, location	3	حرف (ع)
Ping	Am here Are you ?	7	حرف (ح)
JK	Just kidding	9	حرف (ص)
(لوول) lool	(للضحك) Laughing out loud	‘9	حرف (ض)
(برب) brb	Be right back	2	الهمزة (ء)
CU	See You	‘3	حرف (غ)
ISA	إنشاء الله	$	حرف (ش)
MSA	ماشاء الله	5	حرف (خ)
IDK	I don’t Know	6	حرف (ط)
AFK	Away From Keyboard	‘d	حرف (ذ)
ASAP	As Soon As Possible	8	حرف (ق)
MOF	Male or Female	4	For
BAK	Back At Keyboard	2	To
BB	Be Back	@	At
F2F	Face To Face	GA	Go Ahead
H&K	Hug and Kiss	N/A	Not Acceptable
HAND	Have a Nice Day	):	Angry or sad
(>.<)	Sleepy	(-__-)	sick
(ʘ_ʘ)	Heart Break	(:	smile
IC	I see	OMG	Oh my God
143	I Love You	)_:	Crying
#	Hashtag	><	Fish
{}	Hug	3>	Love
3/>	Heart Break		

كذلك تستخدم الوجوه التعبيرية في غرف الدردشة ومواقع التواصل الاجتماعي بكثرة. في الصورة أدناه أمثلة لبعض الوجوه التعبيرية المستخدمة .

ملحق رقم (٢)
نموذج لعقد أخلاقي بين التلميذ/ التلميذة وولي أمره/أمرها

أعلمُ أن الإنترنت يمكن أن يكون مكاناً رائعاً يستحق أن يزار. وأعلم أيضاً أن من المهم لي أن أتبع القواعد التي من شأنها أن تحافظ على سلامتي أثناء زياراتي وتصفحي للانترنت. وأوافق على القواعد التالية :

1. أختار كلما أمكن مواقع آمنة ومعقولة لنفسي لا تعمل على إذاعة أي معلومات شخصية عني وعن أسرتي .

2. سأحتفظ بجميع كلمات السر الخاصة بي ولن أبوح بها لأي شخص مهما كان .

3. سأناقش مع والديَّ جميع البرامج والتطبيقات المختلفة التي أستخدمها في حاسوبي وفي الإنترنت، وسأتكلم معهما بشأن المواقع التي أزورها. وسأراجع مع والديّ أولاً، قبل القيام بتنزيل أو تحميل برنامج جديد أو الانضمام إلى موقع جديد، لكي أتأكد من موافقتهما عليه .

4. سأعامل الآخرين بالطريقة التي أحب أن يعاملونني بها.

5. سأتبع سلوكاً حميداً عندما أكون على الانترنت، بما في ذلك استخدام لغة حسنة وإبداء الاحترام. ولن أفتعل مشاجرة أو أستخدم ألفاظاً غير حميدة .

6. أجعل من سلامتي الشخصية أولوية لي، حيث أعلم أن هناك بعض الموجودين على الانترنت ينتحلون شخصيات أخرى خلاف شخصيتهم.

7. سأكون أميناً مع والديّ بشأن من أقابلهم في الانترنت، وسأحدثهم دائماً وبدون أن يسألونني عن هؤلاء الناس .

8. لن أرد على أي بريد إلكتروني أو رسائل فورية من أي شخص لا أعرفه في الواقع ويعرفه والديَّ .

9. إذا ما رأيت، أو قرأت، شيئاً سيئاً أو محرجاً، فسأغادر الموقع وأخبر والديّ بذلك بحيث يمكن لهما أن يتأكدا من أن ذلك لن يحدث ثانية .

10. سأخبر والديّ إذا ما تلقيت صوراً أو روابط إلى مواقع سيئة (إباحية أو عارية)، أو بريد إلكتروني أو رسائل فورية تحتوي على لغة سيئة أو إذا ما كنت في غرفة محادثة يستخدم فيها الناس ألفاظ سباب أو لغة هابطة وكريهة .

11. لن أفعل أي شيء في الانترنت يطلب شخص ما مني أن أفعله إذا ما جعلني ذلك أشعر بعدم الارتياح، وبخاصة إذا كنت أعرف أنه شيء لن يسرَّ والديّ أو يحظى بموافقتهما .

12. لن أتصل بأي أحد قابلته في الانترنت أو أكتب له رسالة بالبريد العادي أو أقابله شخصياً بدون موافقة والديّ أو ذهاب بالغ راشد أثق به إلى هذه المقابلة معي .

13. أتفهم بأن والديّ سيقومان بالإشراف علي الوقت الذي أمضيه في الانترنت وقد يستخدمان برمجيات لرصد ما أتفحصه في الانترنت أو الحد منه.

أنا الموقع أدناه بكامل ارادتي ومعرفتي أوافق على كل ماذكر أعلاه

توقيع الطفل	توقيع ولي الأمر
التاريخ	التاريخ

ملحق رقم (٣)
قائمة المصطلحات

Account (حساب): يسمح لك الحساب بالخضوع للتوثيق والحصول على الإذن لاستخدام خدمات الإنترنت من خلال اسم المستخدم وكلمة المرور. كما يمكن إنشاء حسابات مستخدمين جدد ترتبط بنظام التشغيل لكل فرد يستخدم الكمبيوتر.

Acronym (الاختصار): هي تسمية مختصر تتألف من الحروف الأولي من كل كلمة في عبارة أو تعبير، كثير ما تستخدم من قبل من يمارسون الدردشة لإيصال المعني بشكل سريع.

Administrator (مدير النظام): هو المستخدم الذي يملك أعلى صلاحيات تتيح له تنفيذ وتعديل وإضافة.

Alert (إنذار): صندوق صغير يظهر على الشاشة لإعطاء معلومات أو التحذير من عملية قد تكون تخريبية.

Anti–Virus (برنامج الحماية من الفيروسات): برنامج للكمبيوتر يحاول رصد فيروسات الكمبيوتر وغيرها من البرمجيات الخبيثة وعزلها ومنعها وإزالتها. ويقوم هذا البرنامج مبدئياً بمسح الملفات بحثاً عن الفيروسات غير المعروفة ثم يقوم بتعريف السلوك المشتبه فيه من برامج الكمبيوتر إذا كان يشير إلى وجود إصابة.

Anti–Spyware (برامج الحماية ضد التجسس): برنامج يقاوم برمجيات التجسس، ويقوم بمسح جميع البيانات الواردة بحثاً عن برمجيات التجسس ثم يقوم بمنع التهديدات التي عثر عليها وتقديم قائمة يمكنك الحذف منها.

Attachment (المرفقات): ملف أو أكثر يتم إرساله مع رسائل البريد الالكتروني.

Avatar (الصورة الافتراضية): ملف تعريف المستخدم الذي يمثل اسم المستخدم إلى جانب صورة أو أيقونة أو شخصية ثلاثية الإبعاد في ألعاب الكمبيوتر وعالم الإنترنت.

BIOS : أخذت كلمة البيوس من الحروف الأولى لـ (basic input output system) أي نظام الإدخال والإخراج الأساسي. والهدف الرئيسي من البيوس هو البدء بعملية إقلاع الحاسوب والتحضير اللازم لتنزيل نظام التشغيل في ذاكرة الحاسوب.

Blog (المدونة): لفظ مختصر لعبارة «مدونة الشبكة»، وهي عبارة عن موقع يقوم فيه فرد أو مجموعة بإضافة محتوى، وغالباً ما يكون بصورة متكررة.

Browser (المتصفح): برنامج يستخدم لاستعراض مواقع الانترنت، ومن أشهر المتصفحات: Internet Explorer – google Chrome – Firefox.

Bullying (المضايقة): التحرش من خلال الأذى اللفظي أو التعليقات الجنسية أوالاعتداء الجسدي.

CD–Rom (ذاكرة الأسطوانة المدمجة): اسطوانة تخزينية تستخدم لتخزين معلومات في شكل ملفات حاسوبية (يمكن أن تكون ملفات مكتبية أو صور أو فيديوهات أو برامج ، وغيرها).

Chat (الدردشة): الاتصال المتزامن من على الانترنت عن طريق الرسائل المكتوبة باستخدام تطبيقات الدردشة والرسائل الفورية (مثل msn messenger).

Chat room (غرفة الدردشة): مكان افتراضي عام للاتصال اللحظي. يستطيع أشخاص من مختلف أنحاء العالم الالتقاء في غرفة الدردشة والتحاور من خلال الرسائل التي يكتبونها بواسطة لوحة المفاتيح.

Child pornography (المواد الإباحية المتعلقة بالأطفال): المواد الإباحية المتعلقة بالأطفال لها تعريفات قانونية مختلفة في الدول، غير أن الحد الأدنى منها هو ما يعرفها على أنها محتوى الكتروني لطفل يبدو ضلعاً في نشاط جنسي واضح.

Computer File (ملف الكمبيوتر): مجموعة من المعلومات ذات الصلة (وثائق، برامج، الخ) مخزنة على الكمبيوتر تحت مسمي خاص بها. ويمكن اعتبار ملفات الكمبيوتر النظير الحديث للوثائق الورقية التي كانت تحفظ في ملفات المكاتب والمكتبات.

Computer Program (برامج الكمبيوتر): يشار إليها أيضاً بـ «برنامج» أو «برمجيات»، ويتألف الواحد منها من سلسلة من الأوامر المعدة التي وضعها مبرمجو الكمبيوتر بحيث تمكن مستخدمي الكمبيوتر من إنجاز المهام.

Contact List (قائمة الأسماء): مجموعة من أسماء الأشخاص الذين يمكن الاتصال بهم في البرامج المختلفة مثل الرسائل الفورية والبريد الالكتروني والألعاب على الانترنت والمحمول.

Cookies (ملفات تعريف الارتباط): ملف يضيفه موقع الإنترنت إلى متصفحك وفي كل مرة تدخل على هذا الموقع تعود هذه الملفات إلى الخادم المخزن عليه الموقع وتحمل هذه الملفات أيضاً معلومات عن تفضيلاتك على الموقع.

Copyright (حقوق النشر والتأليف): مجموعة من الحقوق الحصرية تنظم استخدام فكرة أو عمل أو معلومات ويشار إليها بالرمز «©»

Cracker (مخترق): برنامج يخترق سرية برامج أخرى ويتخلل نظام التشغيل أو الشخص الذي يقوم ببرمجة هذا البرنامج.

Cyber bulling (المضايقة على الإنترنت): المضايقة عبر الوسائط الإلكترونية، غالباً من خلال شبكات التواصل الاجتماعي والبريد الإلكتروني وقد ينطوي على تكرار الأذى والتعليقات الجنسية والكلام المهين.

Digital Game (الألعاب الرقمية): الألعاب التي يتم بتصميمها وتطويرها بغرض لعبها على الحاسوب فردياً أو من خلال شبكة تضم أكثر من لاعب (كما في الانترنت).

Directory (الدليل): وحدة تنظيمية يستخدمها الكمبيوتر لتنظيم المجلدات والملفات في هيكل هرمي.

DHCP اختصار لـ Dynamic Host Configuration Protocol يستخدم هذا البروتوكول لإسناد عناوين الانترنت (IP Address) بشكل آلي لحواسيب أو أجهزة متصلة بشبكة تعمل على TCP/IP، وبذلك نتجنب حالات التضارب في عناوين الانترنت والتي تحدث نتيجة استخدام نفس عنوان الانترنت لأكثر من جهاز.

Download (التحميل): نسخ ملف من خدمة أو موقع على الانترنت إلى الكمبيوتر.

Email (البريد الإلكتروني): وسيط للاتصال الكتابي الإلكتروني يسمح بإرسال رسائل الكترونية عبر الانترنت لشخص آخر بواسطة عنوان بريده الالكتروني.

Email address (عنوان البريد الإلكتروني): عنوان افتراضي تصل إليه رسائل البريد الإلكتروني، ويتألف عنوان البريد الإلكتروني من جزأين تفصلهما علامة *.

Favorites (المواقع المفضلة): أحد مجلدات المتصفح التي يمكن تخصيصها ويمكنها أن تخزن به الروابط المرجعية المميزة.

File sharing (مشاركة الملفات): عمليات تبادل الملفات بين أجهزة الكمبيوتر على الإنترنت، وغالباً ما تتم المشاركة في الملفات بواسطة شبكة النظير للنظير (P2P).

Firewall (جدار ناري): جهاز يتم تنصيبه في الشبكة أو برنامج يتم تثبيته على الكمبيوتر يقوم بمنع المستخدمين غير المصرح لهم من الدخول إلى الكمبيوتر أو شبكة الحواسيب.

Flaming (الرسالة النارية): التفاعل العدائي والمهين بين مستخدمي الانترنت الذي غالباً ما يدور على ساحات النقاش والدردشة عبر الإنترنت أو حتى من خلال البريد الالكتروني.

Folder (المجلد): كيان داخل نظام الملفات يحتوي على مجموعة من الملفات، ويمكن أن تضم المجلدات عدة مستندات وهي تستخدم لتنظيم المعلومات.

Form (Online Form) (نموذج استمارة (على الانترنت)): وثيقة منسقة تحتوي على خانات فارغة يمكن ملؤها بالبيانات المطلوبة.

Forum (منتدى) : مجموعة نقاش على الإنترنت تمكن المشاركين من ذوي الاهتمامات المشتركة تبادل الرسائل.

Freeware and Shareware (البرمجيات المجانية و البرمجيات المشتركة): تتمتع البرمجيات بصفة عامة بحماية حقوق النشر والتأليف ولذا لا يسمح بتحميلها قانونياً. ويقصد بالبرمجيات المجانية أن صاحب حقوق النشر والتأليف يوافق على استخدام البرمجيات من قبل أي شخص دون مقابل، أما

البرمجيات المشتركة فتعني أن صاحب حقوق النشر والتأليف يوافق على استخدام البرمجيات من قبل أي شخص لفترة تجريبية. وبعد انتهاء تلك الفترة، يتعين على المستخدم دفع رسوم للاستمرار في استخدام الخدمة .

Grooming (الاستمالة): استخدام شبكات التواصل الاجتماعي من قبل غير الأسوياء لاستمالة الأطفال بالتظاهر بأنهم نظراء لهم. ويبدأ هؤلاء في الحوار مع الضحايا المحتملين لاستخلاص معلومات بشأن أماكنهم واهتماماتهم وهوايتهم وخبراتهم .

Hardware (مكونات الكمبيوتر أو ما يعرف بالعتاد): الجزء الملموس من الكمبيوتر. وهذه الأجزاء قد تكون داخلية: كاللوحات الأم و محركات الإقراض الصلبة وذاكرة الوصول العشوائي (غالبا ما يشار إليها بالمكونات) أو خارجية: كالشاشات ولوحات المفاتيح والطابعات (تسمى أيضا بالوحدات الطرفية للكمبيوتر) .

Homepage (الصفحة الرئيسية): صفحة على الإنترنت تظهر تلقائيا عند كتابة عنوان انترنت محدد على المتصفح وتعرف أيضاً بالصفحة الأمامية أو الصفحة الرئيسية .

Identity Theft (سرقة الهوية): سرقة بيانات شخصية واستخدامها بطرق غير قانونية.

Illegal Content (محتوى غير قانوني): محتوى على الإنترنت يصنف على أنه غير قانوني وفقا للتشريعات الوطنية. وأكثر أنواعه شيوعا هو المواقع الاباحية ومواقع الكراهية ومواقع القمار وغيرها.

IM" Instant Messaging" (الرسائل الفورية): صورة من صور الاتصال الإلكتروني الفوري واللحظي بين مستخدمَين أو أكثر. وتتيح الرسائل الفورية التواصل مع قائمة مختارة من الأشخاص.

Internet (الإنترنت): شبكة عالمية عامة مفتوحة للجميع تتألف من مجموعة من الشبكات الأصغر حجماً يتم من خلالها نقل وتبادل المعلومات وتقديم الخدمات المختلفة مثل البريد الالكتروني ، الدردشة ، التسوق الالكتروني ، الحكومة الالكترونية ، الاتصال الهاتفي ، الالعاب وغيرها.

Internet Connection (وسيلة الاتصال بالانترنت): يشير إلى الارتباط الذي يمكن من خلاله للمستخدمين الاتصال بالانترنت. من وسائل الاتصال بالانترنت: الاتصال الهاتفي – Wi–Fi – الأقمار الصناعية – GPRS.

Junk Mail (البريد المزعج): رسائل البريد التي لا يرغب فيها المستخدم.

Link (الرابط): إشارة مرجعية إلى وثيقة متاحة على الانترنت (كصفحة من موقع أو وثيقة نصية أو صورة)..

Malware (البرمجيات الخبيثة): برمجيات صممت لاختراق أنظمة الكمبيوتر أو إلحاق الضرر بها، تشمل الفيروسات والبرامج الدودية وفيروسات أحصنة طروادة وبرمجيات التجسس والبرمجيات الإعلانية المضللة وغيرها .

Manipulate (التلاعب): التغيير في صورة أو ملف أو رسم إيضاحي بطريقة واضحة أو غير واضحة، وتوجد حاليا العديد من الأدوات التي يمكن استخدامها على محتوى أو شكل البيانات مما يؤدي إلى نتيجة تختلف عن الواقع .

Memory/USB stick (بطاقة ذاكرة/جهاز USB): وسيلة تخزين بيانات تعتمد على منفذ USB وهي بطاقات صغيرة في المعتاد وخفيفة الوزن ويمكن نقلها وإعادة التخزين عليها.

Mobile (المحمول): جهاز إلكتروني للاتصال الهاتفي ونقل البيانات ويعرف أيضاً بالهاتف السيّار والخلوي والنقّال .

Mp٣ (تنسيق Mp٣): صيغة ترميز خاصة بالملفات المسموعة. يعتبر خجم ملفات MP٣ صغيراً مقارنة بالملفات الصوتية الأصلية وبجودة مقبولة. وبسبب حجمه الصغير ونقاء جودته، صارت ملفات Mp٣ طريقة شائعة لتخزين ملفات الموسيقي على أجهزة الحاسوب والأجهزة المحمولة .

Net (الشبكة): اختصار لشبكة الإنترنت .

Nickname (الاسم المستعار على الانترنت): مرادف لاسم العرض وكود التعريف، فهو يمثل مستخدم احدي خدمات الإنترنت ويحدده المستخدم نفسه، كما يمثل الاسم الذي يظهر للمستخدمين الآخرين .

Operating System OS (نظام التشغيل): برنامج يقوم بتشغيل الوظائف الأساسية للكمبيوتر

(المقصود الأجهزة الالكترونية مثل الهاتف والموجه (router))، ويمكن البرامج الأخرى من آداء مهامها. ومن أشهر الأمثلة Mac – Linux – Windows.

Password (كلمة المرور): كلمة المرور أو كلمة السر هي تشكيلة من الحروف الأبجدية والأرقام والرموز تمكن من يعرفها من الوصول أو استعمال مورد أو خدمة محمية.

Personal Data (البيانات الشخصية): أية معلومات خاصة بشخص ما.

Phishing (الاحتيال أو التصيّد): هو محاولة الحصول على المعلومات الخاصة بمستخدمي الانترنت سواء عن طريق الرسائل الإلكترونية أو مواقع الانترنت التي تبدو وكأنها مبعوثة من شركات موثوقة أو مؤسسات مالية وحكومية أو أفراد معروفين.

Pop–up Window (النافذة المنبثقة): نافذة تظهر عند زيارة موقع ما أو الضغط على زر له وظيفة خاصة.

Port (المنفذ): كلمة (port) تستخدم اما لتعريف الفتحات الخارجية للحاسوب والتي تساعد في توصيل أجهزة خارجية بنظام التشغيل. أو هو رقم ملحق بعنوان الأي بي يستخدم في بروتوكولات الشبكة بهدف تمييز الخدمات أو البرامج المختلفة العاملة على ذات جهاز الحاسوب سامحا باستخدام اتصال واحد إلى الشبكة لتقديم أكثر من خدمة.

Privacy (الخصوصية): قدرة الفرد أو المجموعة على التحكم في تدفق المعلومات الخاصة بهم، بما يتيح لهم الكشف عن هويتهم أو إخفاءها باختيارهم.

Privacy settings (إعدادات الخصوصية): مجموعة من تفاصيل الخصوصية المتعلقة بحساب المستخدم.

Processor (المعالج): أو وحدة المعالجة المركزية هو ذلك الجزء من الحاسوب الذي يعالج البيانات ويصدر إشارات التحكم ويخزن النتائج. وهذه الوحدة – إلى جانب ذاكرة الكمبيوتر – يمثلان مركز الكمبيوتر.

Profile (ملف التعريف): المعلومات الخاصة بالمستخدم في مواقع التواصل الاجتماعي وأنظمة الرسائل الفورية وتطبيقات الدردشة على الانترنت والألعاب وغيرها.

Recycle Bin (سلة المهملات): تخزن به مؤقتاً الملفات المحذوفة قبل أن يقوم المستخدم بحذفها نهائياً. ويتعين عليك المداومة على التخلص من البيانات القديمة التي لا تحتاجها من سلة المهملات لتحرير مساحة على القرص الصلب.

Report (الإبلاغ): خاصية تسمح للمستخدمين عامة بالإبلاغ عن مشكلة (سواء مشكلة فنية أو سلوك غير مقبول من أحد المستخدمين أو محتوى غير قانوني، الخ).

Scan (مسح): الفحص ضد الفيروسات أو البرامج الضارة.

Search Engine (محرك البحث): أداة تستخدم للبحث عن معلومات على مواقع الإنترنت من أشهر محركات البحث Google و Yahoo.

Sign–up (الانضمام): يعني الاشتراك في خدمة على الانترنت: كالرسائل الإخبارية ومنتديات النقاش والبريد الإلكتروني ومنابر الدردشة. ويتاح في المعتاد للمستخدمين خيار تسجيل الخروج وقتما يشاؤون.

Social Network (الشبكات الاجتماعية): مجموعة من الأعضاء على الإنترنت تجمعهم اهتمامات وأنشطة مشتركة، يتفاعلون ويتعارفون على الإنترنت باستخدام برمجيات وخدمات ملائمة.

Social Networking Sites (مواقع التواصل الاجتماعي): هي مواقع أو تطبيقات تستخدم كمنابر افتراضية تستضيف مجموعات الأعضاء الذين تجمعهم اهتمامات أو أنشطة مشتركة (يمكن أن تجمعهم مدينة أو جامعة أو قبيلة الخ)..

Software (البرمجيات): انظر تعريف برامج الكمبيوتر.

Spam (الرسائل الاقتحامية): البريد الإلكتروني غير المرغوب فيه، غالباً ما يكون ذا طبيعة تجارية ويتم إرساله بأعداد ضخمة. إرسال الرسائل الاقتحامية يعود بأضرار متفاوتة على مستخدم البريد

الالكتروني ومزودو خدمة الانترنت .

Spam Filter (عامل الحماية ضد الرسائل الاقتحامية): تطبيق منع تخزين الرسائل الاقتحامية في صندوق الوارد ببريدك الإلكتروني .

Spyware (برمجيات التجسس): برمجيات خبيثة ترفق سرا بالملفات التي يتم تحميلها من الإنترنت تقوم بتثبيت ذاتها على الحاسوب لمراقبة الأنشطة ثم تقوم بإرسال المعلومات إلى طرف ثالث يكون في الغالب شركات تهتم بتحديد ملفات التعريف الشخصية بغرض إرسال إعلانات وغيرها من المعلومات أو إلى المخترقين ممن يرغبون في الوصول إلى بياناتك الخاصة .

Subscribe (الاشتراك): عملية التسجيل الطوعي في خدمة أو تحديث إخباري يتم بموجبها إرسال المعلومات مباشرة إلى صندوقك للبريد الإلكتروني الوارد .

Toolbar (شريط الأدوات): مجموعة من الأيقونات أو الأزرار التي تشكل جزءاً من واجهة برنامج للكمبيوتر. وتتمثل فائدة شريط الأدوات في كونه واجهة سهلة الاستخدام .

Trial Software (برمجيات تجريبية): البرمجيات التي يمكنك تجربتها قبل شرائها، وتحتوي النسخ التجريبية من البرمجيات في أغلب الأحيان على جميع الخواص الوظيفية للنسخة المعتادةالأصلية إلا انه لا يمكن استخدامها الا لمدة محددة .

Trojan Horses (أحصنة طروادة): كود خبيث أو برنامج يمكنه الدخول إلى الحاسوب متخفياً وراء مظهر برئ كالألعاب أو ربما برنامج تعقب الفيروسات. ولا تقوم أحصنة طروادة بالتكاثر ذاتياً إلا أنها في المعتاد تكون مصممة بحيث تدخل إلى البيانات الحساسة أو تدميرها أو مسح محتوى القرص الصلب أو سرقة معلومات سرية .

URL (Uniform Resource Locator) (عنوان محدد المواقع): عنوان موقع او ملف بعينه على الإنترنت. ولا يتضمن حروف خاصة أو مسافات ويشير الجزء الأول من العنوان إلى البروتوكول المستخدم، أما الجزء الثاني فيحدد عنوان الIP (بروتوكول الإنترنت) أو اسم النطاق الذي يوجد به المصدر .

Virus (فيروس) : نوع من البرمجيات الخبيثة صمم كي ينتشر بتدخل من قبل المستخدم . وينتشر

الفيروس في المعتاد من خلال مرفقات البريد الالكتروني وأدوات الذاكرة الخارجية المصابة (كبطاقة USB أو الاسطوانة المدمجة) .

VoIP (Voice over Internet Protocol) (نقل الصوت عبر بروتوكول الإنترنت): تكنولوجيا تسمح للمستخدمين بالتحدث عبر الإنترنت بعد تحميل البرمجيات اللازمة. ويمكن أن تكون المكالمات مجانية بالنسبة للمتحدثين الذين يستخدمون البرنامج نفسه مثل (Skype, Viber) كما توفر مثل هذه البرمجيات إمكانية الدردشة ومشاركة الملفات .

Wallpaper (خلفيات الشاشة): نقش أو رسم أو صورة تشكل خلفية شاشة الحاسوب .

Web (الشبكة العنكبوتية) : مجموعة من الوثائق على الانترنت بتنسيق HTML (لغة تحديد النص المترابط) تشمل روابط تقود إلى وثائق أخرى كالصور والملفات الصوتية أو ملفات الفيديو .

Website (موقع ويب): موقع من المواقع على شبكة الإنترنت، ويحتوي كل موقع على صفحة رئيسية هي الوثيقة الأولي التي تراها حين تدخل الموقع. وعادة ما يضم كل موقع روابط إلى ملفات ومواقع إضافية .

Webcam (كاميرا الويب) : كاميرا الويب يمكنها أن تبث ما تلتقطه عبر الإنترنت في الرسائل الفورية وتطبيقات المؤتمرات المرئية عبر الحاسوب الشخصي ومنابر الدردشة، الخ .

Worm (الدودة): نوع من الفيروسات يتكاثر ذاتياً ويمكنه الانتشار بدون تدخل من المستخدم عبر مختلف أجهزة الحاسوب وإلحاق الضرر بالشبكة أو شغل جزء كبير من عرض النطاق الترددي أو إغلاق الحاسوب .