2019

الإنترنت والإبتزاز الإلكتروني

إعداد : بلال جناجرة

للتواصل : goldenacademy13@gmail.com

فهرس المواضيع

المقدمة

دخل الإنترنت بسرعة البرق في مختلف مجالات الحياة وأصبح لايمكن الإستغناء عنه ولايوجد بديلاً له ، وهو أساس من أساسيات الحياة ويستخدم في التجارة والصناعة والتعليم والإتصالات ، وأقبل عليه سكان العالم بنسبة كبيرة بشكل متفاوت ، فلا يختلف إثنان أن شبكة الإنترنت زادت إتساعاً وإنتشاراً حول العالم .

فقد بلغ عدد مستخدمي الإنترنت في العالم تجاوز 4 مليارات مستخدم وإن 3مليارات يستخدمون مواقع التواصل الإجتماعي بشكل يومي ، حيث يستخدم 9 من أصل 10 مستخدمين هواتفهم الذكية للدخول على مواقع التواصل الإجتماعي.

الإنترنت

هو تقنية حديثة أحدثت ثورة في عالم الإتصالات ، حيث تتيح للمستخدمين من كافة أنحاء العالم بالتواصل مع بعضهم البعض أو الوصول إلى المعلومات من خلال شبكات الكمبيوتر التي تربط الاجهزة مع بعضها البعض ، وقد ظهر الإنترنت في الولايات المتحدة الأمريكية في عام 1970م لكن لم يكن إستخدامه متاحاً للناس الإ في بداية التسعينيات من القرن الماضي .

فوائد الإنترنت

هناك الكثير من الفوائد نذكر منها :

- إرسال وإستقبال الرسائل الإلكترونية من خلال خدمات البريد الإلكتروني
- المكتبات الإفتراضية
- التبرع من خلال الإنترنت
- التسوق عبر الإنترنت

- التواصل مع الاخرين من خلال التطبيقات والمواقع المختلفة مثل مواقع التواصل الإجتماعي
- التعليم أصبح الإنترنت يقدم خدمات التعليم للمدارس والجامعات وللطلاب والباحثين وطلاب الدراسات العليا .
- يستخدم في كثير من المجالات المختلفة منها الطب والبحث العلمي ونشر الملعومات المفيدة والقيمة
- أصبح يخدم الأغراض التجارية وأصبحت معظم الشركات والمؤسسات تقوم في تسويق منجاتها عبر الإنترنت

سلبيات الإنترنت

هناك سلبيات للإنترنت نذكر منها :

- إستخدام الأطفال لمواقع الإنترنت ولمواقع خاصة يعرضهم لخطر التحرش من قبل بعض المرضى.
- الجلوس طويلاً أمام شاشة الحاسوب بسبب بعض الأضرار الصحية مثل زيادة الوزن وضعف البصر وغيرها.
- الإستخدام الكثير لشبكة الإنترنت يقلل من الإجتماع بأفراد العائلة وقضاء فترة إجتماعية مع الأهل والأصدقاء والإنعزال عن المجتمع .
- الدخول إلى المواقع الغير أخلاقية مع سرعة وسهولة الوصول إلى الإنترنت يكون سهلاً للكثيرون القيام بإيذاء غيرهم ونشر صور غير أخلاقية أو حتى صور لممارسات عنيفه ، بالإضافة إلى أن الكثيرون يتعرضون للإبتزاز بسبب تهديدهم بنشر صور فاضحة لهم أو إستغلالهم.

الرقابة على الإنترنت

تتيح الإنترنت لمستخدميها وصولاً سريعاً وغير محدود للمعلومات إلا أن فيها أيضاً بعض الحواجز على شكل رقابة ، أما دوافع هذه الرقابة فتتراوح بين :-

- الرغبة في حماية الأطفال من بعض المحتويات التي لاتناسب سنهم .
- محاولات السيطرة على المعلومات التي تدخل إلى بلد معين ومهما كانت الدوافع فإن النتيجة واحدة وهي الحيلولة دون الوصول إلى بعض المواقع غير المرغوب فيها.

لاتقتصر الرقابة على الآباء والحكومات بل هناك بعض البرامج الحاسوبية في السوق التي تقوم بالرقابة وتمنع الدخول إلى مواقع محددة وتعرف هذه البرامج بإسم "فلترة المواقع" أو "برامج الرقابة" أو "خدمات الأمان" .

وهناك مؤيدون ومعارضون للرقابة وقد يلجأ بعض المعارضين إلى المحاكم لمعارضة سياسات الرقابة الحكومية ويقوم اخرون بتقديم معلومات سرية إلى مستخدمي الإنترنت تمكنهم من التلاعب لدخول المواقع الممنوعة والحصول على المعلومات التي يريدونها.

الرقابة على الإنترنت في البيت

لاشك بأن الإنترنت يحتوي على مواد ومعلومات لايرغب الآباء بأن يطلع أبناؤهم عليها لأنها تؤثر في تربيتهم بشكل سلبي ، ويواجه الآباء صعوبة في مراقبة ما يشاهده الطفل على الإنترنت طوال الوقت لذلك كثيراً ما يستخدمون برامج حاسوبية وأجهزة لحل هذه المشكله ، وتتميز البرامج الحاسوبية لفلترة المواقع بأن فيها مجموعة من الخيارات للآباء للحد من عدد المواقع التي يستطيع الأبناء الدخول إليها فمثلاً يمكنهم منع الدخول إلى المواقع الإباحية والمواقع التي تدعو إلى الكراهية والعنصرية أو مواقع لعب القمار وغيرها من المواقع .

تستخدم معظم مواقع الفلترة تقنيتين أساسيتين للحيلولة دون الدخول إلى بعض المواقع وهي تقنية "القائمة السوداء" وتقنية "المنع بواسطة كلمة البحث" وتتضمن القائمة السوداء مواقع صنفها واضعو البرامج على أنها غير مرغوب فيها وهي تتغير وتتطور مع الوقت ، وتزود معظم الشركات التي تنتجها مستخدمي هذه البرامج بالقوائم الجديدة للقائمة السوداء مجاناً.

أما في تقنية المنع بواسطة كلمة البحث فيقوم البرنامج بمسح صفحة الموقع الذي يحاول المستخدم الدخول إليها ويحللها ليرى فيما إذا كانت تحتوي على إحدى كلمات البحث المحظورة ، وإذا وجد أن صفحة الموقع غير مناسبة فإنه يمنع الدخول إليها ، وقد تحصل في هذا البرنامج بعض الإشكالات لأن البرنامج لا يمكنه إدراك المضمون وإنما يتعرف إلى الكلمات فقط لذلك قد يمنع الدخول إلى مواقع لمجرد أنها تحتوي على كلمة البحث مع أنها قد تحتوي على إنتقاد للموضوع ذاته.

يوجد تقنية متطورة وهي Firewall لكن هذه تحتاج للعمل عليها إلى مختص في علم الحاسوب أو الإتصالات أو تخصص له علاقه .

الشركات الكبيرة والرقابة على الإنترنت

تقوم الشركات الكبيرة بالحد من المواقع التي يستطيع موظفوها الدخول إليها وذلك لعدة أسباب أولها وأهمها زيادة الإنتاجية ، في حين من المفترض أن يستخدم الموظفون الإنترنت للأبحاث أو للتواصل فإنهم قد يستخدمونها كوسيلة للهو والتسلية وإضاعة الوقت.
وقد تستخدم الشركات برامج فلترة المواقع الإ أن معظمها يستخدم نظام Firewall وبواسطة هذا البرنامج تستطيع الشركة إختيار المواقع أو حتى الموضوعات التي تريد منعها.
وفي كثير من أماكن العمل عندما يحاول أحد الموظفين الدخول إلى موقع ممنوع تظهر على شاشته رسالة تقول بأن الإدارة صنفت الموقع على أنه غير مناسب وتعرض أمامه خيارات احدها الطلب من المسؤول السماح بالدخول إلى موقع محدد إذا كان الموظف يعتقد بأن منعه غير مشروع ، كما تستطيع الشركات المسؤولة عن الدخول إلى الإنترنت أن تلعب دوراً بارزاً في إختيار المواقع التي يستطيع المستخدمون الدخول إليها.

الرقابة على الإنترنت على المستوى الدولي

تقوم كثير من الدول بفرض رقابة على الإنترنت للحد من الدخول إلى محتوياتها ، وهناك قوانين في جميع الدول تحدد نوعية المعلومات التي يمكن الدخول إليها في المدارس وفي المكتبات العامة ، وهناك دول تتشدد أكثر من ذلك في الدخول إلى الإنترنت حتى إن بعضها قد يمنع الدخول إلى الإنترنت منعاً باتاً ، أما الدوافع وراء هذا المنع فهي :

- سياسية : يحتوي الموقع على أراء مضادة لسياسة الدول أو قد تكون له علاقة بحقوق الإنسان وبالحركات الدينية وقضايا إجتماعية أخرى.
- إجتماعية : مثل المواقع التي تركز على الجنس والقمار والمخدرات وموضوعات أخرى ترى الدولة أنها مضرة أو عدوانية.
- تتعلق بالصراعات وبتهديد الأمن العام : مواقع لها علاقة بالحروب والمشادات والمعارضات وصراعات أخرى.
- تتعلق بأدوات الإنترنت : مواقع تقدم أدوات ووسائل إلكترونية للمراوغة والتلاعب على الرقابة ، وتقوم بعض الحكومات بمراقبة مقاهي الإنترنت بواسطة حواسيب تلتقط ما يعرض على الشاشات كل عدة دقائق ، ولدى الصين نظام فلترة متطور جداً يدعى "بجدار الصين الناري" ويستطيع هذا النظام البحث في المواقع الجديدة ومنع الدخول إليها في وقت قياسي ، كما يستطيع البحث في "المدونات" عن المحتوى غير مرغوب فيها والتي تعتبرها الحكومة مخربة ويمنع مستخدمي الإنترنت من الدخول إليها.

إدمان الإنترنت

كما ذكرنا سابقاً الإنترنت هي مصدر هائل للمعلومات يستخدمه مختلف الطوائف بحثاً عن المعلومات فالدارس أو الباحث يستخدمه كأداة للبحث في حين يستخدمه رجال الأعمال للتعرف على أحدث المنتجات في مجالهم أما الشركات فقد أصبحت تعتمد عليها كوسيلة تسويقية جيدة قليلة

التكلفة وكذلك كوسيلة إتصال لإرسال رسائل الفاكس والمكالمات الهاتفيه باهظة التكاليف .
أيضاً تستخدم الأسر والأشخاص العاديين الإنترنت كوسيلة للتسوق أو الدفع الإلكتروني للفواتير بالإضافة إلى وسيلة للإتصال بباقي أفراد أسرهم وأصدقائهم في الأماكن البعيدة.

ما هو إدمان الإنترنت

هو عبارة عن تعلق مرضي بوسائل التواصل الإجتماعي فأنت لا تستطيع الإندماج مع المجتمع العادي ، كما أنك في هذه الحالات لا تهتم بشيء غير الإنترنت وتعتبره نافذة أكثر وضوحاً من عالمك الذي تعيش فيه .

المشكلة بالنسبة للبعض تكمن في أن عالم الإنترنت يستحوذ عليهم للدرجة التي يطفي فيها على عالمهم الحقيقي ، بعض الناس قد إختاروا بالفعل أن يكونوا على إتصال بالكمبيوتر بدلاً من التواصل مع ذويهم وأصدقائهم في العالم الحقيقي هؤلاء الناس هم من وصل بهم "إدمان الإنترنت" للدرجة التي أثرت أو تؤثر الإنترنت فيها على علاقاتهم سواء الأسرية أو الزوجية أو نجاحهم في العمل ، إن إدمان الإنترنت ليس مثيلاً لحالات الإدمان الأخرى كالمخدرات والكحوليات بل هو عادة قد تم فقد السيطرة عليها للدرجة التي أصبحت تؤثر على طبيعة حياة الشخص العادية وعلاقاته بالمجتمع المحيط.

علامات إدمان الإنترنت

- الرغبة الملحة في كثرة إستخدام الإنترنت ، بشكل غير ضروري .
- ترك الأصدقاء ومجالس العائلة لفتح الإنترنت ، دون أن يكون هناك ضرورة لذلك .
- الجلوس لوقت طويل على الإنترنت لمجرد الجلوس دون الإستفادة من المعلومات المختلفة ، مع عدم تقدير الوقت عند الجلوس .

- الشعور بالإحباط عند عدم فتح الحاسب أو المحمول لمدة ساعات قليلة .
- إنخفاض الأداء المهني والأداء المدرسي في العمل والمدرسة بسبب الجلوس طويلاً على الإنترنت .
- الإعتراف بأن الإنترنت ما يمثله هو الواقع الحقيقي ورفض المجتمع الحقيقي .

أضرار إدمان الإنترنت

- الإصابة بالإرهاق والإجهاد طوال الوقت ، فالحاسبات اللوحية والهواتف المحمولة ، ليست هي التي تعطينا طاقة ، للخروج من الضغوط ، لذا فإن ملازمة الإنترنت طوال الوقت تشعر الشخص بالإجهاد .
- صداع العين وذلك نتيجة الجلوس الطويل على الإنترنت لفترة فإن عينيك تتعرض للإجهاد المستمر نتيجة لتعرضها للأشعة الخارجة من شاشة الحاسوب أو الموبايل ، فقد تصاب بصداع بين منطقة الحاجبين .
- صعوبة تكوين علاقات إجتماعية مع طول فترة الجلوس على الإنترنت ، فتجد أنك لاتستطيع تكوين علاقات إجتماعية مع الأشخاص الذين تقابلهم في حياتك ، فعندما تتعرض لموقف قد لا تجد من يساندك خارج إطار شاشة الحاسوب ، وقد يعرضك هذا لفشل الحياة الزوجية ويؤدي إلى مشاكل الإنفصال والطلاق ، بسبب عدم الإهتمام بالأسرة .
- الام العمود الفقري من كثرة الجلوس على شاشة الحاسوب ، فهذا يسبب لك الام في الظهر والرقبة ، بسبب الجلوس لساعات دون تغيير في الوضع .
- السمنة المفرطة عدم الحركة لفترة طويلة يجعلك لا تفقد وزنك ، فأنت لا تبذل مجهود لكي تفقد وزنك .
- التأخر في إنجاز المهام ترك مهامك في العمل والجلوس لمتابعة مواقع التواصل الإجتماعي ، يجعلك تتأخر عن أدائها مما يجعلك لا تأخذ قسط من الراحة ، وتنهي عملك متأخراً .

علاج إدمان الإنترنت

يوجد بعض الإقتراحات للتخص من الإدمان :

- تكلم مع طبيب نفسي في هذا الوقت ليساعدك على التخلص من إدمان الإنترنت بشكل سلوكي محترف .
- حدد وقت تتصفح الإنترنت فيه ، فكلما حددت وقتاً كلما تخلصت بسهولة من إهدار الوقت.
- حدد مهامك داخل الإنترنت ، كلما كنت محدداً أكثر كلما قلت فرص إضاعة الوقت ، مثل أن تقول لنفسك سأجلس لمدة ساعة ، سأقرأ فيها كتاباً أو قراءة رسائل البريد الإلكتروني ، في البداية قد يفيدك منبه أو ساعة إيقاف الوقت.
- إشغل يومك بممارسة الأنشطة المفيدة مثل الأعمال اليدوية كالرسم وغيرها والرياضه ايضاً .
- حاول أن تؤجل قراءة الرسائل الغير مهمة إلى وقت حدده أنت في وسط الأسبوع حتى لاتعطلك عن مهامك الأخرى داخل الإنترنت .

أمن المعلومات

إن التخريب والسرقة بما فيها سرقة المال ، أو المنقولات الثمينة ، والمعلومات المهمة من الآخرين ، وإيقاع الضرر بهم – من أقدم الأخطار التي يتعرض لها الإنسان وتختلف دوافع التخريب والسرقة من شخص لآخر ، ولكن في النهاية هناك طرف يقع عليه الضرر وتطاله الخسارة .

ففي الماضي وخصوصاً قبل ظهور الوسائط الإلكترونية لتخزين المال والمعلومات ونقلها ، كان من السهل إكتشاف السرقة وبسرعة لأن السارق لابد أن يترك في معظم الأحوال أثراً لفعلته مثل قفل مكسور أو باب مهشم وما شابه ذلك ، إلا أنه مع ظهور الإنترنت وإتساع نطاق إستعمالاته قد يصعب إكتشاف أثر السرقه ولذلك لا يشعر المتضرر بفقد المعلومة أو المال إلابعد فوات الأوان في بعض الحالات .

وسوف تتفاقم هذه الأضرار مع تسارع التقدم في مجالات الإتصالات والحاسبات ، وما ينتج عن ذلك من زيادة حجم المعلومات المنقولة على شبكات الإتصالات والمعلومات المخزنة في الحاسبات .

إن من أصعب مهام المتخصصين في أمن المعلومات هو نقل صورة كاملة وواقعية ، دون مبالغة أو تهويل أو زيادة في تبسيط لمستخدمي الوسائط الإلكترونية حول الأخطار التي تتعرض لها المعلومات المخزنة إلكترونياً ، أو المنقولة عبر الإنترنت من سرقة أو تغيير ولاتزال هذه المهام صعبة ، يصرف النظر عن المتلقي سواء كان مستخدماً مبتدئاً أو مديراً لشركة كبرى ومن أبرز الأخطار مايلي :

- تغيير البرامج أو إدخال برامج جديدة مغلوطة أو مدمرة مثل الفيروسات .
- الإطلاع غير المشروع على المعلومات السرية عن طريق التنصت على شبكات الإتصالات أو الدخول غير المصرح به إلى الشبكات أو قواعد البيانات .
- الإطلاع بصفة غير مقصودة مثل الشاشات المفتوحة أو الطابعات أو حتى تجميع ما تم حذفه في سلة المحذوفات .
- التزوير والتزييف بإدخال معلومات مغلوطة بسوء نية أو عن غير قصد .
- مسح المعلومات أو إخفاؤها أو عدم إدخال المعلومات أو تغييرها سهواً أو عمداً ، وكذلك تغيير كلمات السر ، أو الأرقام السرية ، أو مفاتيح التشفيير .

برزت في القرن المنصرم ظواهرتقنية عديدة تركت أثراً بيناً في حياة الناس لكن يبقى الحاسوب أبرز هذه الظواهر قاطبة وذلك لسرعة تطوره وإنتشاره ولعمق أثره في حياة الناس وقد ساهم الحاسوب في رفع نوعية الحياة التي يعيشها الناس بتذليله كثيراً من الصعوبات وإختصاره للوقت والجهد و أصبحت كثير من الأمور لايمكن أن تسير إلا بمساعدة الحاسوب ومن ذلك على سبيل المثال المعاملات المالية والإدارية وتنظيم رحلات الطائرات وتشغيل الكثير من

الأجهـــزة الطبيـــة والصـــناعية وزادت الخـــدمات التـــي يقـــدمها الحاسوب بظهور الإنترنت وزاد إنتشاره.

تعريف أمن المعلومات

إذاً يمكـــن تعريـــف أمـــن المعلومـــات بأنـــه علـــم مخـــتص بتـــأمين المعلومـــات المتداولـــة عبـــر شـــبكة الإنترنـــت مـــن المخـــاطر التـــي تهددها .

ويمكـــن تعريفـــه أيضـــاً بأنـــه العلـــم الـــذي يعمـــل علـــى تـــوفير الحمايـــة للمعلومـــات مـــن المخـــاطر التـــي تهـــددها أو الحـــاجز الـــذي يمنـــع الإعتـــداء عليهـــا وذلـــك مـــن خـــلال تـــوفير الأدوات والوســـائل الـــلازم توفيرهـــا لحمايـــة المعلومـــات مـــن المخـــاطر الداخليـــه أو الخارجيـــة . المعـــايير والإجـــراءات المتخـــذة لمنـــع وصـــول المعلومـــات إلـــى أيـــدي أشـــخاص غيـــر مخـــولين عبـــر الإتصـــالات ولضمان أصالة وصحة هذه الإتصالات .

إن حمايـــة المعلومـــات هـــو أمـــر قـــديم ولكـــن بـــدأ إســـتخدامه بشـــكل فعلـــي منـــذ بـــدايات تطـــور التكنولوجيـــا ويرتكـــز أمـــن المعلومـــات إلى :
أنظمـــة حمايـــة نظـــم التشـــغيل – أنظمـــة حمايـــة البـــرامج والتطبيقـــات – أنظمـــة حمايـــة قواعـــد البيانـــات – أنظمـــة حمايـــة الولوج أو الدخول إلى الأنظمة .

إعتماد وتدقيق أمن المعلومات

أصـــبحت الـــنظم المعلوماتيـــة وقواعـــد البيانـــات وشـــبكات الإتصـــال عصـــب العـــالم المعرفـــي والصـــناعي والمـــالي والصـــحي وغيرهـــا مـــن القطاعـــات حيـــث أصـــبح مـــن المهـــم الحفـــاظ علـــى أمـــن المعلومـــات بعناصـــره الرئيســـية الـــثلاث : الســـرية – الصـــوابية – الإستمرارية .
وعلـــى المســـتوى العـــالمي يبـــرز نظـــام الأيـــزو للإعتمـــاد والتقيـــيم 27001 لضـــمان أمـــن المعلومـــات كمـــا يوجـــد نظـــام HIPAA فـــي الولايـــات المتحـــدة الأمريكيـــة لضـــمان أمـــن المعلومـــات الصـــحية ونظام COBIT من ISACA لأمن المعلومات .

مهددات أمن المعلومات

- الفيروسات

الفيروس هو برنامج صغير مكتوب بأحد لغات الحاسب ويقوم بإحداث أضرار في الحاسب والمعلومات الموجودة على الحاسب بمعنى أنه يتركز على ثلاث خواص وهي التخفي ، التضاعف ، وإلحاق الأذى .

مصادر الفيروس

يكمن مصادر الفيروس من خلال الرسائل الإلكترونية المجهولة صفحات الإنترنت المشبوهة ، نسخ البرامج المقلدة ، إستخدام برامج غير موثقة ، كذالك تبادل وسائل التخزين دون عمل فحص مسبق مثل الأقراص والذاكرة المتنقلة وإرسال الملفات داخل الشبكة المحلية . للفيروس ثلاث خواص مؤثرة وهي :

1. التضاعف : تتم عملية تضاعف الفيروس عند التحاق الفيروس بأحد الملفات وهنا تتم عملية زيادة عدد العمليات التي تتم إلى ملايين العمليات مما يسبب البطء في العمل أو توقف الحاسب عن العمل .
2. التخفي : لابد للفيروس من التخفي حتى لاينكشف ويصبح غير فعال ، ولكي يتخفى فأنه يقوم بعدة أساليب منها على سبيل المثال صغر حجم الفيروس لكي سينالة الإختباء بنجاح في الذاكرة أو ملف أخر .
3. إلحاق الأذى : قد يتراوح الأذى الذي يسببه الفيروس بالأكتفاء بإصدار صوت موسيقي أو مسح جميع المعلومات المخزنة لديك ، ومن الأمثلة الأخرى في إلحاق الأذى إلغاء بعض ملفات النظام ، إغلاق الحاسب من تلقاء نفسه عند الدخول على الإنترنت مثلا أو إلغاء البرنامج المكتوب على BIOS .

- هجوم تعطيل الخدمة

هذا النوع من الخدمة يقوم فيه المتعدي بإجراء أعمال خاصة تؤدي إلى تعطيل الأجهزة التي تقدم الخدمة Server في الشبكات .

- مهاجمة المعلومات المرسلة

هو إعتراض المعلومات عند إرسالها من جهة إلى أخرى ، ويحدث هذا التعامل غالباً أثناء تبادل الرسائل خلال الشبكات - الإنترنت - الشبكات التي تستخدم شبكة الهاتف العامة

- هجوم السيطرة الكاملة

في هذا النوع يقوم المتعدي بالسيطرة الكاملة على جهاز الضحية والتحكم في جميع ملفاته كما لو كانت في جهازه هو ويمكن للمتعدي مراقبة الضحية بصورة كاملة . يتم الهجوم بعد أن يضع المتعدي ملف صغير على جهاز الضحية عن طريق البريد الإلكتروني أو وسيلة أخرى أو عن طريق إستغلال نقاط الضعف في أنظمة التشغيل .

- هجوم التضليل

وفيه يقوم المتعدي بإنتحال شخصية موقع عام . كما يمكن للمتعدي أن ينتحل شخصية مستخدم موثوق به للحصول على معلومات غير مصرحة له .

- الوصول المباشر لكوابل التوصيل

يقوم المتعدي بالوصول المباشر لأسلاك التوصيل والتجسس على المعلومات المارة ، ولكنه هجوم صعب ويتطلب عتاد خاص .

طرق وأدوات لحماية أمن المعلومات

- التأمين المادي للأجهزة والمعدات
- تركيب مضاد فيروسات قوي وتحديثه بشكل دوري
- تركيب أنظمة كشف الإختراق وتحديثها
- تركيب أنظمة مراقبة الشبكة للتنبيه عن نقاط الضعف التأمينية
- عمل سياسة للنسخ الإحتياطي
- إستخدام أنظمة قوية لتشفير المعلومات المرسلة
- دعم أجهزة عدم إنقطاع التيار الكهربائي
- نشر التعليم والوعي الأمني

الإبتزاز الإلكتروني والجريمة الإلكترونية

أفرز التطور والتقدم العلمي والتقني في مجال الإتصالات و تكنولوجيا المعلومات وشبكة الإنترنت (وسائل التواصل الإجتماعي) أنماطاً مستحدثة من الجرائم المعقدة في طرق إرتكابها وفي وسائل كشفها ، وتشكل هذه الجرائم خطراً يؤرق المجتمع الدولي والمحلي على حد سواء ، وعليه كان لابد من التوعية والتطرق للأفعال التي تعرض من يرتكبها للمساءلة القانونية وتطبيق العقوبة التي تتناسب مع جسامة الفعل المرتكب .

يعرف الإبتزاز الإلكتروني : هو عملية تهديد وترهيب للضحية بنشر صور أو مواد فيلمية أو تسريب معلومات سرية تخص الضحية ، مقابل دفع مبالغ مالية أو إستغلال الضحية للقيام بأعمال غير مشروعة لصالح المبتزين كالإفصاح بمعلومات سرية خاصة بجهة العمل أو غيرها من الأعمال الغير قانونية .

وعـــادة مـــا يـــتم تصـــيد الضـــحايا عـــن طريـــق البريـــد الإلكترونـــي أو وســـائل التواصـــل الإجتمـــاعي المختلفـــة كـــ الفـــيس بـــوك ، تـــويتر ، وإنســـتغرام وغيرهـــا مـــن وســـائل التواصـــل الإجتمـــاعي نظـــراً لإنتشـــارها الواســـع وإســـتخدامها الكبيـــر مـــن قبـــل جميـــع فئـــات المجتمـــع وتتزايـــد عمليـــات الإبتـــزاز الإلكترونـــي فـــي ظـــل تنـــامي عـــدد مســـتخدمي وســـائل التواصـــل الإجتمـــاعي والتســـارع المشـــهود فـــي اعـــداد بـــرامج المحادثـــات المختلفة .

عملية الإبتزاز

غالبـــاً تبـــدأ العمليـــة عـــن طريـــق إقامـــة علاقـــة صـــداقة مـــع الشـــخص المســـتهدف ، ثـــم يـــتم الإنتقـــال إلـــى مرحلـــة التواصـــل عـــن طريـــق بـــرامج المحادثـــات المرئيـــة ، ليقـــوم بعـــد ذلـــك المبتـــز بإســـتدراج الضـــحية وتســـجيل المحادثـــة التـــي تحتـــوي علـــى محتـــوى مســـيء وفاضـــح للضـــحية ثـــم يقـــوم أخيـــراً بتهديـــده وإبتـــزازه بطلـــب تحويـــل مبـــالغ ماليـــة أو تســـريب معلومـــات ســـرية ، وقـــد تصـــل درجـــة الإبتـــزاز فـــي بعـــض الحـــالات إلـــى إســـناد أوامـــر مخلـــة بالشـــرف و الأعـــراف والتقاليـــد مســـتغلاً بـــذلك إستســـلام الضـــحية وجهلـــه بالأســـاليب المتبعـــة للتعامـــل مـــع مثـــل هـــذه الحالات .

تصنيفات وأنواع الجرائم الإلكترونية

أ – تصنيف الجرائم تبعاً لنوع المعطيات ومحل الجريمة

- الجرائم التي تمس بقيمة معطيات الحاسوب
- الجـــرائم التـــي تمـــس بالمعطيـــات الشخصـــية أو البيانـــات المتصـــلة بالحياة الخاصة
- الجـــرائم التـــي تمـــس بحقـــوق الملكيـــة الفكريـــة للبـــرامج الحاســـوبية ونظمه (جرائم قرصنة البرمجيات)

ب – تصنيف الجرائم تبعاً لدور الحاسوب في الجريمة

- الجـــرائم التـــي تســـتهدف عناصـــر (الســـرية والســـلامة ووفـــرة المعطيات والنظم) وتضم :
- الـــدخول غيـــر القـــانوني (غيـــر المصـــرح بـــه) : حيـــث يقـــوم الشـــخص بـــإختراق الشـــبكات والحواســـيب التـــي تـــرتبط بشـــبكة الإنترنـــت وذلـــك بـــإختراق نظـــام الأمـــن فـــي الشـــبكة والـــدخول إلـــى الجهاز والكشف عن محتوياته .
- الإعتراض غير القانوني .
- تـــدمير المعطيـــات (يكـــون هـــذا الأمـــر بعـــد إختـــراق الشـــبكة وقيـــام الشـــخص بمســـح البيانـــات أو تشـــويها أو تعطيـــل البـــرامج المخزنـــة وجعلها غير قابلة للإستخدام .
- إعتراض النظم .
- أساءة إستخدام الأجهزة .

- الجرائم المرتبطة بالحاسوب وتضم :
- التزوير المرتبط بالحاسوب - الإحتيال المرتبط بالحاسوب

- الجـــرائم المرتبطـــة بـــالمحتوى ، وتضـــم طائفـــة واحـــدة وفـــق هـــذه الإتفاقيـــة ، وهـــي الجـــرائم المتعلقـــة بالأفعـــال الإباحيـــة واللـــلا أخلاقية .
- الجرائم المرتبطة بالإخلال بحق المؤلف وقرصنة البرمجيات

ج – تصنيف الجرائم تبعاً لمساسها بالأشخاص والأموال

- طائفـــة الجـــرائم التـــي تســـتهدف الأشـــخاص وتضـــم طـــائفتين رئيسيتين هما :
- الجـــرائم الغيـــر جنســـية التـــي تســـتهدف الأشـــخاص – Non Sexual Crimes – Against Persons
- طائفـــة الجـــرائم الجنســـية Sexual Crimes وتشـــمل القتـــل بالحاسوب Computer Murder

- طائفة جرائم الأموال – عدا السرقة – أو الملكية المتضمنة أنشطة الإختراق والإتلاف .
- جرائم الإحتيال والسرقة Fraud And Theft Crimes
- وقد نظن أن السرقة مقصورة على الأشياء العادية كالأموال والممتلكات ، لكن السرقة طالت أيضاً المعلومات الإلكترونية المخزنة في الأجهزة والمرسلة عبر الشبكات .
- جرائم التزوير Forgery ويقصد بها عملية التلاعب بالمعلومات المخزنة في الجهاز ، أو إعتراض المعلومات المرسلة بين الحواسيب المرتبطة بالشبكة وذلك لغرض التضليل عن طريق تغييرها وتحريفها وتزويرها .
- جرائم المقامرة gambling
- الجرائم الأخرى المضادة للدين والأخلاق الحميدة والآداب السامية .

وهي تنطوي على بث مواد وأفكار ذات إتجاهات هادمة ومعادية للدين ، وهي من وجهة نظر الكثير أخطر أنواع الجرائم الإلكترونية التي تواجه العالم الإسلامي ، حيث تقوم بعض الجهات المتطرفة والمعادية ببث مواد ومعلومات تخالف الدين والثقافة الإسلامية ، وتشكك فيهما وتزرع في عقول الأجيال الجديدة أفكاراً مشوهة تزعزع إيمانهم وتضعفه ولاننسى تأثير هذه المواد في الأخلاق الحميدة والعادات والقيم الفاضلة ، خاصة مع إنتشار الصور الجنسية الفاضحة والمقالات المغرضة والأفلام والدعايات والمواقع المخلة بالآداب.

- جرائم الحاسوب المضادة للحكومة Crimes Against Government Against Morality

الحاسوب هدف وأداة

وكما نلاحظ فإن الحاسوب له صلة وثيقة بالجرائم الإلكترونية ، فلا جريمة إلكترونية بدون حاسوب ، فهذا الجهاز له دوراً أساسي وفعال في مجال الجريمة ويؤدي ثلاث أدوار في ميدان إرتكاب

الجـرائم ، ودوراً رئيسـاً فـي حقـل إكتشـافها **ففـي حقـل إرتكـاب الجـرائم يكون له الأدوار التالية :**

الأول : يكـون الحاسـوب هـدفاً للجريمـة (Target Of An Offense) وذلـك كمـا فـي حالـة الـدخول غيـر المصـرح بـه إلـى النظـام ، أو زراعـة الفيروسـات لتـدمير المعطيـات والملفـات المخزنـة أو تعـديلها ، أو كمـا فـي حالـة الإسـتيلاء علـى البيانـات المخزنـة أو المنقولـة عبـر النظم .

الثاني : يكون الحاسوب أداة الجريمة لإرتكاب جرائم تقليدية

الثالـث : يكـون الحاسـوب بيئـة الجريمـة ، وذلـك كمـا فـي تخـزين البـرامج المقرصـنة فيـه ، أو فـي حالـة إسـتخدامه لنشـر المـواد غيـر القانونيـة ، أو إسـتخدامه أداة تخـزين أو إتصـال لصـفقات تـرويج المخدرات و أنشطة الشبكات الإباحية ونحوها.

أمـا مـن حيـث دور الحاسـوب فـي إكتشـاف الجريمـة ، فإنـه يسـتخدم الأن علـى نطـاق واسـع فـي التحقيـق الإسـتدلالي لجميـع الجـرائم ، ثـم إن جهـات تنفيـذ القـانون تعتمـد علـى الـنظم التقنيـة فـي إدارة المهـام مـن طريـق بنـاء قواعـد البيانـات ضـمن جهـاز إدارة العدالـة والتطبيـق القانوني .

ومـع تزايـد نطـاق جـرائم الحاسـوب ، وإعتمـاد مرتكبيهـا علـى وسـائل التقنيـة المتجـددة والمتطـورة ، فإنـه أصـبح لزامـاً إسـتخدام نفـس وسـائل الجريمـة المتطـورة للكشـف عنهـا ، ومـن هنـا يـؤدي الحاسـوب بذاتـه دوراً رئيسـياً فـي كشـف الجـرائم وتتبـع فاعليهـا بـل وإبطـال أثـر الهجمـات التدميريـة لمخترقـي الـنظم وتحديـداً هجمـات الفيروسـات وإنكار الخدمة وقرصنة البرمجيات .

وعنـدما نتسـاءل عـن هويـة الـذين يقومـون بإرتكـاب جـرائم الحاسـوب والإنترنـت نجـد الإجابـة فـي تصـنيف يعـد مـن أفضـل التصـنيفات لمجرمـي التقنيـة وهـو الـذي أورده David Icove , Karl Seger And William Vonstorcho فـي مـؤلفهم جـرائم الحاسـوب الصـادر عـام 1995 حيـث قسـموا مجرمـي التقنيـة إلـى ثـلاث طوائـف المختـرقين والمحتـرفين والحاقـدين ، ومـن المهـم التمييـز بـين صـغار

السن من مجرمي الحاسوب البالغين الذين يتجهون للعمل معاً لتكوين المنظمات الإجرامية الخطرة .

ودوافع إرتكاب جرائم الحاسوب هي إما السعي إلى تحقيق الكسب المالي أو الإنتقام من مسؤول العمل وإلحاق الضرر به أو حتى الرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية.

ماهو حجم الجريمة الإلكترونية ؟

تعتبر شبكة الإنترنت أكبر شبكة في تاريخ البشرية ، وهي أحدث أدوات العالم لربط أكثر من 500 مليون حاسوب في أكثر من 200 دولة ، ويستخدمها أكثر من مليار مشترك والجريمة الإلكترونية هي صراع بين التقدم التقاني وحماية وأمن الخصوصية Privacy يقال إن السرقات السنوية وصلت إلى أكثر من مليوني حالة ، إضافة إلى مئات الألاف من الشركات التي وقعت ضحية القراصنة والمتلصصين ، وذلك بسبب الخلل وعدم الإحكام في وسائل الأمن لدى المواقع الإلكترونية والتي يجب سدها في أقرب وقت ، حيث أنه من المتوقع أن تتضاعف هذه الأرقام .

من هم القراصنة

إن معظم المتسببين في عمليات القرصنة هم أصلا مبرمجون لديهم دوافع نفسية غير سوية ، كأن الواحد منهم يقول "أنا هنا ألا تشعرون بي" ونستطيع تقسيم هؤلاء المؤلفين أو القراصنة إلى ثلاث أنواع :

- ذوو الياقات البيضاء : الذين يهاجمون الحواسيب بطريقة شرعية وبأوامر من السلطة وبهجمات مخططة وينظمون الهجوم عندما يطلب منهم.
- ذوو الياقات الرمادية : أحياناً يقومون بالمهمة كقراصنة أشرار وأحيان الهدف أخر، وبعضهم يؤمنون بنظرية "حرية المعلومات أيا كانت هذه المعلومات" ومنها التي تتعلق بتأمين الأجهزة والشبكات ومعرفة نقاط الضعف ولايرون غضاضة في الهجوم على أي موقع من أجل المزيد من إجراءات الأمن والوقاية .

- ذوو اليقـــات الســـوداء : يهـــاجمون بهـــدف ســـطو مـــالي أو معلوماتي ضار .

كـــذلك يجـــب التفريـــق بـــين نـــوعين همـــا **العـــابثون** Hackers **والمتلصصـــون** Crackers فأمـــا **العـــابثون** فتكـــون أفعـــالهم إمـــا بســـبب الهوايـــة ، أو العمـــل أصـــلا لتخريـــب مواقـــع هامـــة أو شـــراء بعـــض المنتجـــات والبـــرامج بطـــرق ملتويـــة ، وأيضـــاً الحصـــول علـــى معلومـــات هامـــة مـــن أمـــاكن مختلفـــة ، وأخطـــرهم صـــانعو الفيروســـات وملفـــات كســـر الحمايـــة ، ذلـــك أنهـــم مبرمجـــون متخصصـــون ذوو قـــدرات عاليـــة جـــداً أمـــا **المتلصـــص** هـــو مســـتخدم عـــادي أو هـــاوٍ لديـــه القـــدرة علـــى البرمجـــة والبحـــث الجيـــد علـــى صـــفحات الإنترنـــت للوصـــول إلـــى ملفـــات كســـر الحمايـــه بغـــرض إســـتعمالها ، وأيضـــاً يكـــون مـــن أصـــحاب النســـخ غير القانوني للبرامج .

كيف يقوم المحتال بإبتزازك إلكترونياً

المجـــرم غايتـــه وهدفـــه أشـــياء كثيـــرة وأهمهـــا المـــال والجـــنس وهـــذه اولويتـــه إمـــا أن كـــان لايريـــد ذلـــك فهـــو يبحـــث عـــن شـــيء خـــاص بـــك كـــأن يخـــرب حياتـــك أو يفصـــلك عـــن شـــريكك أو يـــدمر أعمالـــك بطـــرق كثيـــرة وســـهلة إن وقـــت بيـــد مجـــرم محتـــرف فـــي الإبتـــزاز الإلكترونـــي وغالبـــا ما يقوم المجرمون بهذه الأعمال لإبتزازك إلكترونياً

- يحـــاول أن يســـرق حســـاباتك الخاصـــة فـــي المواقـــع كإرســـال لـــك روابط تصيد إحتيالي أو يرسل لك ملفات يطلب منك تحميلها.
- يثيـــر فضـــولك ويرســـلك إلـــى مواقـــع تجهلهـــا ويطلـــب منـــك ملـــئ معلومات خاصه بك.
- يقـــدم لـــك أشـــياء تحلـــم بـــأن تتقمصـــها كـــأن يقـــول لـــك (ســـأجعلك تختـــرق حســـابات أصـــدقائك وتشـــاهدهم علـــى الكـــاميرا مـــن غيـــر أن يعلموا).
- يحـــاول جاهـــداً أن يحصـــل علـــى صـــورك أو مقـــاطع خاصـــة بـــك أو أن يتراسل ويتبادل الملفات بينك وبينه .
- يطلـــب منـــك التحـــدث علـــى ســـكايب أو أحـــد مواقـــع التواصـــل الإجتمـــاعي ويقـــوم بفـــتح الكـــاميرا فـــوراً والشـــخص الموجـــود

يوهمك أنه هو الشخص الحقيقي وما هو إلا عبارة عن تسجيل فيديو سابق .

- يعرض أجزاء من جسمه دون أن تطلب منه ذلك ليطلب منك أن تعرض جسمك أنت أيضاً.
- يجمع أكبر قدر من معلوماتك وحسابات أصدقائك وأرقامهم وعناوينهم أيضاً.

هذه أغلب الأمور التي يقوم بها المجرمون ليوقعوا بضحيتهم من أجل إبتزازهم جنسياً أو إلكترونياً ثم يستخدم هذه المواد برفعها على اليوتيوب أو على مواقع التواصل الإجتماعي أو على أي موقع أخر ليستفزك بها ويهينك ويبتزك.

كيفية تجنب الوقوع في فخ الإبتزاز

الأمر يحتاج فقط للوعي والمعرفة والثقافة الإلكترونية التي تمكنك من عدم الوقوع في فخ أحد المجرمين الذين يتصيدون المجني عليه عن طريق جهلهم ببعض الأمور البسيطة وتكاد تكون بسيطة جداً حيث أنك فقط تحتاج إلى أن تتحقق من بضعت أمور وعندما تتأكد من عدم صحتها يجب عليك فوراً أن تبتعد عن إتخاذ أي إجراء من قبلك

- تجنب قبول طلب الصداقة من قبل أشخاص غير معروفين.
- عدم الرد والتجاوب على أي محادثة ترد من مصدر غير معروف.
- تجنب مشاركة معلوماتك الشخصية حتى مع أصدقائك في فضاء الإنترنت (أصدقاء المراسلات).
- أرفض طلبات إقامة محادثات الفيديو مع أي شخص ، ما لم تكن تربطك به صلة وثيقة.
- لاتنجذب للصور الجميلة والمغرية وتأكد من شخصية المرسل.
- لاتتصفح المواقع الجنسية غالباً ما يكون هدفها تتبعك وسرقة معلوماتك وسرقة معلومات المتصفح الخاص بك ناهيك عن زرع برامج التجسس من غير علمك وتعتبر وسيلة إلى إسقاط الكثير من الأشخاص.

- إبتعد تماماً عن الفضول في الإنترنت وخاصة إن لم تكن محترف في التعامل مع المواقع الغير موثوقة كأن تجد رابط في بريدك أو في مواقع التواصل الإجتماعي بعنوان فاضح أو مثيرة للفضول بشكل غريب ويطلب منك إدخال معلومات خاصة بك كتسجيل الدخول مجدداً للبريد أو للحساب أو حتى أحياناً لا يحتاج الأمر إلى إرسال بياناتك إذا كان منشئ رابط التصيد الإحتيالي محترف فيرسلك إلى رابط يقوم بتحميل ملفات بشكل تلقائي إلى جهازك.
- في حال حدوث خلل في الحاسوب أو الهاتف المحمول لاتقم في تصليحه الإعند فني موثوق بسبب زرع برامج تجسس وفيروسات تنقل معلومات الجهاز للشخص الأخر.
- يجب عليك أن لاتخاف أبدا من التحدث إلى أهلك أو أصدقاء في حال تعرضت لأي نوع من أنواع الإبتزاز أو الإهانة.

في حال تعرضك لعملية إبتزاز

- عدم التواصل مع الشخص المبتز ، حتى عند التعرض للضغوطات الشديدة .
- عدم تحويل أي مبالغ مالية ، أو الإفصاح عن رقم بطاقة البنك.
- تجنب المشادات مع المبتز وعدم تهديده بالشرطة ، وقم بالإبلاغ عند وقوع الحادثة مباشرة لدى الجهات المختصة.
- إغلاق جميع الحسابات التي قدمتها لهذا الشخص أو يعرفها عنك.
- لاتجاري المجرم لأنه شخص محترف جداً في إحباطك وترهيبك وتخويفك إبتعد عنه فقط (أفضل شيء ممكن أن تفعله) .
- لاترضخ لأي طلب يطلبه المبتز أبداً حتى لو هددك بأنه سيرسل بياناتك لشخص مثل زوجك أو أحد من أهلك.
- إن كنت شاب أو فتاة قم باللجوء إلى صديق أو قريب تثق فيه ثقة عمياء تعرف أنه واعي وأطلب منه المساعدة في تقديم بلاغ للشرطه أو المساعدة في حل المشكلة.

- لا تتصرف من تلقاء نفسك الإ إذا كنت محترف في معرفة هوية المجرم .
- ثق تماماً أنه لن يؤثر عليك بتاتاً ما لم ترضخ لطلباته لذلك لا تعطي الأمر أكثر من حجمه بحيث تفقد أعصابك أو ينقطع أملك بالتخلص من هذه المصيبة .
- إغلاق هاتفك فوراً .

قانون الجريمة الإلكترونية

نظراً لكون هذا النوع من الجرائم حديثاً بعض الشيء فإن القوانين التي تنظم التعامل معه تعتبر قليلة ، أو ربما غير موجودة في بعض الدول وحديثاً صدرت قوانين لمكافحة جرائم تقنية المعلومات مثل الغرامة أو الحبس وغيرها.

تلميحات للأمان عند إستخدام كمبيوتر عام والإنترنت

- لاتحفظ معلومات تسجيل الدخول ، قم دائماً بتسجيل الخروج من المواقع على الإنترنت عبر الضغط على " تسجيل الخروج " على الموقع فلا يكفي إغلاق إطار المستعرض (المتصفح) أو كتابة عنوان أخر .

- تشمل برامج عديدة وخاصة برامج الرسائل الفورية ميزات تسجيل دخول تلقائي تحفظ إسم المستخدم وكلمة المرور عطل هذا الخيار تحسباً أن يقوم شخصاً أخر بتسجيل الدخول بإسمك .

- لاتترك الكمبيوتر من دون مراقبة أثناء عرض معلومات حساسة على الشاشة إذا أضطررت لترك الحاسوب فقم بتسجيل الخروج من كافة البرامج وأغلق كافة الإطارات التي قد تعرض معلومات حساسة .

- لاتـــدخل معلومـــات حساســـة فـــي كمبيـــوتر عـــام ، تـــوفر هـــذه الإجـــراءات بعـــض الحمايـــة ضـــد المتطفلـــين العرضـــيين الـــذين يســـتخدمون الكمبيـــوتر العـــام بعـــد أن تكـــون قـــد إســـتخدمته بنفســـك وأحيانـــاً يكـــون علـــى هـــذه الأجهـــزة بـــرامج تجســـس وتســـجيل المعلومات .

مثـــال : علـــى المعلومـــات الحساســـة ارقـــام بطاقـــات البنـــك والعمـــل وغيرها

- محـــو بيانـــات التصـــفح مـــن المتصـــفح بعـــد الإنتهـــاء مـــن العمـــل على الجهاز العام .

الخاتمة

ثمـــة جهـــود كبيـــرة تبـــذل لمحاربـــة الجريمـــة الإلكترونيـــة بكافـــة أشـــكالها ، لكـــن لتميـــز هـــذه الجـــرائم وعـــدم تقليـــديتها،من الصـــعب الكشـــف عنهـــا وتحديـــد الـــدليل المـــادي الـــذي يـــدين مرتكبهـــا لـــذلك مـــن المتوقـــع أن هـــذا النـــوع مـــن الجـــرائم سيســـتمر ويطغـــى علـــى ســـاحة الإجـــرام بقـــدرٍ كبيـــر ،وســـيتطور مـــع مـــرور الوقـــت إلـــى مـــاهو أخطـــر وأعقـــد ،لـــذا فـــإن وجـــود إســـتراتيجية فعالـــة لـــدى الـــدول تحـــارب هـــذه الجـــرائم هـــي الوســـيلة الضـــامنة لتقليلهـــا ومحاولـــة الـــتحكم بهـــا ، ولاننســـى دور الأفـــراد فـــي محاربتهـــا عـــن طريـــق تبصـــيرهم بإيجابيـــات وســـلبيات إســـتخدام شـــبكة الإنترنـــت ، وحـــث الشـــركات المتخصصـــة علـــى إنتـــاج بـــرامج حمايـــة متخصصـــة تهـــدف إلـــى حمايـــة البـــرامج الأخـــرى ومتصـــفحات الإنترنت.