تمهيد:

يمثل أمن المعلومات حماية وتأمين الموارد المستخدمة كافة والعمل على سريتها وسلامتها، وفي غياب أمن المعلومات، أو نقصه، أو توقفه وعدم الاستفادة القصوى منه يؤدي إلى فقدان الثقة مما يجعله عبئا على المؤسسة. وعلى هذا الأساس يجب حماية المؤسسة والمعلومات من الأضرار التي قد تؤدي إلى فشل الأداء وتعود بالخسارة على المؤسسة والعاملين فيها.

1-مخاطر استخدام تكنولوجيا المعلومات والاتصال: ومن هذا المنطلق يمكن تصنيف مخاطر استخدام تكنولوجيا المعلومات من حيث المصدر إلى (الدلاهمة، 2013، ص17):

أ-مخاطر داخلية: المصدر الرئيس للمخاطر الداخلية يتمثل في موظفي المؤسسة؛ لأنهم الأكثر دراية ومعرفة بنقاط الضعف في نظام الرقابة الداخلي ، ولما لهم من صلاحيات في الدخول إلى النظام حيث ساعد الاستخدام الواسع لتكنولوجيا المعلومات في زيادة المخاطر، ويؤثر هذا النوع من المخاطر على مراحل عمل النظام المختلفة (مرحلة إدخال البيانات، ومرحلة معالجة البيانات، ومرحلة مخرجات النظام)

ب- مخاطر خارجية: تمثل الكوارث الطبيعية وقراصنة المعلومات أهم مصادر المخاطر الخارجية وتتمثل هذه المخاطر في:

- الفيروسات.
- قراصنة المعلومات.
- التطور التكنولوجي.

1-1-مخاطر الفيروسات على المؤسسات:

من أخطر ما يواجه الشبكات المعلوماتية للمؤسسات إمكانية تدمير ما بها من بيانات أو إتلافها أو تعطيلها عن العمل، وذلك من خلال الفيروس المعلوماتي، وما ساعد في ظهوره وانتشاره ثورة الاتصالات الالكترونية الهائلة، فأصبحت وسائل الاتصال من وسائل انتقال الفيروس إلى مسافات بعيدة جدا من خلال شبكة الانترنيت، فيمكن للمشترك فيها استخدامها في نقل الفيروس إلى أبعد مكان في العالم .

1-1-1-تعريف الفيروس المعلوماتي:

الفيروس المعلوماتي هو عبارة عن برنامج، يقوم بنسخ نفسه على أجهزة الكمبيوتر، وله القدرة على ربط نفسه بالبرامج الأخرى، وكذا إعادة إنشاء نفسه حتى يبدو أنه يتوالد ذاتيا، ويقوم بالانتشار بين برامج الحاسب الآلي المختلفة وبين مواقع مختلفة في الذاكرة .وعند نشاطه يقوم بتدمير البرامج والبيانات المسجلة والمخزنة داخل الحاسب،

كما يسبب فشل البرامج وعرض رسائل مزعجة مع تخفيض أداء النظام، وقد يصل الأمر إلى تدمير كل ملفات القرص الصلب المصاب (العاني، 2007، ص119).

توجد من الفيروسات التي تقوم بالتقاط البريد الالكتروني وتقوم بتأليف وإرسال رسائل مرفقة بملحقات ملوثة . وقد ساهم البريد الالكتروني في انتشار الفيروس المعلوماتي بدرجة كبيرة، لأنه يمكن من إرسال رسائل إلى آلاف المستخدمين الذي يشتركون في نظم الحاسب.

1-1-2-خصائص الفيروس المعلوماتي:

تظهر خطورة الفيروس المعلوماتي من خلال خصائصه الضارة المميزة له وتتمثل في (العاني، 2007، ص120):

-القدرة على الاختفاء :حيث تكون للفيروس المعلوماتي القدرة على الاختفاء والتمويه، ويستخدم في ذلك عدة وسائل، كأن يرتبط ببرامج شائعة الاستخدام ومجرد نسخها يجعله ينتقل إلى القرص، وهناك فيروسات تدخل إلى الحاسب في شكل ملفات مختفية لا تظهر عند استعراض فهرس الملفات، ومنها ما تستقر في أماكن مثل الذاكرة التي يصعب ملاحظتها فيها.

-القدرة على الانتشار والاختراق :ساعد تقدم شبكة الاتصالات الحديثة انتشار الفيروس بين ملايين الأجهزة، وساعد في ذلك أيضا سرقة البرامج وتطعيمها بالفيروس وإعادة بيعها، والأكثر من هذا وذاك هو انتشاره في ثوان معدودة من مكان لآخر من العالم، وانتشاره السريع داخل الكمبيوتر نفسه من خلال عمل نسخ عديدة في بضع ثوان.

-القدرة على التدمير :يتمثل نشاط الفيروس التدميري في قيامه بمسح البيانات المخزنة على وسائط أي مسح البيانات وتحويلها إلى الصفر، لذا يسمى بالقنبلة الموقوتة، ويظهر ضرر الفيروس المعلوماتي على البرامج كبيرا جدا، ويلحق الضرر كذلك بأجهزة الحاسب الآلي ولكن بصورة بسيطة.

1-2-القرصنة الالكترونية ومخاطرها على المؤسسات:

من الأسباب القوية لتخوف المؤسسات من استخدام تقنيات الاتصال الحديثة هي المخاطر التي تهدد أمنها، الناتجة أساسا عن التعامل عبر الشبكات المفتوحة خاصة الانترنيت التي ظهر معها ابتكارات في الأساليب الالكترونية للقرصنة.

ويعرف الاختراق الالكتروني بأنه القدرة على الوصول لجهاز أو شبكة أو موقع بطريقة غير مشروعة عن طريق الثغرات الأمنية الموجودة في نظام الحماية الخاص بالهدف، كالدخول على أجهزة الآخرين عنوة أو التلصص داخل شبكاتهم. حيث يتاح للشخص المخترق أن ينقل أو يمسح أو يضيف ملفات أو برامج كما أنه بإمكانه أن يتحكم في نظام التشغيل فيقوم بإصدار أوامر مثل إعطاء أمر الطباعة أو التصوير أو التخزين (درار، 2017، ص117).

1-2-1-أساليب القرصنة الإلكترونية:

من أهم الأساليب المتبعة في تهديد أمن المؤسسات من قبل المخترقين المجرمين أو العابثين نذكر(العاني، 2007، ص116):

أ -التقمص: إن التكلفة المنخفضة لبناء موقع على الإنترنت، وسهولة نسخ صفحات من مواقع شبكية، يجعل الأمر سهلا جدا لبناء مواقع غير شرعية، تتقمص واجهة مواقع حقيقية لخداع الزوار وإعطاء معلوماتهم الشخصية وبطاقات الائتمان الخاصة بهم، ظنا منهم بأن المواقع المتقمصة هي مواقع لشركات محترمة.

ب -التنصت: عند تصفح المواقع الشبكية على الإنترنت، والقيام بعمليات شراء، فإن ما يحدث هو انتقال المعلومات عبر الإنترنت، والتي قد تكون أرقام بطاقات ائتمان أو معلومات شخصية .وتكون هذ المعلومات وبخاصة التي لم يتم تشفيرها عرضة لسرقتها عن طريق التنصت، واستخدامها في تنفيذ أعمال غير مشروعة من قبل المخترقين.

ج -التخريب المتعمد: قد يلجأ البعض من المنافسين أو المخترقين إلى استخدام أساليب اختراق موقع المنشأة، وتغيير بعض الصفحات بغية الإساءة إلى المنشأة أو تعطيل الموقع بحيث يصبح غير قادر على تقديم الخدمة إلى العملاء.

د -تغيير البيانات: ليس من الممكن فقط القيام بعمليات التنصت على البيانات المتناقلة على الانترنت من خلال إنجاز صفقات تجارية إلكترونية، وإنما يمكن أيضا القيام بالعبث بتلك البيانات وإحداث تغييرات فيها كتغيير قيمة المنتج، أو الخدمة أو حتى تغيير المعلومات الشخصية.

هـ-الاعتداء باستعمال أسلوب انتحال عنوان IP :تقوم معدات الشبكات مع نظام شغال باستخدام عنوان IPلجهاز كمبيوتر من أجل تحديد عنوان ساري المفعول، حيث يمكن تعديل عنوان IP لزبون من قبل مهاجم من أجل التمكن من قراءة وكتابة المعلومات الخاصة به، فمن الأسهل للمهاجمين بعد الوصول إلى الشبكة كنتيجة لتعديل عنوان IPالساري المفعول إعادة كتابة أو حذف المعلومات (بوالفول، 2018، ص313).

1-2-2-المخاطر الناتجة عن استخدام تلك الأساليب:

على الرغم من الفوائد والمزايا التي تحققها تقنيات الاتصال الحديثة للمنشآت والدول على حد سواء، لا يزال يهدد تلك التقنيات مخاطر متعلقة بمدى توفر خصوصية البيانات والمعلومات الخاصة بالمتعاملين، لاسيما الانترنيت فيما يلي (العاني، 2007، ص ص117، 118):

أ -تغيير محتويات معلومات المنشأة على شبكة الاتصال الالكتروني :

والتي يقوم بها بعض المحترفين، بالهجوم واختراق البيانات المتوفرة على الشبكة، أو تقوم بها بعض المؤسسات المنافسة لهذه المؤسسة بغية الإساءة لها وإفساد علاقاتها مع عملائها، وما يترتب عن هذا الهجوم من تغيير للبيانات الخاصة بالمشتركين في تنفيذ الصفقات الالكترونية، فقد يحدث تغيير اسم المدفوع لأمره في الشيكات الالكترونية، أو تغيير المبلغ المحول إلى حساب بنكي، ومن خلال ذلك يمكنه تحصيل أموال بعض التجار، العملاء والمستهلكين.

ب –استخدام البيانات على شبكة الاتصال الإلكتروني لتنفيذ بعض الأعمال غير المشروعة:

يمكن أيضا لمخترقي مقر بيانات المؤسسة على الشبكة الالكترونية للاتصال، أن يقوموا باستخدام تلك البيانات في تنفيذ أعمال غير مشروعة، كتنفيذ بعض الجرائم، وإخفاء بعض المسروقات .فمن خلال الاختراق يمكن سرقة أرقام حسابات العملاء وسرقة أرقام بطاقات الائتمان، فضلا عن سرقة معلومات الفواتير، أما من خلال التقمص الذي يقوم به المحتالين من خلال دفع مبلغ بسيط لإنشاء موقع لهم على شبكة الانترنت، فيتخذون ذلك ستارا للقيام ببعض عمليات النصب، حيث يقدموا منتجات وهمية، وفي المقابل يحصلون من العميل على رقم بطاقته، الامر الذي يساعدهم على سرقة أموال العملاء.

ج –التعرف على النظم والسياسات الداخلية للمؤسسة :

حيث يمكن للمنافسين للمؤسسة التي تمارس أعمالها على الشبكة الدخول إلى مقر معلوماتها والقيام بالعبث بنظامها الداخلي، ومن خلال ذلك يصبح ممكنا إلغاء بعض المعلومات الداخلية ذات الأهمية لهذه المؤسسة، أو الحصول على المعلومات التي تخص السياسات الداخلية لها، وبالتالي استغلالها استغلالا في غير صالحها، مما قد يترتب عنه نتائج سلبية لهذه المؤسسة وقد يصل الأمر إلى حد توقف نشاطها.

د –توقف مقر معلومات المنشأة على الشبكة الالكتروني عن العمل :

حيث يقوم المهاجمين بشغل المقر الرئيسي لمعلومات المؤسسة بالكثير من المعاملات والاستفسارات والرسائل، مما يترتب عليه فقدان قدرة المقر على التعامل مع المستخدمين له، وهو ما يشكل خطرا كبيرا على المؤسسة التي تعتمد بصورة أساسية على هذا المقر لتوفير خدماتها لعملائها .

هـ –تخريب مقر معلومات المؤسسة على الشبكة :حيث يقوم المهاجمون بالدخول إلى البرامج الخاصة بإدارة المقر وتغيير بعض خصائصه، فيحدث أخطاء في التشغيل أو تخريب المقر وتوقفه كلية عن العمل.

2–الأمن الالكتروني في المؤسسات:

إن استخدام اصطلاح أمن المعلومات وان كان استخداما قديما سابقا لوجود وسائل تكنولوجيا المعلومات، الا انه وجد استخدامه الشائع بل والفعلي مع شيوع الوسائل التقنية لمعالجة وخزن البيانات وتداولها والتفاعل معها عبر شبكات المعلومات– وتحديدا الإنترنت — احتلت ابحاث ودراسات أمن المعلومات مساحة كبيرة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة.

2-1- مفهوم أمن المعلومات:

لقد اختلفت المفاهيم التي أوردها الباحثون بشأن تحديد مفهوم لأمن المعلومات وفيما يأتي بعض هذه المفاهيم:

-أمن المعلومات يعني كل السياسات والإجراءات والأدوات التقنية التي تستخدم لحماية المعلومات من أشكال الاستخدام غير الشرعي كلها للموارد مثل السرقة ,والتغير ,والتعديل, والحاق الضرر بالمعلومات المتعمد (عبد الكريم، الربيعي، 2013، ص295)

-تعريف أمن المعلومات: هو الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية ، حيث تؤمن المنشأة نفسها والأفراد العاملين فيها والأجهزة ووسائط المعلومات التي تحتوي على بيانات المنشأة، وذلك في جميع مراحل تواجد المعلومة (التخزين، النقل، المعالجة) (الحمادي، 2010، ص14).

-وهناك تعريف آخر وهو عبارة السياسات والممارسات والتقنية التي يجب أن تكون داخل المؤسسة لتداول حركات الأعمال إلكترونيا عبر الشبكات بدرجة معقولة ومؤكدة من الأمان، هذا الأمان ينطبق على كل النشاطات والحركات والتخزين الإلكتروني وعلى شركات الأعمال والزبائن والمنظمين والمستفيدين وأي شخص آخر ممكن أن يكون معرضاً لمخاطر الاختراق (الحمادي، 2010، ص13).

-مفهوم أمن المعلومات من عدة زوايا وهي: زاوية أكاديمية : هو العلم الذي يبحث في نظريات واستراتيجيات توافر الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. زاوية تقنية : هي الوسائل والأدوات والإجراءات اللازم توافرها لضمان حماية المعلومات من الإخطار الداخلية والخارجية. زاوية قانونية : فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوافر المعلومات ,ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة(ليتيم، ليتيم، ص 239).

2-2- عناصر أمن المعلومات:

ان غرض وسائل أمن المعلومات هو ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها: (ليتيم، ليتيم، 2015، ص ص239، 240):

- ✓ السرية أو الموثوقية: وتعني التأكد من ان المعلومات لا تكشف ولا يطلع عليها من قبل اشخاص غير مخولين بذلك.

- ✓ التكاملية وسلامة المحتوى: التأكد من ان محتوى المعلومات صحيح ولم يتم تعديله او العبث به وبشكل خاص لن يتم تدمير المحتوى او تغيره او العبث به في اية مرحلة من مراحل المعالجة او التبادل سواء في مرحلة التعامل الداخلي مع المعلومات او عن طريق تدخل غير مشروع.
- ✓ استمرارية توفر المعلومات او الخدمة: لتأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وان مستخدم المعلومات لن يتعرض الى منع استخدامه لها او دخوله اليها .
- ✓ عدم إنكار التصرف المرتبط بالمعلومات ممن قام به: ويقصد به ضمان عدم انكار الشخص الذي قام بتصرف ما متصل بالمعلومات او مواقعها انكار انه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة اثبات ان تصرفا ما قد تم من شخص ما في وقت معين .

2-3- وسائل تحقيق أمن المعلومات:

هي مجموعة الآليات والإجراءات والأدوات التي تستخدم للوقاية من المخاطر أو تقليل الخسائر بعد وقوع الحدث على المعلومات وأنظمتها. وتتعدد وسائل الحماية من حيث الطبيعة والغرض وفيما يلي بعض هذه الآليات:

-سلامة المعلومات: لكي نحقق الأمن والسرية لمعلومات الشركة يجب أن نضع بعض السياسات والإجراءات التي تستوجب لتوفير الحماية الكافية للمعلومات لعدم الاطلاع عليها من قبل الآخرين غير المصرح لهم، ويرى المختصين والباحثين والمهتمين بتقنية المعلومات ومنهم ما أشار إليه، بأنه لابد من وضع مستويات متعددة للحماية والمرور إذا كانت طبيعة المعلومات والموارد الأخرى المخزونة تتطلب هذا النوع من الحماية، أو وضع نظام حماية فعال يقلل إلى أدنى حد ممكن مشكلة كشف المعلومات ذات الأهمية القصوى للشركة .ومن الإجراءات مثلا عمل نسخ احتياطية لبعض الملفات المهمة خشية من التدمير، أو الفقدان وكذلك تطبيق وسائل حماية إضافية مثل مفتش الكابلات، ومحلل البروتوكول الذي يستخدم لفحص محتوى الرزم المعلوماتية التي تنقل عبر شبكة اتصالات نظم المعلومات. كما إن من متطلبات امن المعلومات وضع عددا من القوانين واللوائح والتوجيهات وعلى مستوى المسؤولية عن امن المعلومات لتحديد الأدوار الرئيسة والحد الأدنى لضوابط أمن المعلومات. فضلا عما تقدم توجد وسائل مهمة لتقليل المخاطر أو الحد منها وهذه الوسائل هي(عبد الكريم، الربيعي، 2013، ص ص 298، 299):

1-البناء السليم لنظام المعلومات هو البداية الصحيحة لوضع إستراتيجية فاعلة لمراقبة وتقويم النظام ولحماية آمنة وسلامة موارده.

2-تدريب المستخدمين لنظام المعلومات في مجالات أمن المعلومات، أمن قواعد البيانات، وأمن الشبكات.
3-تطبيق إجراءات جدية وحازمة لحماية البرامج والأجهزة منذ اللحظة الأولى لتشغيل نظام المعلومات.

كما يجب التحكم في الأشخاص المسموح لهم بالوصول للمعلومات والنظم العاملة عليها، وتستخدم عملية التحقق من المستخدمين التقنيات التالية :بطاقات الهوية العادية، كلمات السر، الشهادات الرقمية، البطاقات الذكية المستخدمة للتعريف، التوقيع الالكتروني، وسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي مثل بصمة اليد، بصمة العين ،الصوت .

-**التوقيع الالكتروني**: عرف التوقيع الالكتروني بانه بيانات في شكل الكتروني مدرجة في رسالة بيانات او مضافة اليها او مرتبطة بها منطقيا، و يجوز ان تستخدم لتعيين هوية الموقع بالنسبة الى رسالة البيانات و بيان موافقة الموقع على المعلومات الواردة في رسالة البيانات .اي ان التوقيع الالكتروني يتمثل في حروف و ارقام و اشارات مجموعة في ملف رقمي صغير يساعد على تمييز هوية الموقع وشخصيته دون غيره وبانه هو من قام بإجراء المعاملة و تنفيذها (بوعقل وآخرون، 2016، ص 384).

-تشفير البيانات: التشفير هو عملية دمج المعلومات في شفرة سرية غير مفهومة ثم فك هذه الشفرة بعد وصولها الى وحدة خدمة الويب الامنة ، أي ان التشفير هو استبدال مستند او رسالة باستخدام برنامج معين، و لهذا تنطوي عملية التشفير على تحويل النصوص البسيطة الى رموز (حروف، ارقام، اشارات) قبل ارسالها الى مستقبلها شريطة ان يكون لهذا الاخير القدرة على حل الشفرة و تحويل الرسالة الى صيغتها الاصلية باستخدام مفتاح التشفير (بوعقل وآخرون، 2016، ص 383).

-الشهادات الرقمية: تصدر الشهادات الرقمية عن الجهات التي تعرف بجهة أو سلطة المصادقة الموثوق بها التي توقع عليها، وتستخدم هذه الشهادات للتحقق من موثوقية المفاتيح العامة التي أصدرت.

تعريف الشهادة الرقمية: الشهادة الرقمية هي شهادة تصدرها جهة وسيطة، أو جهة ثالثة ما بين طرفين متعاملين إلكترونيا، وفي عقود التّجارة الالكترونية عبر الانترنيت فإن الجهة الوسيطة تصدر شهادة رقمية أو شهادة مصادقة، تفيد فيها بصحة التوقيع الالكتروني لأحد المتعاقدين، فضلا على البيانات الأخرى المسموح للشهادة أن تشملها، حتى يطمئن الطرف الآخر لصحة البيانات والتعاقدات، ويصدر توقيعه ومن ثم يصبح العقد الالكتروني موثوقا (العاني، 2007، ص 130).

-**مضادات الفيروسات**: وهي مجموعة من البرامج التي تتصدى للفيروسات الداخلة إلى الجهاز وتتفاوت مضادات، من حيث القوة والفاعلية إلا انه يمكن لصناع الفيروسات وناشريها تجاوز مفعولها في كثير من الأحيان (الحمادي، 2010، ص ص 26، 27).

-الجدران النارية: الجدار الناري أو كما يعرف أيضا حائط المنع عبارة عن نظام الكتروني حمائي يعمل بمثابة حاجز ما بين الشبكة الداخلية للمؤسسة وشبكة الانترنيت، ويقوم بترشيح عملية النفاذ ويقننها في حال الدخول إلى مقر معلومات المؤسسة أو الخروج منها، وفقا لقواعد ومبادئ محكمة تحددها المؤسسة صاحبة الشبكة الالكترونية، وهو بذلك يوفر سياسات أمنية للمتعاملين (العاني، 2007، ص134).

قد انتقلت وسائل حماية الشبكات من مستويات الحماية الفردية أو ذات الاتجاه الفردي، التي تقوم على وضع وسائل الحماية ومنها الجدران النارية في المنطقة التي تفصل الشبكة الخاصة عن الموجهات التي تنقل الاتصال إلى الشبكة العالمية (الإنترنت) ، إلى مستويات الأمن المتعددة والتي تقوم على فكرة توفير خطوط إضافية من الدفاع بالنسبة لنوع معين من المعلومات أو نظم المعلومات داخل الشبكة الخاصة ، وتعتمد وسائل الأمن متعددة الاتجاهات والأغراض آليات مختلفة لتوفير الأمن الشامل.