دولة ليبيا
وزارة التعليم
مركز المناهج التعليمية والبحوث التربوية

تقنية المعلومات

للسنة الثالثة بمرحلة التعليم الثانوي
القسم العلمي

الدرس الاول

المدرسة الليبية بفرنسا ـ تور

العام الدراسي:
1441 / 1442 هـ . 2020 / 2021 م.

الفصل الأول:

1 Security of data and information

أمنية البيانات والمعلومات

الانتشار الواسع لتقنية المعلومات ساهم في تضخم حجم المعلومات الرقمية المتبادلة بين المؤسسات والأفراد عبر شبكات الاتصالات بأنواعها. هذا الوضع أوجد فرصاً كبيرة لاختراق البيانات والمعلومات المتدفقة عبر شبكات الاتصال من قبل أشخاص غير مخولين بالاطلاع على البيانات المرسلة، ومن تم إمكانية تخريبها أو استغلالها بصورة غير مشروعة مثل حالات التجسس بين الشركات المتنافسة، هذا بالإضافة إلى التأثيرات السلبية للأعطال الفنية في أثناء سريان البيانات أو حدوث الكوارث بأنواعها التي تسهم في فقدان المعلومات، ونظراً لبروز نوع جديد من الجرائم المتمثلة في جرائم الحاسوب، صار أمن المعلومات يشكل هاجساً كبيراً للدول والمؤسسات وكذلك الأفراد.

1.1 جرائم الحاسوب

جرائم الحاسوب هي الجرائم التي يكون الحاسوب وسيلة في تنفيذها، فمع الانتشار الواسع لاستخدامات الحاسوب في أغراض شتى، زادت فرص الاستغلال السيىء لتقنيات الاتصالات والمعلوماتية، وهناك العديد من الممارسات التي صارت تُعد جرائم يعاقب عليها القانون مثل:

- نشر المعلومات المخلة بالآداب.
- سرقة وقت الحاسوب.
- التشهير الإلكتروني.
- الاصطياد الإلكتروني.
- قرصنة المعلومات.

1.1.1 نشر المعلومات المخلة بالآداب

لقد راج مؤخراً استغلال النظم المعلوماتية في نشر وترويج المعلومات المخلة للآداب، فالشعوب لها عادات وتقاليد لاتسمح باستعمال أو نشر أي معلومة نصية أو مصورة من شأنها إثارة الغرائز والشهوات البشرية، وينتشر في فضاء الانترنت كم هائل من المواقع التجارية التي تروج للإباحية والاتجار بها بين الشباب والقاصرين، وبعض الدول لا تضع قيوداً قانونية على نشر واستغلال المواد الإباحية ويقتصر الحظر على المعلومات الإباحية ذات العلاقة باستغلال الأطفال في هذا الشأن.

2.1.1 سرقة وقت الحاسوب

تتمثل هذه الجريمة في أن يقوم شخص باستخدام الحاسوب في مهام غير المنصوص عليها ضمن اختصاصه الوظيفي، وهو غالبا ما يتم دون الحصول على تصريح بذلك من صاحب العمل، فالشخص الذى يقوم باستخدام الحاسوب في مصالحه الشخصية يعتبر قد انتفع بالجهاز دون أن يدفع مقابلاً ماديّاً لذلك الاستغلال، وهو ما تعتبره تشريعات بعض الدول جريمة يعاقب عليها القانون، وفي المقابل بعض الدول لاتعد ذلك جريمة يعاقب عليها القانون مثل الولايات المتحدة الأمريكية. عادة لايترتب على هذا النوع من الأنشطة أضرار كثيرة مقارنة بالجرائم الأخرى لسوء استخدام الحاسوب، وربما هذا ما جعل اعتبار سرقة وقت الحاسوب جريمة أم لا، مسألة تختلف من بلد لآخر.

3.1.1 التشهير الإلكتروني

جريمة التشهير الإلكتروني تتمثل في نشر معلومات مضللة أو كاذبة عن المؤسسات أو الشخصيات العامة بقصد التشهير، وذلك اعتماداً على وسائل تقنية المعلومات، ويتم التشهير الإلكتروني عبر تصميم مواقع خاصة بالتشهير أو إرسال رسائل بريد إلكتروني إلى الأشخاص والمجموعات البريدية، تحتوي على معلومات أو فضائح مالية أو سلوكية مفبركة، وغالبا ما يسبب التشهير الإلكتروني في أضرار اجتماعية أو اقتصادية للأشخاص المشهر بهم أو الجهات

الرسمية أو التجارية ذات الصلة، وكل من يسهم في استغلال وسائل تقنية المعلومات في إنشاء مواقع التشهير أو تزويد مواقع معينة بمعلومات تؤدي إلى التشهير بالآخرين فهو معرض للمحاسبة الجنائية.

1.1.4 الاصطياد الإلكتروني

يتمثل الاصطياد الإلكتروني في قيام قراصنة المعلومات بانتحال شخصية مؤسسات مالية كالمصارف أو جمعيات المساعدة، يقوم القراصنة باستدراج الضحية عن طريق إرسال بريد الكتروني يُطلب فيه من الضحية تزويد الجاني بمعلومات حساسة، مثل كلمات العبور أو أرقام الحسابات أو البطاقات الشخصية، وذلك لاستخدامها في التبرع بالمال أو الحصول على جائزة أو سداد أجر معاملة وغيرها، عند استجابة الضحية وتزويد الجاني بالمعلومات المطلوبة، يقوم الجناة بالسطو على الحسابات المصرفية للضحية أو استغلال بيانات بطاقة الائتمان في شراء سلع بالتحايل، وتتجاوز أعمال التصيد استخدام البريد الإلكتروني فشملت أيضا الرسائل النصية القصيرة (SMS) وغرف الدردشة.

من نماذج الاصطياد الإلكتروني، تسلّم المستخدم رسالة توهمه فيها بأنه سيربح مبلغا كبيراً أو سيربح جهازا مفيدا له إذا تبرع بمبلغ نقدي في مجالات إنسانية - مثل دعم أبحاث الإيدز، أو مساعدة فقراء إفريقيا - يطلب من الضحية أن يرسل عنوانه البريدي ورقم بطاقة الائتمان لسحب المبلغ المتبرع به، وهنا تكمن الخطورة حيث يقوم الجاني بسرقة أموال الضحية اعتماداً على معلوماته المصرفية، والجناة غالبا يتخفون وراء أسماء لجمعيات شهيرة في مجال العون الإنساني أو جمعيات وهمية.

1.1.5 قرصنة المعلومات

الانتشار الواسع لشبكات الحواسيب ساهم في تعزيز فرص نقل واستقبال البيانات على نطاق واسع، مما وفر فرصاً وطرقاً جديدة لإدارة الأعمال وتقديم الخدمات الإلكترونية بأنواعها، ورغم المزايا الكبيرة للشبكات إلا أنها يمكن أن تشكل ثغرة أمنية يمكن من خلالها سرقة البيانات المرسلة أو اتلافها أو استغلالها من قبل قراصنة المعلومات، وانصب الاهتمام بأمن الشبكات على تعريف مجموعة من الإجراءات،

والقوانين، والتقنيات التي تسهم في تأمين حماية البيانات من الضياع ومن جميع أنواع الاستغلال غير المشروع للبيانات المرسلة.

يمكن تصنيف المخاطر الأمنية لأنظمة الشبكات والاتصالات إلى مخاطر تهدد المباني والأجهزة، نتيجة للأعطال والكوارث الطبيعية التي تسبب أضراراً كبيرة للمباني والمعدات، النوع الثاني من المخاطر يتمثل في المخاطر التي مصدرها برمجيات الشبكات مثل: الخطأ في إصدار التعليمات البرمجية المناسبة، كالحذف غير المتعمد للملفات أو مخاطر الفيروسات، التي يستغلها القراصنة لتعطيل عمل الشبكة، أو خفض أدائها وجعلها بطيئة الأداء، إضافة لذلك تمثل كلمات العبور أحد المخاطر العالية، حيث يمكن تسرب كلمات العبور سواء بالتجسس على المستخدمين أو بالحدس، فبعض المستخدمين يلجؤون إلى استخدام كلمات عبور سهلة التخمين كأن يعتمدوا على بيانات سهلة التذكر مثل: تاريخ الميلاد، أو أسماء المدن التي يعيشون بها، أو النوادي التي يشجعونها، عند تسرب كلمات العبور إلى أشخاص غير مخولين يمكن عن طريقها اختراق بيانات الأشخاص وتزييفها أو إتلافها على أي نحو.