بسم الله الرحمن الرحيم

محاضرة علمية بعنوان :

الجرائم الالكترونية

إعداد وتقديم : أ. نور هرشو

إشراف د. هانيبال يوسف حرب

قدمت هذه المحاضرة على التيليغرام على : الأكاديمية الأمريكية FG-Group

- المقدمة :

أصبحنا في عصر انتشار تكنولوجيا المعلومات أكثر عرضة للوقوع كضحايا للجرائم الإلكترونية ، فانتشار التكنولوجيا ووسائل الاتصال الحديثة يعد سلاح ذو حدين ، يمكن استخدامهم من أجل تسهيل الاتصالات حول العالم ، فهي من أهم وسائل انتقالات الثقافات المختلفة حول العالم من أجل تقريب المسافات بين الدول والحضارات المختلفة ، ولكن يمكن أيضاً استخدامهم في التسبب بأضرار جسيمة لأشخاص بعينهم أو مؤسسات كاملة من أجل خدمة أهداف سياسية او مادية شخصية ، كما احتلّ التقدّم في مجال المعلومات والاتّصالات جانباً كبيراً ومُهمّاً في حياة النّاس وتعاملاتهم ؛ فصار الحاسوب أساس التّعامل بين الأشخاص والشّركات والمؤسسات ، وقد ازداد التوجّه لاستخدام شبكات المعلومات الإلكترونيّة في الفترة الأخيرة بصِفَتها أداة اتّصال دولية في مُختلف مناحي الحياة ، مُوفِّرةً بذلك الكثير من السّرعة والمسافات والجهد على الإنسان .

- مفهوم الجريمة الالكتونية :

الجريمة الإلكترونية هي فعل يتسبب بضرر جسيم للأفراد أو الجماعات والمؤسسات أو إفشاء أسرار أمنية هامة تخص مؤسسات هامة بالدولة أو بيانات وحسابات خاصة بالبنوك والأشخاص ، أو إلحاق الضَّرر النفسيّ والبدنيّ به وتشويه سمعتها من أجل تحقيق مكاسب مادية أو خدمة أهداف سياسية سواءً أكان ذلك بأسلوبٍ مباشر أو غير مباشر ، بالاستعانة بشبكات الاتّصال الحديثة كالإنترنت وما

تتبعها من أدوات كالبريد الإلكتروني وغرف المُحادثة ، والهواتف المحمولة وما تتبعها من أدوات كرسائل الوسائط المُتعدّدة .

تتشابه الجريمة الإلكترونية مع الجريمة العادية في عناصرها من حيث وجود الجاني والضحية وفعل الجريمة ، ولكن تختلف عن الجريمة العادية باختلاف البيئات والوسائل المستخدمة ، فالجريمة الإلكترونية يمكن أن تتم دون وجود الشخص مرتكب الجريمة في مكان الحدث ، كما أن الوسيلة المستخدمة هي التكنولوجيا الحديثة ووسائل الإتصال الحديثة والشبكات المعلوماتية .

تحملُ الجرائم الإلكترونيّة مُسمّياتٍ عدّة ، منها :

- **جرائم الكمبيوتر والإنترنت .**
- **جرائم أصحاب الياقات البيضاء بالإنجليزية white collar crime .**
- **الجرائم السايبيرية بالإنجليزية Cyper crime .**
- **جرائم التقنية العالية بالإنجليزية High Tech Crime .**

- من هو المجرم الالكتروني او كما يُعرف بالمجرم المعلوماتي ؟

المجرم الالكتروني هو الأخطر في " عالم الجريمة " ، خاصة أنه يتميز بقدر من العلم وقدرة على استعمال التقنيات الحديثة ، وبعضهم لديه مهارة فائقة ، ومن ثم يطلق عليهم أصحاب الياقات البيضاء، حيث يرتكبون جرائمهم وهم جالسون في أماكنهم .

و لقد تنوعت الدراسات التي تحدد المجرم ، وشخصيته ومدى جسامة جرمه كأساس لتبرير وتقدير العقوبة ، فهناك سمات مشتركة بين المجرمين الالكترونين ويمكن إجمال تلك السمات فيما يلي :

- مجرم متخصص : له قدرة فائقة في المهارة التقنية ويستغل مداركه ومهاراته في اختراق الشبكات كسر كلمات المرور أو الشفرات ويسبح في عالم الشبكات ليحصل على كل غالٍ وثمين من البيانات والمعلومات الموجودة في أجهزة الحواسب ومن خلال الشبكات .

- مجرم يعود للإجرام : يتميز المجرم المعلوماتي بأنه يعود للجريمة دائمًا فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير

المصرح به مرات ومرات فهو قد لا يحقق جريمة الاختراق بهدف الإيذاء وإنما نتيجة شعوره بقدرته ومهارته في الاختراق .

- مجرم محترف : له من القدرات والمهارات التقنية ما يؤهله لأن يوظف مهاراته في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال .

- مجرم ذكي : حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل و تطوير في الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب .

- صفات المجرم المعلوماتي :

- عادة ما تتراوح أعمار تلك الفئة من المجرمين ما بين 18-45 عامًا .

- المهارة والإلمام الكامل والقدرة الفنية الهائلة في مجال نظم المعلومات فمجرمي تلك الفئة ينتمون إلى طبقة المتعلمين والمثقفين ومن لديهم تخصصية التعامل مع أجهزة الحاسب الآلي والقدرة على اختراق التحصينات والدفاعات التي تعدها شركات البرمجة .

- الثقة الزائدة بالنفس والإحساس بإمكانية ارتكابهم لجرائمهم دون افتضاح أمرهم .

- إلمامه التام بمسرح الجريمة وبأدواته ، وبما يجنبه فجائية المواقف التي قد تؤدي إلى إفشال مخططه وافتضاح أمره .

- أنماط الجناة في الجريمة المعلوماتية :

تتعدد أنماط الجناة في الجريمة المعلوماتية :

هناك الهاكارز " Hackers " أو المتسللون وهم عادةً مجرمون محترفون يستغلون خبراتهم وإمكانياتهم في مجال تقنية المعلومات للتسلل إلى مواقع معينة للحصول على معلومات سرية أو تخريب وإتلاف نظام معين وإلحاق الخسائر به بقصد الانتقام أو الابتزاز .

وهناك الكراكرز " Crackers - المخترقون " سواء كان من الهواة أو المحترفين وعادةً ما يستخدم مجرمو هذا النمط قدراتهم الفنية في اختراق الأنظمة والأجهزة تحقيقاً لأهداف غير شرعية كالحصول على معلومات سرية أو للقيام بأعمال تخريبية .. إلخ .

وهناك العابثون بالشفرات ومؤلفو الفيروسات " Malecions hackers " الخ .

- أدوات الجرائم الإلكترونية :

حتى يتمكن القراصنة (Hackers) من تنفيذ جريمتهم الإلكترونية يستلزم ذلك توفر أدوات لذلك ، ومن أبرزها :

- الاتصال بشبكة الإنترنت وتعتبر أداة رئيسية لتنفيذ الجريمة .

- توفر برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب .

- وسائل التجسس ومنها ربط الكاميرات بخطوط الاتصال الهاتفي .

- البار كود وهي عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شيفرة الرموز .

- طابعات (Printers) .

- هواتف رقمية ونقالة .

- برامج ضارة ومنها Trojan horse إذ تتمثل وظيفته بخداع الضحية وتشجيعه على تشغيله فيلحق الضرر الشامل بالحاسوب والملفات الموجودة عليه .

- أنواع الجرائم الإلكترونية :

- اولا : جرائم تسبب الأذى للأفراد :

ومن خلالها يتم استهداف فئة من الأفراد أو فرد بعينه من أجل الحصول على معلومات هامة تخص حساباته سواء البنكية أو على الإنترنت ، وتتمثل هذه الجرائم في :

• انتحال الشخصية : وفيها يستدرج المجرم الضحية ويستخلص منها المعلومات بطرق غير مباشرة ، ويستهدف فيها معلومات خاصة من أجل الاستفادة منها واستغلالها لتحقيق مكاسب مادية أو التشهير بسمعة أشخاص بعينهم .

• تهديد الأفرا د : يصل المجرم من خلال القرصنة وسرقة المعلومات إلى معلومات شخصية وخاصة جداً بالنسبة للضحية ، ثم يقوم بابتزازه من أجل كسب الأموال وتحريضه للقيام بأفعال غير مشروعة قد يصاب فيها بأذى .

• تشويه السمعة : يقوم المجرم باستخدام المعلومات المسروقة وإضافة بعض المعلومات المغلوطة ، ثم يقوم بارسالها عبر الوسائط الإجتماعية أو عبر البريد الإلكتروني للعديد من الأفراد بغرض تشويه سمعة الضحية وتدميرهم نفسياً .

• المطاردة الإلكترونية : هي الجرائم المُتعلّقة بتعقّب أو مطاردة الأفراد عن طريق الوسائل الإلكترونيّة لغاية تعريضهم للمضايقات الشّخصية أو الإحراج العام أو السّرقة المالية ، وتهديدهم بذلك؛ حيث يجمع مرتكبو هذه الجرائم معلوماتِ الضّحية الشخصية عبر مواقع الشّبكات الاجتماعي وغرف المحادثة وغيرها .

- ثانيا : جرائم تسبب الأذى للمؤسسات :

- اختراق الأنظمة :

• تتسبب الجرائم الإلكترونية بخسائر كبيرة للمؤسسات والشركات المتمثلة في الخسائر المادية والخسائر في النظم ، بحيث يقوم المجرم باختراق أنظمة الشبكات الخاصة بالمؤسسات والشركات والحصول على معلومات قيمة وخاصة بأنظمة الشركات ، ومن ثم يقوم باستخدام المعلومات من أجل خدمة مصالحه الشخصية والتي تتمثل في سرقة الأموال وتدمير أنظمة الشركة الداعمة في عملية الإدارة مما يسبب خسائر جسيمة للشركة أو المؤسسة .

• كما يمكن سرقة المعلومات الخاصة بموظفين المؤسسات والشركات وتحريضهم وابتزازهم من أجل تدمير الأنظمة الداخلية للمؤسسات ، وتثبيت أجهزة التجسس على الحسابات والأنظمة والسعي لاختراقها والسيطرة عليها لتحقيق مكاسب مادية وسياسية .

• وتؤثر الجرائم الالكترونية الخاصة باختراق الشبكات والحسابات والأنظمة بشكل سلبي على حالة الاقتصاد في البلاد ، كما تتسبب في العديد من مشاكل تتعلق بتهديد الأمن القومي للبلاد إذا ما لم يتم السيطرة عليهم ومكافحاتهم بكل جدارة .

• تمثل نسبة الجرائم الإلكترونية والجرائم المعلوماتية حول العالم 170% ، وتزداد النسبة يوم بعد يوم مما يجعلنا جميعاً في خطر محدق بسبب الانتهاكات واختراق الأنظمة والحسابات .

• اختراق المواقع الإلكترونية والسيطرة عليها ، ومن ثم توظيفها لتخدم مصالح كيانات خطيرة تهدف لزعزعة الأمن بالبلاد والسيطرة على عقول الشباب وتحريضهم للقيام بأعمال غير مشروعة .

- تدمير النظم :

• يكون هذا النوع من التدمير باستخدام الطرق الشائعة وهي الفيروسات الإلكترونية والتي تنتشر في النظام وتسبب الفوضى والتدمير .

• او تدمير الخادم الرئيسي الذي يستخدمه جميع من بالمؤسسة من أجل تسهيل الأعمال ، ويتم ذلك من خلال اختراق حسابات الموظفين بالمؤسسة الخاصة بالشبكة المعلوماتية للمؤسسة والدخول على الحسابات جميعاً في نفس ذات الوقت ، ويتسبب ذلك في عطل تام للخادم مما يؤدي إلى تدميره وبالتالي تعطل الأعمال بالشركات والمؤسسات .

- ثالثا : جرائم الأموال :

• الاستيلاء على حسابات البنوك :

وهي اختراق الحسابات البنكية والحسابات المتعلقة بمؤسسات الدولة وغيرها من المؤسسات الخاصة، كما يتم أيضاً سرقة البطاقات الائتمانية ، ومن ثم الاستيلاء عليها وسرقة ما بها من أموال .

• انتهاك حقوق الملكية الفكرية والأدبية :

وهي صناعة نسخ غير أصلية من البرامج وملفات الملتيميديا ونشرها من خلال الإنترنت، ويتسبب ذلك في خسائر فادحة في مؤسسات صناعة البرامج والصوتيات .

- رابعا : الجرائم التي تستهدف أمن الدولة :

• برامج التجسس :

تنتشر العديد من برامج التجسس والمستخدمة في أسباب سياسية والتي تهدد أمن وسلامة الدولة ، ويقوم المجرم بزرع برنامج التجسس داخل الأنظمة الإلكترونية للمؤسسات ، فيقوم أعداء الوطن بهدم أنظمة النظام والاطلاع على مخططات عسكرية تخص أمن البلاد ، لذلك فهي تعتبر من أخطر الجرائم المعلوماتية .

• استخدام المنظمات الإرهابية لأسلوب التضليل :

ويعتمد الإرهابيون على استخدام وسائل الاتصال الحديثة وشبكة الإنترنت من أجل بث ونشر معلومات مغلوطة، والتي قد تؤدي لزعزعة الاستقرار في البلاد وإحداث الفوضى من أجل تنفيذ مصالح سياسية ومخططات إرهابية ، وتضليل عقول الشباب من أجل الانتفاع بمصالح شخصية .

- مخاطر الجرائم الالكترونية و منها :

1- المساس بالاقتصاد والأمن الوطني وتهديده .

2- التّشهير ببعض الأفراد ونشر الأخبار الكاذبة والإشاعات .

3- صعوبة معرفة مرتكب الجريمة، إلّا باستخدام وسائل أمنيّة ذات تقنية عالية .

4- سهولة الوقوع فيها؛ بسبب غياب الرّقابة الأمنية .

5- سهولة إخفاء وطمس مَعالم الجريمة وآثارها والدّلائل التي تُدلّ على مرتكبها .

6- هي أقلّ جهداً وعُنفاً جسديّاً من الجرائم التّقليدية .

7- جريمةٌ لا تتقيّد بمكانٍ أو زمانٍ مُحدّدين .

- أهداف الجرائم الإلكترونية :

تهدفُ الجرائم الإلكترونية لجملةٍ من الغايات ، منها :

1- تحصيل مكسبٍ سياسيّ أو ماديّ أو معنويّ غير مشروع عبر تقنيات المعلومات كعمليّات تزوير بطاقات الائتمان ، والاختراق .

2- تحصيلُ معلوماتٍ ووثائق سريّة للمؤسسات والجهات الحكوميّة والمصرفية والشخصية لابتزازهم من خلالها .

3- الوصول لمعلوماتٍ غير مُخوّل للعامّة الاطلاع عليها بشكلٍ غير مشروع ، وسرقتها أو حذفها أو تعطيلها أو التعديل عليها لتحقيق مصالح مرتكب الجريمة .

مكافحة الجرائم الإلكترونية تسعى الدّول والحكومات بشكلٍ جديّ للحدّ من الجَرائم الإلكترونيّة وآثارها عبر طُرقٍ كثيرة منها :

1- فرضُ سياساتٍ دوليّة وعقوباتٍ كبيرة على مُرتكبي هذه الجَرائم .

2- تفعيل أحدث التقنيات والوسائل للكشفِ عن هويّة مُرتكبي الجرائم .

3- نشر التّوعية في المُجتمعات حول الجرائم الإلكترونية و مَخاطرها ، وتَعريف الأفراد بكيفيّة الحِفاظ على معلوماتهم وخصوصيّاتهم ؛ كحساباتهم البنكية وبطاقاتهم الائتمانية .

4- إنشاء خطوط هاتفيّة ومؤسسات مُعيّنة تابعة للدّولة للإبلاغ عن الحالات التي تتعرّض لمثل هذا النّوع من الجرائم .

5- توجيه التّشريعات والقوانين وتحديثها بما يَتماشى مع التّطورات التكنولوجية ، لفرض قَوانين جديدة فيما يستجدّ من هذه الجرائم .

6- تطوير طرق ووسائل لتتبع مرتكبي الجرائم الإلكترونية بشكل دقيق والإمساك بهم .

7- عدم ترك جهاز الحاسوب مفتوحاً .