**محاضرة 1: تكنولوجيا الاتصال وارتكاب الجرائم في عصر المعلومات:**

1. **تعريف الجريمة الالكترونية:**

يقصد بالجرائم المتصلة بتكنولوجيا الاتصال والإعلام أي جريمة ترتكب ضد /أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي آلية ذات صلة بتكنولوجيات الاتصال والإعلام. ويمكن إعتبار هذا النوع من الجرائم أكثر تعقيدا مقارنة بالجريمة التقليدية، بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة آثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود أو لمساسها بالنظام والأمن العموميين، تتطلب استعمال وسائل تحري خاصة أو خبرة فنية متخصصة أو اللجوء إلى تعاون قضائي دولي.

1. **أنواع الجريمة الالكترونية:** تندرج تحت نمطين مختلفين من الجرائم:

النمط الأول: قد تكون عبارة عن تصرف غير قانوني، يرتكب ضد أجهزة الكمبيوتر أو الاتصالات،

مثل سرقة الأقراص الصلبة، سرقة الكابلات أو سرقة الوقت من الكابلات الهاتفية، أو سرقة المعلومات. ويكون باستخدام الفيروسات

النمط الثاني: قد تكون عبارة عن استخدام أجهزة الكمبيوتر والاتصالات لارتكاب تصرف غير قانوني، مثل: جرائم تعمد الأذى والتدمير: بحيث يسيء المجرم استخدام الكمبيوتر بغرض الأذى وليس الكسب المالي مثلا..

1. **الأشكال المختلفة للجريمة الالكترونية:**

### هجمات البرمجيات الخبيثة:

هجوم البرمجيات الخبيثة هو إصابة نظام الكمبيوتر أو الشبكة بفيروس كمبيوتر أو أي نوع آخر من البرمجيات الخبيثة، ويمكن لمجرمي الإنترنت استخدام الكمبيوتر الذي اخترقوه بالمبرجيات الخبيثة لعدة أغراض، من بينها سرقة البيانات السرية واستخدام الكمبيوتر لتنفيذ أعمال إجرامية أخرى أو التسبب في إتلاف البيانات.

من الأمثلة الشهيرة على هجوم برمجية الفدية الخبيثة WannaCry، وهي جريمة إلكترونية عالمية حدثت في مايو 2017. كان WannaCry نوعًا من برامج الفدية، وهي برامج خبيثة تُستخدم في الابتزاز وأخذ الأموال عن طريق الاحتفاظ ببيانات الضحية أو جهازه وعدم إرجاعهما إلا مقابل فدية. استهدف برنامج الفدية هذا ثغرة أمنية في أجهزة الكمبيوتر التي تعمل بنظام التشغيل Microsoft Windows.

عندما وقع هجوم برنامج الفدية WannaCry، تأثر 230 ألف جهاز كمبيوتر في 150 دولة به! تعذر على المستخدمين الوصول إلى ملفاتهم، وتلقى كل مستخدم رسالة تطلب منه دفع فدية بعملة [البتكوين](https://me.kaspersky.com/resource-center/definitions/what-is-bitcoin) من أجل استعادة الوصول إلى ملفاته.

وعلى الصعيد العالمي، سببت جريمة WannaCry الإلكترونية خسائر مالية قُدّرت بما يصل إلى 4 مليار دولار. لا يزال هذا الهجوم -حتى يومنا هذا- مشهورًا بسبب انتشاره وتأثيره.

* **الجرائم المتعلقة بالإباحية الجنسية والتحرش الجنسي: خصوصا ضد الأطفال**

وتتم جرائم الإباحية الجنسية بتبادل الصور الفوتوغرافية المخلة بحرية تامة عن طريق الشبكة، وإذا كان الغرب يتغاضى عن هذه الممارسات ضد الكبار بدعوى الحق في الخصوصية إلا أن ذلك لا ينطبق على الأطفال بعد أن انتشر استهداف الفئات الصغرى بشكل كبير جدا

* **الرسائل غير مرغوبة في البريد الالكتروني أو عبر مواقع التواصل الاجتماعي:(التصيد الاحتيالي)**

لاشك أن البريد الالكتروني يتمتع بعديد من المزايا، لكنه لا يخلو من الإزعاج، فالرسائل المزعجة في البريد الالكتروني كالعروض الملحة والنصب على العملاء والمشتركين، تعتبر من عيوب التواصل عبر البريد الالكتروني. وقد أصدرت لجنة التجارة الفيدرالية الأمريكية قائمة تضم أسوء 12 موضوعا من هذا النوع، بناء على 250 ألف رسالة، تسبب إزعاجا ومضايقة للمشتركين في الانترنت وصفوها بأنها تتميز بالصفاقة والإلحاح وتتحدث عن أمور لا تهمهم. والبريد الالكتروني المزعج هو مشكلة لكل من يملك جهاز كمبيوتر أو هاتف ذكي فهذه الرسائل تبطئ من نظام البريد الالكتروني.

وعن أهم الموضوعات في "القائمة القذرة" نجد رسائل تتحدث عن:

-فرص تجارية، كوعود بزيادة المداخيل من خلال استثمار صغير لا يتطلب الكثير من المال،

-الخطابات التي تزعم أن بامكان الفرد أن يكسب 50 دولارا في ظرف 90 يوما،

-عرض بعض الفرص مجانا كالفوز بجهاز كمبيوتر مجانا،

-أجهزة لالتقاط أجهزة التلفزيون المشفرة

حملة التصيد الاحتيالي يتم فيها إرسال رسائل بريد إلكتروني عشوائية أو غيرها من أشكال التواصل بهدف خداع المستلمين لفعل بشيء يخترق أمنهم. قد تحتوي رسائل حملات التصيد الاحتيالي على مرفقات بها برمجيات خبيثة أو روابط لمواقع ضارة، أو قد تطلب من مستلمها الرد بمعلومات سرية.

حدث أحد الأمثلة الشهيرة لعمليات التصيد الاحتيالي أثناء كأس العالم 2018. وفقًا لتقرير حول "الاحتيال في كأس العالم 2018"، تضمنت هذه العملية رسائل بريد إلكتروني تم إرسالها إلى مشجعي كرة القدم عن كأس العالم 2018، حاولت رسائل البريد الإلكتروني العشوائية هذه إغراء المشجعين برحلات مجانية مزيّفة إلى موسكو حيث تمت استضافة كأس العالم، وتمت سرقة البيانات الشخصية الخاصة بالأشخاص الذين فتحوا رسائل البريد الإلكتروني هذه والضغط على الروابط الواردة فيها.

هناك نوع آخر من حملات التصيد الاحتيالي وهي حملات التصيد الاحتيالي المستهدفة التي تحاول خداع أفراد معيّنين لتعريض أمن المؤسسة التي يعملون فيها للخطر.

* **التجسس الالكتروني وتهديد الأمن العام:**

أرادت هيئة الأركان الأمريكية التحقق من مدى مناعة تجهيزاتها، فأوكلت إلى فريق من القراصنة العسكريين مهمة اختراق شبكة البنتاغون، ومحاولة النفاذ إلى قواعد معلوماتها عبر شبكة الانترنت والنتيجة أن هذا الفريق استطاع النفاذ إلى 80 بالمئة من مضمون أجهزة الكمبيوتر الرئيسية، فالتجسس الالكتروني عملية معقدة ومفتوحة على كل الخيارات ويمكن أن يأتي الهجوم من أي جهة سواء منظمة أو فردية سواء داخل الوطن أو خارجه. وما يقال على التجسس في المجال العسكري يقال أيضا في مجال التجسس الصناعي والتجاري والبحث العلمي، ولا يقل الأمر خطورة لأنه تهديد للأمن العام عموما.

* **التزييف والتزوير باستخدام الكمبيوتر:**

نظرا للتطور التقني الهائل في أجهزة الكمبيوتر والطابعات وأجهزة المسح الضوئي دخلت التكنولوجيا التزييف والتزوير من باب واسع، وذلك بنقل توقيع شخص ما أو ختم على عقود مزيفة (بيع أرض شقة، صك بريدي، وصل أمانة..الخ). وكذا استخدام التزوير والتزييف في مجال العملات والتي تكاد تتطابق مع العملة الحقيقية ولا يمكن كشفها إلا من خلال خبرة فنية ومهارة عالية.

* **الارهاب الالكتروني:**

لا يوجد تعريف متفق عليه بخصوص الإرهاب وبالتالي الإرهاب الالكتروني، إذ يعرف **الإرهاب** على أنه : "الأفعال التي من طبيعتها أن تثير قلقا لدى شخص ما من شعور بالتهديد أو هي الأعمال التي تؤدي إلى التخويف والرعب بأي قدر وبأي وسيلة"

لكن من أبرز التعريفات ما جاء به باري كولين barry colin الذي قال أن تعريف **الإرهاب الالكتروني** صعب لكنه تبنى التعريف التالي: "هجمات الكترونية غرضها تهديد الحكومات أو العدوان عليها، سعيا لتحقيق أهداف سياسية أو دينية أو أيديولوجية، والهجمة يكون أثرها مدمرا وتخريبي مكافئ للأفعال المادية للإرهاب."

## تأثيرات الجرائم الإلكترونية: للجريمة الالكترونية تأثيرات وأبعاد متعددة على مستوى المعاملات المالية التجارية، والأمن القومي للدول، وكذا تأثيرات نفسية وجسدية على الأشخاص..الخ

ووفقًا ل[تقرير حالة مرونة الأمن السيبراني لعام 2021 من شركة Accenture](https://www.accenture.com/content/dam/accenture/final/a-com-migration/custom/us-en/invest-cyber-resilience/pdf/Accenture-State-Of-Cybersecurity-2021.pdf) فإن سرقة الهوية في ازدياد عام دون توقف، حيث زادت الهجمات الأمنية بنسبة 31٪ من 2020 إلى 2021، وزاد عدد الهجمات لكل شركة من 206 إلى 270 على أساس سنوي. وتؤثر الهجمات ضد الشركات على الأفراد أيضًا لأن العديد منهم يخزنون بيانات حساسة ومعلومات شخصية من العملاء. حيث يمكن لهجوم واحد -سواء كان خرقًا للبيانات أو برمجيات خبيثة أو هجوم حرمان من الخدمات- أن يكلف الشركات من جميع الأحجام ما متوسطه 200 ألف دولار، وتخرج العديد من الشركات المتضررة من العمل في غضون ستة أشهر من الهجوم.

نشرت مؤسسة Javelin Strategy & Research [دراسة عن انتحال الهوية في عام 2021](https://www.javelinstrategy.com/press-release/total-identity-fraud-losses-soar-56-billion-2020) وجدت فيها أن خسائر الاحتيال في الهوية لذلك العام بلغت 56 مليار دولار.

بالنسبة للأفراد والشركات، يمكن أن يكون تأثير الجريمة الإلكترونية عميقًا: من خلال الضرر المالي في المقام الأول، ولكن أيضًا فقدان الثقة والإضرار بالسمعة.