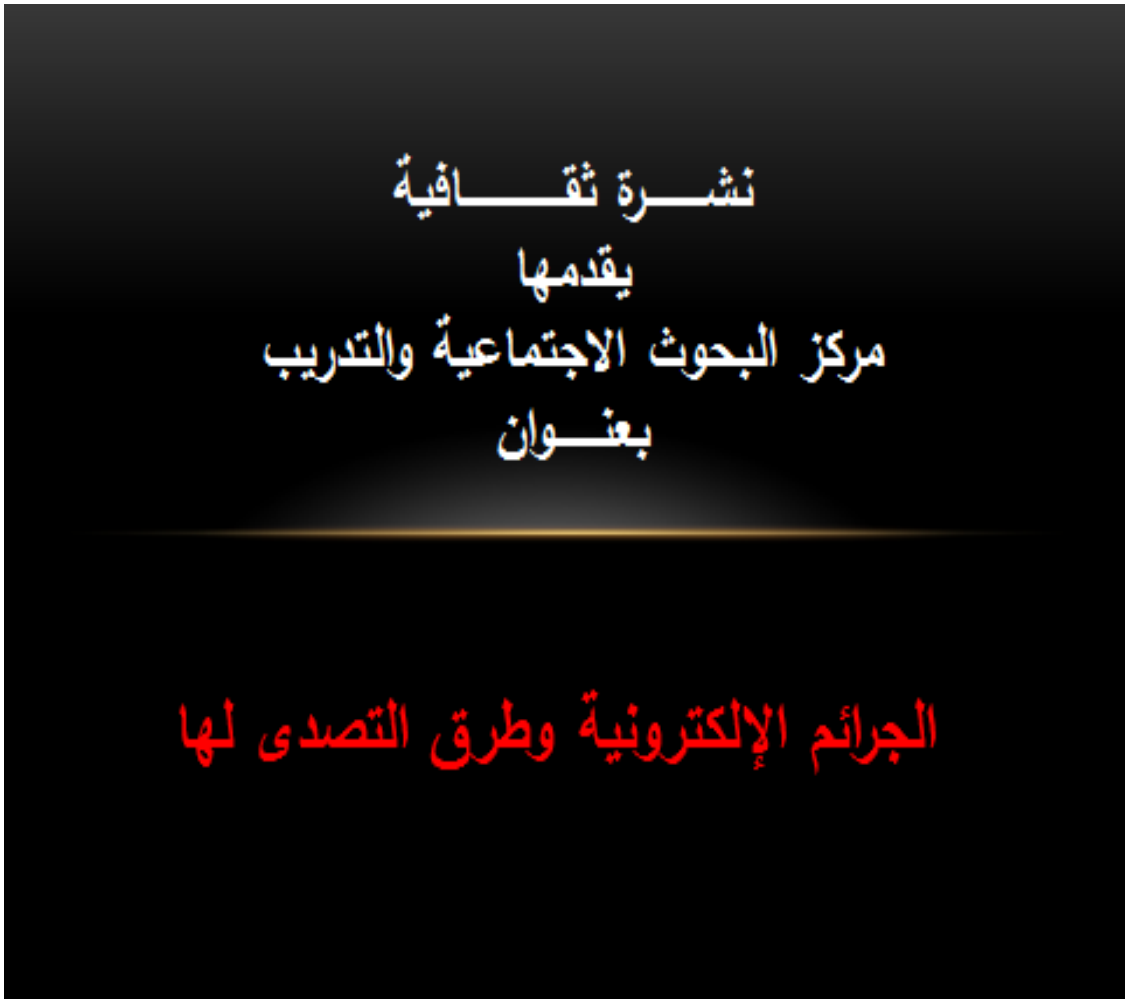
جامعة أسيوط Assiut University	مركز البحوث الاجتماعية والتدريب Social Research & Training Center	كلية الخدمة الإجتماعية Faculty of Social Work



المدير الإدارى للمركز	مدير المركز	رئيس مجلس الإدارة وعميد الكلية
أ/ إيمان عبد رب النبى	أ.م.د/ جابر فوزى محمد	أ.د/ سعودى محمد حسن

الجرائم الإلكترونية

(جرائم الإنترنت- جرائم التقنية العالية- الجريمة السيبرانية)

هى نشاط إجرامى يستهدف جهاز كمبيوتر أو شبكة كمبيوتر أو جهاز متصلا بالشبكة وتحاول استخدامهم. تقع معظم الجرائم الالكترونيةعلى أيدى لصوص أومخترقين يودون كسب الأموال وأحيانا نادره أخرى يكون الهدف من وراء الجرائم الإلكترونية هو إلحاق الضرر بأجهزة الكمبيوتر لاسباب غير الربح وقد تكون هذه الأسباب سياسية أو شخصية

يمكن أن تقع الجرائم الإلكترونية على يد أفراد أو منظمات بعض هؤلاء المجرمين الإلكترونيين منظمين ويستخدمهم التقنيات المتقدمة وهم ذوى مهارات فنية عالية وبعضهم مجرد مخترقين مبتدئين .

ماهى أنواع الجرائم الإلكترونية ؟

- الاحتيال عبر البريد الإلكترونى والانترنت
- تزوير الهوية (حيث تتم سرقة المعلومات الشخصية واستخدامها)
- سرقة البيانات المالية أو بيانات الدفع بالبطاقة
- سرقة بيانات الشركة وبيعها

- الابتزاز الالكترونى (طلب المال لمنع هجوم مهدد
- هجمات برامج الفدية (نوع من الابتزاز الالكترونى)
- السرقة المشفره (حيث يقوم المتسللون بتعدين العملات المشفره باستخدام موارد لا يملكونها)
- التجسس الالكترونى (حيث يتمكن المتسللون من الوصول الى البيانات الحكومة أو الشركة)
- التدخل فى الأنظمة بطريقة تعرض الشبكة للخطر
- انتهاك حقوق النشر
- المقامره غير المشروعة
- بيع السلع غير المشروعة عبر الإنترنت
- طلب مواد إباحية تستغل الأطفال أو انتاجها أو امتلاكها

تشمل الجرائم الإلكترونية الأمرين التاليين أو أحدهما على الأقل:

- نشاط إجرامى يستهدف أجهزة الكمبيوتر باستخدام الفيروسات وانواع أخرى من البرمجيات الخبيثة
- نشاط اجرامى يستخدم أجهزة الكمبيوتر لارتكاب جرائم أخرى.

مرتكبو الجرائم الإلكترونية الذين يستهدفون أجهزة الكمبيوتر قد يصيبونها ببرمجية خبيثة لإتلاف الأجهزة أو إيقافها عن العمل وقد يستخدمون تلك البرمجية الخبيثة فى حذف البيانات أو سرقتها يمكن كذلك ان يعمل مرتكبو الجرائم الالكتونية على منع المستخدمين من استخدام موقع الكتونى أو شبكة او منع شركة تقدم خدمة برمجية من الوصول الى عملائها وهذا الاسلوب معروف باسم هجوم الحرمان من الخدمات (Dos)

قد تشمل الجريمة الالكترونية التى تستخدم أجهزة الكمبيوتر لارتكاب جرائم اخرى استخدام اجهزة الكمبيوتر او الشبكات لارتكاب جرائم اخرى استخدام الكمبيوتر أو الشبكات لنشر البرامج الضارة أو المعلومات والصور غير المشروعة

https://me.kaspersky.com/resource-center/threats/what-is-cybercrime

من هم مرتكبى الجرائم الالكترونية؟

هاكر أو كراكر (Hacker or Cracker): هواة او خبراء بالكمبيوتر يستخدمون الكمبيوتر بشكل غير قانونى للترفيه ويكتشف بفضول أجهزة كمبيوتر الاخرين. الكراكرز أو الهاكرز المحترفون هم عصابات متخصصة فى جرائم الانترنت.

https://www.law-house.net/

أنواع الجرائم الإلكترونية

- الجرائم ضد الأفراد: تسمى بجرائم الانترنت الشخصية تتمثل فى سرقةالهوية ومنها البريد الالكترونى او سرقة الاشتراك فى موقع شبكة الانترنت وانتحال شخصية اخرى بطريقة

غير شرعية عبر الانترنت بهدف الاستفادة من تلك الشخصية او لاخفاء هوية المجرم لتسهيل عملية الاجرام.

- الجرائم ضد الملكية : تتمثل فى نقل البرمجيات الضارة المضمنه فى بعض البرامج التطبيقية او الخدمية وغيرها بهدف تدمير الاجهزة او البرامج المملوكة للشركات او الاجهزة الحكومية او البنوك او حتى الممتلكات الشخصية
- الجرائم ضد الحكومات: مهاجمة المواقع الرسمية وانظمة الشبكات الحكومية والتى تستخدم تلك التطبيقات على المستوى المحلى والدولى كالهجمات الارهابية على شبكة الانترنت وهى تتركز على تدمير البنية التحتية ومهاجمة شبكات الكمبيوتر وغالبا ما يكون هدفها سياسى.

خصائص وسمات الجرائم الإلكترونية:

- سهولة ارتكاب الجريمة بعيدا عن الرقابة الامنية فهى ترتكب عبر جهاز الكمبيوتر مما يسهل تنفيذها من قبل المجرم دون ان يراه احد او تكتشفه
- صعوبة التحكم فى تحديد حجم الضرر الناجم عنه قياسا بالجرائم الالكترونية تتنوع بتنوع مرتكبيها واهدافهم وبالتالى لا يمكن تحديد حجم الاضرار الناجمة عنها
- مرتكبيها من بين الفئات متعددة تجعل من التنبؤ بالمشتبه بهم امرا صعبا اعمارهم تتراوح غالبا ما بين ١٨ : ٤٨ سنه
- تنطوى على سلوكيات غير مألوفة عن المجتمع
- اعتبارها اقل عنفا فى التنفيذ فهى تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية لان المجرم عن تنفيذه لمثل هذه الجرائم لا يبذل جهدا فهى تطبق على الاجهزة الالكترونية وبعيدا عن اى رقابة مما يسهل القيام بها
- جريمة عابره للحدود لا تعترف بعنصر المكان والزمان فهى تتميز بالتباعد الجغرافى واختلاف التوقيتات بين الجانى والمجنى عليه، فالسهولة فى حركة المعلومات عبر الانظمة التقنية الحديثة جعل بالامكان ارتكابها عن طريق حاسوب موجود فى دولة معينة بينما يتحقق الفعل الاجرامى فى دولة اخرى.

- سهولة إتلاف الأدلة من قبل الجناة فالمعلومات المتداولة عبر الانترنت على هيئة رموز مخزنة على وسائط تخزين ممغنطة وهى عباره عن نبضات الكترونية غير مرئية مما يجعل امر طمس ومحو الدليل أمر سهل.

اهداف الجرائم الالكترونية :

- التمكين من الوصول الى المعلومات بشكل غير قانونى كسرقة المعلومات او حذفها والاطلاع عليها.
- التمكن من الوصول بواسطة الشبكة العنكبوتية الى الاجهزة الخادمة الموفرة للمعلومات وتعطيلها او التلاعب بمعطياتها
- الحصول على المعلومات السية للجهات المستخدمة للتكنولوجيا كالبنوك والمؤسسات والحكومات والافراد والقيام بتهديدهم اما لتحقيق هدف مادى او سياسى.
- الكسب المادى او المعنوى او السياسى غير المشروع مثل تزوير بطاقات الائتمان وسرقة الحسابات المصرفية .

أدوات الجريمة الالكترونية:

- برامج نسخ المعلومات المخزنة فى اجهزة الحاسب الآلى
- الانترنت كوسيط لتنفيذ الجريمة
- خطوط الاتصال الهاتفى التى تستخدم لربط الكاميرات ووسائل التجسس
- أدوات مسح الترميز الرقمى (الباركود)
- الطابعات
- أجهزة الهاتف النقال والهواتف الرقمية الثابتة
- برامج مدمره: مثل برنامج حصان طروادة Trojan horseبحيث يقوم بخداع المستخدم لتشغيله حيث يظهر على شكل برنامج مفيد وآمن ويؤدى تشغيله الى تعطيل الحاسب المصاب وبرنامج الدودة الذى يشبه الفيروس ولكنه يصيب أجهزة الحاسب دون الحاجة الى اى فعل وغالبا يحدث عندما ترسل بريد إلكترونى الى كل الاسماء الموجودة فى سجل الاسماء.

دوافع الجرائم الالكترونية

- دافع مادية ويتمثل فى تحقيق الكسب المادى تعد الرغبة فى تحقيق الثراء من العوامل الرئيسية لارتكاب الجريمة عبر الانترنت نظرا للربح الكبير وغالبا ما يكون الدافع لارتكاب هذه الجريمة هو وقوع الجانى فى مشاكل مادية مثال على ذلك تحويل حساب مادلى الى حسابه
- دوافع شخصية:تتمثل فى:

- **الرغبة فى التعلم:** يكرس مرتكبو هذه الجريمة وقته فى تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية الحاسوبية.
- **دوافع ذهنية أو نمطية:** غالبا ما يكون الدافع لدى مرتكب الجرائم عبر الانترنت هو الرغبة فى اثبات الذات وتحقيق الانتصار على تقنية الانظمة المعلوماتية دون ان يكون لهم نوايا اثمة.
- **دافع الانتقام:** تعد من أخطر الدوافع التى يمكن ات تنفع شخص يملك معلومات كبيره عن المؤسسة أو شركة يعمل بها تجعله يقدم على ارتكاب جريمته.
- دوافع التسلية: هى جريمة ترتكب من اجل التسلية لا يقصد من ورائها احداث جرائم

- دافع سياسى يتم غالبا فى المواقع السياسية المعادية للحكومة ويتمثل فى تلفيق الاخباروالمعلومات ولو زورا او حتى الاستناد الى جزء بسيط جدا من الحقيقة ومن ثم نسخ الأخبار الملفقة حولها تعد الدوافع السياسية من ابرز المحاولات الدولية لاختراق شبكات حكومية فى مختلف دول العالم

https://ar.wikipedia.org/wiki/

مخاطر الجرائم الإلكترونية على المجتمع

تعد هذه الجرائم الإلكترونية مرضا يسبب الفتك بالمجتمعات والعلاقات الانسانية ويؤخر من عجلة التقدم والتنمية التى يعيشها العالم مؤخرا

أول هذه الآثار هى تدمير قيم الأسرة من خلال استغلال أفرادها والاساءة له وصورته التى تؤثر أسرته لمدة طويلة.

بحث عن الجرائم الإلكترونية ثانى هذه الآثار هو على المجتمع وهو إيقاع الضرر عليه وعلى الاقتصاد والخصوصيات للأفراد كذلك إيقاع الضرر على الدولة التى يتفكك أفرادها مسببا أعمال انقلاب عسكرية وحروب أهلية .

كذلك يسبب انتشار الجرائم الإلكترونية انتاج جيل غير سوى يبرر الجريمة ويرتكبها بأريحية دون النظر الى خطورة ذلك وتداعياته بسبب زيادة استخدام وسائل التواصل وانتشارها داخل المنزل وبين الجميع من الأطفال الى الكبار

دون النظر الى الآثار السلبية التى تسببهامثل هذه الجرائم من مشكلات اجتماعية وصحية للضحايا من نشر معلوماتهم وبياناتهم والاخبار الكاذبة التى تضر بهم وعائلاتهم

كثرة استغلال الضحية وابتزازها من أجل الحصول على مال يضر بمصالحة الشخصيه وذمته المالية

https://qanonbelaraby.com/

كيفية الابلاغ عن جريمة الكترونية فى مصر

يمكنك الإبلاغ عن الجرائم الالكترونية من خلال التواصل مع الادارة العامة لتكنولوجيا المعلومات أرقام : ٠٢٢٤٠٦٥٠٥٢ / ٠٢٢٤٠٦٥٠٥١ أو من خلال الجهاز القومى لتنظيم الاتصالات الخط الساخن ١٠٨

https://me.kaspersky.com/resource-center/threats/what-is-cybercrime

ازاى تحمى نفسك من الابتزاز الالكترونى فى ثلاث خطوات:

كثير من المواطنين يتساءل يوميا عن الاجراءات التى يجب اتباعها فى حالات التعرض للابتزاز او التهديد الالكترونى ويوضح اليوم السابع فى خطوات أهم الاجراءات التى يجب اتباعها عن التعرض للابتزاز او التهديد الالكترونى

١. تقديم بلاغ على موقع الرسمى لوزارة الداخلية على اللينك https://moi.gov.eg
٢. استخدام الخط الساخن (١٠٨) وهو خط مخصص للابلاغ عن الجرائم الالكترونية وجرائم الانترنت ويعمل على مدار ٢٤ ساعة
٣. إخطار ادارة مكافحة جرائم الحاسبات وشبكات المعلومات بمقر وزارة الداخلية بالتجمع الخامس فى القاهرة الجديدة، بالحضور الشخصى او الاتصال بأرقام ٢٧٩٢٨٤٨٤/ ٢٧٩٢٦٠٧١/ ٢٧٩٢١٤٩٠ / ٢٧٩٢١٤٩١

https://www.youm7.com/story

- توعية الاشخاص بكل مكان عن أسباب حدوث الجرائم المعلوماتية وكيفية تنفيذها فالاعلام له دور هام فى توعية المواطنين عن مدى خطورة الجرائم الالكترونية كما يجب الاشارة ايضا الى كيفية التعامل معها والحماية منها
- تجنب نشر اى صور شخصية او معلومات شخصية على مواقع التواصل الاجتماعى او اى مواقع اخرى وذلك حتى لا تتعرض للسرقة ومن ثم الابتزاز من قبل مرتكبى الجرائم الالكترونية.
- عدم كشف كلمات المرور لاى حساب سواء كان حساب مصرفى او بطاقة ائتمان أو حساب على موقع معين بالانترنت كما يجب ايضا تغييرها باستمرار لضمان عدم وقوعها الايدى الخاطئة.
- تجنب استخدام اى برامج مجهولة المصدر. كما يجب تجنب ادخال أى أكواد أو كلمات مرور مجهولة تجنبا للتعرض للقرصنة وسرقة الحسابات المستخدمة.
- تجنب فتح أى رسائل الكترونية مجهولة، وذلك حتى لا يتم اختراق نظام الحاسوب لديك وسرقة كل ما عليه معلومات شخصية وحسابات وكلمات مرور الخاصة بك
- تثبيت برامج حماية من الفيروسات والاختراقات من أجل الحفاظ على سلامة الجهاز المستخدم وسرية ما به من معلومات .
- وضع قوانين عقوبات رادعة لمرتكبى الجرائم المعلوماتية، وذلك للحد من انتشارها.
- تطوير طرق ووسائل لتتبع مرتكبى الجرائم الالكترونية بشكل دقيق والامساك بهم.

https://www.it-pillars.com/ar/blog/

طرق التصدى لهذه الجرائم

- توعية الناس لمفهوم الجريمة اللإلكترونية وانه الخطر القادم ويجب مواجهته والحرص على ألا يقعوا ضحية له.
- ضرورة التأكد من العناوين الإلكترونية التى تتطلب معلومات سرية خاصة كبطاقة ائتمانية أو حساب بنكى.
- عدم الإفصاح عن كلمة السر لاى شخص والحرص على تحديثها بشكل دورى واختيار كلمات سر غير مألوفة
- عدم حفظ الصور الشخصية فى الكمبيوتر.
- عدم تنزيل أى ملف أو برنامج من مصادر غير معروفة
- عدم إيقاف برامج مكافحة الفيروسات والجدار النارى
- الحرص على تحديث أنظمة الحماية
- تكوين منظمة لمكافحة الجريمة الإلكترونية.
- إبلاغ الجهات المختصة فى حال التعرض لجريمة إلكترونية
- وضع أنظمة تشريعية متطورة لتنظيم البيئة القانونية والتنظيمية والتى تخدم أمن تقنيات ونظم المعلومات.
- تتبع تطورات الجريمة الإلكترونية وتطوير الوسائل والاجهزة والتشريعات لمكافحتها.
- تطوير برمجيات آمنه ونظم تشغيل قوية التى تحد من الاختراقات الالكترونية وبرمجيات الفيروسات وبرامج التجسس.

https://kenanaonline.com/users/ahmedkordy/posts/320920