الجريمة السيبرانية (بالإنجليزية: Cybercrime) تشير إلى أي جريمة تتضمن الحاسوب أو الشبكات الحاسوبية. قد يستخدم الحاسوب في ارتكاب الجريمة وقد يكون هو الهدف. ويمكن تعريف الجريمة الإلكترونية على أنها أي مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي ونية الإساءة لسمعة الضحية أو لجسدها أو عقليتها، سواءً كان ذلك بطريقة مباشرة أو غير مباشرة، وأن يتم ذلك باستخدام وسائل الاتصالات الحديثة مثل الإنترنت، تشهد التقنية والتكنولوجيا تطورات كثيرة واستحداث لأمور جديدة، هذا الامر ينذر بتطور أدوات وسبل الجريمة الإلكترونية بشكل أكثر تعقيدا أو أشد ضررا من قبل، الأمر الذي يلزم الدول لتطوير آليات مكافحة هذه الجرائم واستحداث خطوط دفاع وسن قوانين وتوعية الناس بمستحدثات هذه الجرائم وتشجيعهم للإبلاغ عنها. هي كل سلوك غير قانوني يتم باستخدام الأجهزة الإلكترونية، ينتج عنها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات. تمتد من شيوع استخدام الحاسب الآلي في الستينات إلى غاية 1970، اقتضت معالجة على المقالات تمثلت في التلاعب بالبيانات المخزنة وتدميرها. في الثمانينات حيث طفح على السطوح مفهوم جديد لجرائم الكمبيوتر والإنترنت تمثلت في اقتحام الأنظمة ونشر الفيروسات. في التسعينات حيث شهدت هذه المرحلة تناميا هائلا في حقل الجرائم الإلكترونية، نظرا لانتشار الإنترنت في هذه الفترة مما سهل من عمليات دخول الأنظمة واقتحام شبكة المعلومات مثلا: تعطيل نظام تقني، مفاهيم الجريمة الإلكترونية أدت الحداثة التي تتميز بها الجريمة الإلكترونية واختلاف النظم القانونية والثقافية بين الدول إلى اختلاف في مفهوم الجريمة الإلكترونية من بينها: حسب اللجنة الأوروبية فان مصطلح الجريمة الإلكترونية يضم كل المظاهر التقليدية للجريمة مثل الغش وتزييف المعلومات، ونشر مواد إلكترونية ذات محتوى مخل بالأخلاق أو دعوى لفتن طائفية. حسب وزارة العدل في الولايات المتحدة الأمريكية التي عرفت الجريمة عبر الإنترنت بأنها «أي جريمة لفاعلها معرفة فنية بتقنية الحاسبات تمكنه من ارتكابها». حسب منظمة التعاون الاقتصادي للجريمة المرتكبة عبر الإنترنت «هي كل سلوك غير مشروع أو غير اخلاقي أو غير مصرح به، بعض تسميات الجرائم الإلكترونية جرائم الإنترنت (Computer crime) جرائم التقنية العالية (Hi-tech crime) أنواع الجرائم الإلكترونية الجرائم ضد الافراد: وتسمى بجرائم الإنترنت الشخصية تتمثل في سرقة الهوية ومنها البريد الإلكتروني، أو سرقة الاشتراك في موقع شبكة الإنترنت وانتحال شخصية أخرى بطريقة غير شرعية عبر الإنترنت بهدف الاستفادة من تلك الشخصية أو لإخفاء هوية المجرم لتسهيل عملية الإجرام. الجرائم ضد الملكية: تتمثل في نقل البرمجيات الضارة المضمنة في بعض البرامج التطبيقية والخدمية أو غيرها، بهدف تدمير الأجهزة أو البرامج المملوكة للشركات أو الأجهزة الحكومية أو البنوك أو حتى الممتلكات الشخصية. الجرائم ضد الحكومات: مهاجمة المواقع الرسمية وأنظمة الشبكات الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الإنترنت، خصائص وسمات الجرائم الإلكترونية سهولة ارتكاب الجريمة بعيدا عن الرقابة الأمنية، فهي ترتكب عبر جهاز الكمبيوتر مما يسهل تنفيذها من قبل المجرم دون أن يراه أحد أو يكتشفه. صعوبة التحكم في تحديد حجم الضرر الناجم عنه قياسا بالجرائم الإلكترونية فالجرائم الإلكترونية تتنوع بتنوع مرتكبيها وأهدافهم وبالتالي لا يمكن تحديد حجم الأضرار الناجمة عنها. مرتكبها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم أمرا صعبا أعمارهم تتراوح غالبا ما بين (18 إلى 48 سنة). تنطوي على سلوكيات غير مألوفة عن المجتمع. اعتبارها أقل عنفا في التنفيذ فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية، لأن المجرم عند تنفيذه لمثل هذه الجرائم لا يبذل جهدا فهي تطبق على الأجهزة الإلكترونية وبعيدا عن أي رقابة مما يسهل القيام بها. جريمة عابرة للحدود لا تعترف بعنصر المكان والزمان فهي تتميز بالتباعد الجغرافي واختلاف التوقيتات بين الجاني والمجني عليه، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكابها عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى. سهولة إتلاف الأدلة من قبل الجناة، الجريمة وتقنية المعلومات التقنيات كهدف مثلا اختراق أنظمة البنوك والشركات. التقنيات كسلاح مثلا الترويج لأفكار هدامة ضارة بالمجتمع. أهداف الجرائم الإلكترونية التمكين من الوصول إلى المعلومات بشكل غير قانوني كسرقة المعلومات أو حذفها والإطلاع عليها. التمكن من الوصول بواسطة الشبكة العنكبوتية إلى الاجهزة الخادمة الموفرة للمعلومات وتعطيلها أو التلاعب بمعطياتها مثل أداة المسح (nc) وتدعى سكينة الجيش السويسري في مجموعة أدوات الأمن بحيث تقدم هذه الاداة خدمة مسح قوية للبروتوكول الافتراضي وتنفذ بالشكل netcat وأيضا البروتوكول النقل tcp ولمسح هذا البرتوكول يجب إضافة المعامل2 netcat –u أداة المسح (strobe) تستخدم لمسح منفذ بروتوكول النقل المضمون tcp. الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالبنوك والمؤسسات والحكومات والأفراد والقيام بتهديدهم إما لتحقيق هدف مادي أو سياسي, أدوات الجريمة الإلكترونية برامج نسخ

المعلومات المخزنة في أجهزة الحاسب الآلي. الإنترنت كوسيط لتنفيذ الجريمة. خطوط الاتصال الهاتفي التي تستخدم لربط الكاميرات ووسائل التجسس. والهواتف الرقمية الثابتة. برامج مدمرة: مثل برنامج حصان طروادة trojan horse بحيث يقوم بخداع المستخدم لتشغيله، القراصنة الهواة Hackers : يقصد بهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الالية وبعضهم يطلق عليهم صغار نوابغ المعلوماتية وأغلبهم من الطلبة. تضم هذه الطائفة الاشخاص الذين يستهدفون من الدخول إلى انظمة الحاسبات الالية غير المصرح لهم بالدخول إليها. القراصنة المحترفين Crackers أعمارهم تتراوح ما بين 25–45 سنة في الغالب يكونون ذوي مكانة في المجتمع ودائمًا ما يكونوا من المختصين في مجال التقنية الإلكترونية. طائفة الحاقدين يطلق عليهم المنتقمون لأنها تنطلق ضد أصحاب العمل والمنشات التي كانوا يعملون بها وانتقاما من رب العمل وهم أقل خطورة، يرى الباحثون ان أهداف وأغراض الجريمة غير متوفرة لدى هذه الطائفة فهم لا يهدفون إلى إثبات قدراتهم التقنية ومهارتهم الفنية وليبغون تحقيق مكاسب مادية أو سياسية، طائفة المتطرفين الفكريين يعرف التطرف في هذا المجال بأنه عبارة عن انشطة توظف شبكة الإنترنت في نشر وبث واستقبال وإنشاء المواقع والخدمات التي تسهل انتقال وترويج المواد الفكرية المغذية للتطرف الفكري، مما دفع بعض المتشددين إلى سلوك الطريق الإجرامي وأصبح هناك ما يعرف بالمجرم المعلوماتي المتطرف الذي يستعمل بما في ذلك للشبكات الإعلامية الإخبارية التي تتبع نشطات الجماعية ونشر بيانات وتصريحات قادتها، طائفة المتجسسون يقوم هؤلاء بالعبث أو الإتلاف محتويات الشبكة من جانب ومن جانب آخر وهو الأهم والذي يشكل الخطر الحقيقي على تلك الواقع على سبيل المثال قد يتم تنزيل الأسرار الصناعية من كمبيوتر في إحدى الشركات وإرسالها بالبريد الإلكتروني مباشرة إلى منافستها، طائفة مخترقي الأنظمة: يتبادل أفراد هذه الطائفة المعلومات فيما بينهم بغية اطلاع بعضهم على مواطن الضعف في الانظمة المعلوماتية وتجري عملية التبادل للمعلومات بينهم بواسطة النشرات الاعلامية الإلكترونية مثل: مجموعات الأخبار، خصائص وسمات مرتكبو الجرائم شخص ذو مهارات فنية عالية متخصص في الجرائم المعلوماتية يستغل مداركه ومهارته في اختراق الشبكات وكسر كلمات المرور والشفرات ويسبح في عالم الشبكات، ليحصل على كل غالي وثمين من البيانات والمعلومات الموجودة في أجهزة الحواسيب من خلال الشبكات. شخص قادر على استخدام خبراته في الاختراق وتغيير المعلومات. شخص قادر على تقليد البرامج أو تحويل اموال. شخص محترف في التعامل مع شبكات الحاسبة. شخص غير عنيف لأن تلك الجريمة لا تلجأ للعنف في ارتكابها. شخص يتمتع بذكاء إذ يمكنه التغلب على كثير من العقبات التي تواجهه أثناء ارتكابه الجريمة، حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الانظمة الامنية حتى لا تستطيع ان تلاحقه وتتبع أعماله الاجرامية من خلال الشبكات أو داخل اجهزة الحواسب بالإجرام المعلوماتي هو اجرام ذكاء. شخص اجتماعي له القدرة على التكيف مع الآخرين. دوافع ارتكاب الجريمة الإلكترونية نظرًا للربح الكبير، دوافع شخصية وتتمثل في: الرغبة في التعلم يكرس مرتكبو هذه الجريمة وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة الحاسوبية. دوافع ذهنية أو نمطية: غالبا ما يكون الدافع لدى مرتكب الجرائم عبر الإنترنت هو الرغبة في إثبات الذات وتحقيق الانتصار على تقنية الانظمة المعلوماتية دون ان يكون لهم نوايا اثمة. دافع الانتقام تعد من أخطر الدوافع التي يمكن ان تنفع شخص يملك معلومات كبيرة عن المؤسسة أو شركة يعمل بها تجعله يقدم على ارتكاب جريمته. دافع سياسي يتم غالبا في المواقع السياسية المعادية للحكومة، ويتمثل في تلفيق الأخبار والمعلومات ولو زورا أو حتى الاستناد إلى جزء بسيط جدا من الحقيقة ومن ثم نسخ الأخبار الملفقة حولها، أشكال الجرائم الإلكترونية اقتحام شبكات الحاسب الالي وتخريبها (قرصنة البرامج). سرقة المعلومات أو الاطلاع عليها بدون ترخيص. انتهاك الأعراض وتشويه السمعة. جمع المعلومات والبيانات وإعادة استخدامها. مكافحة الجرائم الإلكترونية محاربة الجريمة الإلكترونية تحتاج لوقفة طويلة وقوية من قبل الدول والأفراد الكل مسؤول عن الإسهام قدر الإمكان لمحاربة والتصدي لها: تتجسد أول طرق مكافحة الجرائم الإلكترونية عبر الإنترنت في الاستدلال الذي يتضمن كل من التفتيش والمعاينة والخبرة والتي تعود إلى خصوصية الجريمة الإلكترونية عبر الإنترنت، أما الثاني سبل مكافحة الجريمة الإلكترونية هي تلك الجهود الدولية والداخلية لتجسيد قانونية للوقاية من هذه الجريمة المستحدثة، فأما الدولية فتتمثل في جهود الهيئات والمنظمات الدولية والتي تتمثل في: توعية الناس لمفهوم الجريمة الإلكترونية وانه الخطر القائم ويجب مواجهته والحرص على ألا يقعوا ضحية له. ضرورة التأكد من العناوين الإلكترونية التي تتطلب معلومات سرية خاصة كبطاقة ائتمانية أو حساب بنكي. عدم الإفصاح عن كلمة السر لأي شخص والحرص على تحديثها بشكل دوري واختيار كلمات سر غير مألوفة. عدم حفظ الصور الشخصية في الكمبيوتر. عدم تنزيل أي ملف أو برنامج من مصادر غير معروفة. الخ. تكوين منظمة لمكافحة الجريمة الإلكترونية. ابلاغ الجهات

المختصة في حال تعرض لجريمة إلكترونية. تتبع تطورات الجريمة الإلكترونية وتطوير الرسائل والأجهزة والتشريعات لمكافحتها. الهجمات الإلكترونية وصلت الجرائم الإلكترونية إلى حد القتل؛ ففي شهر 9 من عام 2020، توفيت امرأة في دوسلدورف في أحد المستشفيات الألمانية بعد تعطل نظام الحاسوب بسبب برنامج للقرصنة بواسطة الفدية، وهو برنامج خبيث يقيد الوصول إلى نظام الحاسوب الذي يصيبه. ويعكس هذا الهجوم الإلكتروني مدى هشاشة القطاع الصحي في مواجهة هذه الهجمات. وقال الكاتب أنوش سيدتاغيا في تقرير نشرته صحيفة لوتون (le temps) السويسرية، إنه لم يحدث أن سُجلت حالات وفاة نتيجة هجوم إلكتروني. ولكن تسبب هجوم سيبراني في وفاة مريضة في مستشفى بدوسلدورف نتيجة عدم تلقيها للعلاج. وأعلنت السلطات الألمانية عن العواقب المأساوية للهجوم السيبراني «الإلكتروني» الذي استهدف الشبكة الإلكترونية للمستشفى الجامعي في دوسلدورف ليصيب أنظمته بالشلل الجزئي منذ 9 سبتمبر/أيلول. وبرنامج الفدية المعروف باسم «رانسوم وير» هو برنامج ضار يستهدف نقاط الضعف في برامج معينة للسماح للمهاجمين بالتحكم عن بُعد في أنظمة الحاسوب. ومقابل إعادة الوصول إلى الملفات المحملة على أجهزة الحاسوب،