ما هى الجرائم الإلكترونية ؟ انواعها ؟ كيفية تنفيذها وطرق مواجهتها

صبحنا في عصر انتشار تكنولوجيا المعلومات أكثر عرضة للوقوع كضحايا للجرائم الإلكترونية، فانتشار التكنولوجيا ووسائل الإتصال الحديثة يعد سلاح ذو حدين، يمكن استخدامهم من أجل تسهيل الإتصالات حول العالم، فهم 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،

**ولكن ما هي الجرائم الإلكترونية؟   وما أنواعها؟   وما هي طرق تنفيذ الجرائم الإلكترونية   وكيفية مواجهتها؟**

## **مفهوم الجرائم الإلكترونية (الجرائم المعلوماتية):**

الجريمة الإلكترونية هي فعل يتسبب بضرر جسيم للأفراد أو الجماعات والمؤسسات، بهدف ابتزاز الضحية وتشويه سمعتها من أجل تحقيق مكاسب مادية أو خدمة أهداف سياسية باستخدام الحاسوب ووسائل الإتصال الحديثة مثل الإنترنت.

فتكون الجرائم المعلوماتية بهدف سرقة معلومات واستخدامها من أجل التسبب بأذى نفسي ومادي جسيم للضحية، أو إفشاء أسرار أمنية هامة تخص مؤسسات هامة بالدولة أو بيانات وحسابات خاصة بالبنوك والأشخاص، 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.

## **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 الإستفادة منها واستغلالها لتحقيق مكاسب مادية أو التشهير بسمعة أشاص بعينهم وقلب الوسط رأساً على عقب، وإفساد العلاقات سواء الإجتماعية أو علاقات العمل.
* **تهديد الأفراد:** 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.
* **تحريض على أعمال غير مشروعة:** يقوم المجرم باستخدام المعلومات المسروقة عن أفراد بعينهم واستغلالها في ابتزاز الضحايا بالقيام بأعمال غير مشروعة تتعلق بالدعارة وتجارة المخدرات وغسيل الأموال والعديد من الجرائم الإلكترونية الأخرى.

### **ثانيا: جرائم تسبب الأذى للمؤسسات.**

#### **اختراق الأنظمة:**

* وتتسبب 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 الإلكترونية](https://www.it-pillars.com/ar/blog/xdata-and-sambacry/) الخاصة باختراق الشبكات والحسابات والأنظمة بشكل سلبي على حالة الإقتصاد في البلاد، كما تتسبب في العديد من مشاكل تتعلق بتهديد الأمن القومي للبلاد إذا ما لم يتم السيطرة عليم ومكافحاتهم بكل جدارة، وتمثل نسبة الجرائم الإلكترونية والجرائم المعلوماتية حول العالم 170%، وتزداد النسبة يوم بعد يوم مما يجعلنا جميعاً في خطر محدق بسبب الإنتهاكات 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، ويتسبب ذلك في العديد من الخسائر المرتبطة بالملفات المدمرة ومدى أهميتها في إدارة وتنظيم الشركات والمؤسسات.
* 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.**

* **الإستيلاء على حسابات البنوك:**

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

* **انتهاك حقوق الملكية الفكرية والأدبية:**

وهي صناعة نسخ غير أصلية من البرامج وملفات المالتيميديا 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 والإطلاع على مخططات عسكرية تخص أمن البلاد، لذلك فهي تعتبر من أخطر الجرائم المعلوماتية.

* **استخدام المنظمات الإرهابية لأسلوب التضليل:**

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

****

## **طرق مكافحة الجرائم الإلكترونية والحد من انتشارها:**

* توعية الأشخاص بكل مكان عن أسباب حدوث الجرائم المعلوماتية وكيفية تنفيذها، فالإعلام له دور هام في توعية المواطنين عن مدى خطورة الجرائم الإلكترونية، كما يجب الإشارة أيضاً إلى كيفية التعامل معها والحماية منها.
* تجنب نشر أي صور شخصية أو معلومات شخصية على مواقع التواصل الإجتماعي أو أي مواقع أخرى، وذلك حتى لا تتعرض للسرقة ومن ثم الإبتزاز من قبل مرتكبي الجرائم الإلكترونية.
* عدم كشف كلمات المرور لأي حساب سواء كان حساب مصرفي أو بطاقة ائتمان أو حساب على موقع معين بالإنترنت، كما يجب أيضاً تغييرها باستمرار لضمان عدم وقوعها الأيدي الخاطئة.
* تجنب استخدام أي برامج مجهولة المصدر، كما يجب تجنب ادخال أي أكواد أو كلمات مرور مجهولة تجنباً للتعرض للقرصنة وسرقة الحسابات المستخدمة.
* تجنب فتح أي رسائل إلكترونية مجهولة، وذلك حتى لا يتم اختراق نظام الحاسوب لديك وسرقة كل ما عليه من مععلومات شخصية وحسابات وكلمات المرورو الخاصة بك.
* تثبيت برامج حماية من الفيروسات والإختراقات من أجل الحفاظ على سلامة الجهاز المستخدم وسرية ما به من معلومات.
* وضع قوانين عقوبات رادعة لمرتكبي الجرائم المعلوماتية، وذلك للحد من انتشارها.
* تطوير طرق ووسائل لتتبع مرتكبي الجرائم الإلكترونية بشكل دقيق والإمساك بهم.

**بعض تسميات الجرائم الإلكترونية**

* جرائم الإنترنت (Computer crime)
* جرائم التقنية العالية (Hi-tech crime)
* الجريمة السيبرانية (Cyber crime)

**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 الالكترونية تتنوع بتنوع مرتكبيها وأهدافهم وبالتالي لايمكن تحديد حجم الأضرار الناجمة عنها.
* مرتكبها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم امرا 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، فالمعلومات المتداولة عبر الإنترنت على هيئة رموز مخزنة على وسائط تخزين ممغنطة وهي عبارة عن نبضات إلكترونية غير مرئية مما يجعل أمر طمس ومحو الدليل أمر سهل.

**الجريمة وتقنية المعلومات**

* التقنيات كهدف مثلا اختراق أنظمة البنوك والشركات.
* التقنيات كسلاح مثلا الترويج لأفكار هدامة ضارة بالمجتمع.
* التقنيات كمساعد مثلا استعمالها في التزوير والتزييف والاحتيال.

**اهداف 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 اداة المسح (nc) وتدعى سكينة الجيش السويسري في مجموعة ادوات الأمن بحيث تقدم هذه الاداة خدمة مسح قوية للبروتوكول الافتراضي وتنفذ بالشكلnetcat وأيضا البروتوكول النقلtcp ولمسح هذا البرتوكول يجب إضافة المعامل2 u- netcat اداة المسح (strobe) تستخدم لمسح منفذ بروتوكول النقل المضمون tcp.
* الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالبنوك والمؤسسات والحكومات والأفراد والقيام بتهديدهم اما لتحقيق هدف مادي أو سياسي
* الكسب المادي أو المعنوي أو السياسي غير المشروع مثل تزوير بطاقات الائتمان وسرقة الحسابات المصرفية.

**ادوات الجريمة الإلكترونية**

* برامج نسخ المعلومات المخزنة في اجهزة الحاسب الالي.
* الإنترنت كوسيط لتنفيذ الجريمة.
* خطوط الاتصال الهاتفي التي تستخدم لربط الكمرات ووسائل التجسس.
* ادوات مسح الترميز الرقمي (البا ركو د)
* الطابعات.
* اجهزة الهاتف النقال والهواتف الرقمية الثابتة.
* برامج مدمرة: مثل برنامج حصان طروادة trojan horse بحيث يقوم بخداع المستخدم لتشغيله، حيث يظهر على شكل برنامج مفيد وامن ويؤدي تشغيله إلى تعطيل الحاسب المصاب و برنامج الدودة الذي يشبه الفيروس ولكنه يصيب اجهزة الحاسب دون الحاجة إلى اي فعل وغالبا يحدث عندما ترسل بريد إلكتروني إلى كل الأسماء الموجودة في سجل الأسماء.

**مرتكبوا الجرائم الإلكترونية**

* **طائفة القراصنة'**

وهي بدورها تنقسم إلى:

* **القراصنة الهواة Hackers :**

يقصد بهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الالية وبعضهم يطلق عليهم صغار نوابغ المعلوماتية واغلبهم من الطلبة. تضم هذه الطائفة الاشخاص الذين يستهدفون من الدخول إلى انظمة الحاسبات الالية غير المصرح لهم بالدخول اليها. كسر الحواجز الامنية الموضوعة لهذا الغرض وذلك بهدف الخبرة أو الفضول.

* **القراصنة المحترفين Crackers**

أعمارهم تتراوح مابين 25–45 سنة في الغالب يكونون ذوي مكانة في المجتمع ودائمًا ما يكونوا من المختصين في مجال التقنية الإلكترونية. هم أكثر خطورة وعادة مايعودون إلى ارتكاب الجريمة مرة اخرى.

* **طائفة الحاقدين**

يطلق عليهم المنتقمون لأنها تنطلق ضد اصحاب العمل والمنشات التي كانوا يعملون بها وانتقاما من رب العمل وهم اقل خطورة، يرى الباحثون ان اهداف وأغراض الجريمة غير متوفرة لدى هذه الطائفة فهم لا يهدفون إلى اثبات قدراتهم التقنية ومهارتهم الفنية وليبغون تحقيق مكاسب مادية أو سياسية، بل يعمدون إلى اخفاء وإنكار افعالهم واغلب انشطتهم تتم باستخدام تقنيات زراعة الفيروسات والبرامج الضارة لتخريب الانظمة المعلوماتية.

* **طائفة المتطرفين الفكريين**

يعرف التطرف في هذا المجال بأنه عبارة عن انشطة توظف شبكة الإنترنت في نشر وبث واستقبال وإنشاء المواقع و الخدمات التي تسهل انتقال وترويج المواد الفكرية المغذية للتطرف الفكري، مما دفع بعض المتشددين إلى سلوك الطريق الإجرامي وأصبح هناك ما بعرف بالمجرم المعلوماتي المتطرف الذي يستعمل بما في ذلك للشبكات الاعلامية الاخبارية التي تتبع نشطات الجماعية ونشر بيانات وتصريحات قادتها، وعادة ما يقوم هؤلاء بالاتصال من مقاهي ومكاتب الإنترنت يستعملون كافة المواقع الإلكترونية التي تسعى لتحقيق اغراض دعائية لصالحهم.

* **طائفة المتجسسون**

يقوم هؤلاء بالعبث أو الإتلاف محتويات الشبكة من جانب ومن جانب اخر وهو الأهم و الذي يشكل الخطر الحقيقي على تلك الواقع على سبيل المثال قد يتم تنزيل الاسرار الصناعية من كمبيوتر في احدى الشريكات و ارسالها بالبريد الإلكتروني مباشرة إلى منافستها، ومن أهم اهداف هذه الطائفة في استخدام الانظمة المعلوماتية هي الحصول على معلومات الاعداء والأصدقاء على حد سواء

* طائفة مخترقي الانظمة:

يتبادل افراد 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 الاخبار، بل ان افراد هذه الطائفة يتولون عقد المؤتمرات لكافة مخترقي الانظمة المعلوماتية بحيث يدعى اليها الخبراء من بينهم للتشاور حول وسائل الاختراق واليات نجاحها.

**خصائص وسمات مرتكبو الجرائم**

* شخص ذو مهارات فنية عالية متخصص في الجرائم المعلوماتية يستغل مداركه ومهارته في اختراق الشبكات وكسر كلمات المرور و الشفرات ويسبح في عالم الشبكات، ليحصل على كل غالي وثمين من البيانات والمعلومات الموجودة في اجهزة 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 تلجا للعنف في ارتكابها.
* شخص يتمتع بذكاء اذ يمكنه التغلب على كثير من العقبات التي تواجهه اثناء ارتكابه الجريمة، حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الانظمة الامنية حتى لا تستطيع ان تلاحقه وتتبع اعماله الاجرامية من خلال الشبكات أو داخل اجهزة الحواسب فالإجرام المعلوماتي هو اجرام ذكاء.
* شخص اجتماعي له القدرة على التكيف مع الاخرين.

**دوافع ارتكاب الجريمة الإلكترونية**

* دوافع مادية ويتمثل في:تحقيق الكسب المادي: تعد الرغبة في تحقيق الثراء من العوامل الرئيسية لارتكاب الجريمة عبر الإنترنت. نظرا للربح الكبير، وغالبا ما يكون الدافع لارتكاب هذه الجريمة هو وقوع الجاني في مشاكل مادية مثال على ذلك تحويل حساب مالي إلى حسابه.
* دوافع شخصية وتتمثل في:
  + الرغبة في التعلم يكرس مرتكبو هذه الجريمة وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الامنية للأنظمة الحاسوبية.
  + دوافع ذهنية أو نمطية: غالبا ما يكون الدافع لدى مرتكب الجرائم عبر الإنترنت هو الرغبة في اثبات الذات وتحقيق الانتصار على تقنية الانظمة المعلوماتية دون ان يكون لهم نوايا اثمة.
  + دافع لانتقام تعد من اخطر الدوافع التي يمكن ان تنفع شخص يملك معلومات كبيرة عن المؤسسة أو شركة يعمل بها تجعله يقدم على ارتكاب جريمته.
  + دافع التسلية هي جريمة ترتكب من اجل التسلية لايقصد من ورائها احداث جرائم.
  + دافع سياسي يتم غالبا في المواقع السياسية المعادية للحكومة، ويتمثل في تلفيق الاخبار والمعلومات ولو زورا أو حتى الاستناد إلى جزء بسيط جدا من الحقيقة ومن ثم نسخ الاخبار الملفقة حولها، تعد الدوافع السياسية من ابرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم.

**اشكال الجرائم الإلكترونية**

* اقتحام شبكات الحاسب الالي وتخريبها(قرصنة البرامج).
* سرقة المعلومات أو الاطلاع عليها بدون ترخيص.
* انتهاك الاعراض وتشويه السمعة.
* اتلاف وتغيير ومحو البيانات والمعلومات.
* تسريب المعلومات والبيانات.
* جمع المعلومات والبيانات و اعادة استخدامها.
* نشر واستخدام برامج الحاسب الالي بما يشكل انتهاك لقوانين حقوق الملكية و الاسرار التجارية.

مكافحة الجرائم الإلكترونية

* محاربة الجريمة الإلكترونية تحتاج لوقفة طويلة وقوية من قبل الدول و الأفراد الكل مسؤول عن الإسهام قدر الإمكان لمحاربة و التصدي 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، اما الثاني سبل مكافحة الجريمة الإلكترونية هي تلك الجهود الدولية و الداخلية 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 اي ملف أو برنامج من مصادر غير معروفة.
* الحرص على تحديث انظمة الحماية مثل:استخدام برامج الحماية مثل نورتون norton، كاسبر سكي، مكافي.Mcafee...الخ.
* تكوين منظمة لمكافحة الجريمة الإلكترونية.
* ابلاغ الجهات المختصة في حال تعرض لجريمة إلكترونية.
* تتبع تطورات الجريمة الإلكترونية وتطوير الرسائل والأجهزة والتشريعات لمكافحتها.
* تطوير برمجيات امنة ونظم تشغيل قوية التي تحد من الاختراقات الإلكترونية وبرمجيات الفيروسات وبرامج التجسس مثل مضادات التجسس وهي برامج تقوم بمسح الحاسب للبحث عن مكونات التجسس وإلغائها مثل: lava soft

**الهجمات الإلكترونية**

وصلت الجرائم الإلكترونية إلى حد القتل ؛ففي شهر 9 من عام 2020، توفيت امرأة في [دوسلدورف](https://ar.wikipedia.org/wiki/%D8%AF%D9%88%D8%B3%D9%84%D8%AF%D9%88%D8%B1%D9%81) 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](https://ar.wikipedia.org/wiki/%D9%87%D8%AC%D9%88%D9%85_%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A) 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

و[برنامج الفدية](https://ar.wikipedia.org/wiki/%D8%A8%D8%B1%D9%86%D8%A7%D9%85%D8%AC_%D9%81%D8%AF%D9%8A%D8%A9) 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، عادة ما يطلب المخترق فدية تصل إلى عشرات أو حتى مئات الآلاف من الفرنكات.

