ما هي الجريمة الإلكترونية؟

الجرائم الإلكترونية هي نشاط إجرامي يستهدف جهاز كمبيوتر أو شبكة كمبيوتر أو جهازًا متصلًا بالشبكة وتحاول استخدامهم. تقع معظم الجرائم الإلكترونية على أيدي لصوص أو مخترقين يودون كسب الأموال، وأحيانًا نادرة أخرى يكون الهدف من وراء الجرائم الإلكترونية هو إلحاق الضرر بأجهزة الكمبيوتر لأسباب غير الربح، وقد تكون هذه الأسباب سياسية أو شخصية.

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

ما هي أنواع الجرائم الإلكترونية؟

أنواع الجريمة الإلكترونية تشمل ما يلي:

1. الاحتيال عبر البريد الإلكتروني والإنترنت.
2. تزوير الهوية (حيث تتم سرقة المعلومات الشخصية واستخدامها.)
3. سرقة البيانات المالية أو بيانات الدفع بالبطاقة.
4. سرقة بيانات الشركة وبيعها.
5. الابتزاز الإلكتروني (طلب المال لمنع هجوم مهدد.)
6. هجمات برامج الفدية) نوع من الابتزاز الإلكتروني.)
7. السرقة المشفّرة) حيث يقوم المتسللون بتعدين العملات المشفّرة باستخدام موارد لا يملكونها.)
8. التجسس الإلكتروني (حيث يتمكن المتسللون من الوصول إلى بيانات الحكومة أو الشركة.)
9. التدخل في الأنظمة بطريقة تعرّض الشبكة للخطر.
10. انتهاك حقوق النشر.
11. المقامرة غير المشروعة.
12. بيع السلع غير المشروعة عبر الإنترنت.
13. طلب مواد إباحية تستغل الأطفال أو إنتاجها أو امتلاكها.

تشمل الجرائم الإلكترونية الأمرين التاليين أو أحدهما على الأقل:

- نشاط إجرامي *يستهدف* أجهزة الكمبيوتر باستخدام الفيروسات وأنواع أخرى من البرمجيات الخبيثة.
- نشاط إجرامي *يستخدم* أجهزة الكمبيوتر لارتكاب جرائم أخرى.

مرتكبو الجرائم الإلكترونية الذين *يستهدفون* أجهزة الكمبيوتر قد يصيبونها ببرمجية خبيثة لإتلاف الأجهزة أو إيقافهاعن العمل، وقد يستخدمون تلك البرمجية الخبيثة في حذف البيانات أو سرقتها. يمكن كذلك أن يعمل مرتكبو الجرائم

الإلكترونية على منع المستخدمين من استخدام موقع إلكتروني أو شبكة أو منع شركة تقدم خدمة برمجية من الوصول إلى عملائها، وهذا الأسلوب معروف باسم هجوم الحرمان من الخدمات.(DoS)

قد تشمل الجريمة الإلكترونية التي تستخدم أجهزة الكمبيوتر لارتكاب جرائم أخرى استخدام أجهزة الكمبيوتر أو الشبكات لنشر البرامج الضارة أو المعلومات أو الصور غير المشروعة.

غالبًا ما يفعل مرتكبو الجرائم الإلكترونية الأمرين في الوقت نفسه. قد يستهدفون أجهزة الكمبيوتر التي تحتوي على فيروسات أولاً ثم يستخدمونها لنشر البرمجيات الخبيثة على أجهزة أخرى أو عبر الشبكة. توجد كذلك بعض البلاد التي تضع فئة ثالثة من الجرائم الإلكترونية حيث يتم استخدام أجهزة كمبيوتر كملحق في الجريمة. من أمثلة ذلك استخدام أجهزة كمبيوتر لتخزين البيانات المسروقة.

أمثلة على الجرائم الإلكترونية

فيما يلي بعض الأمثلة الشهيرة لأنواع مختلفة من هجمات الجرائم الإلكترونية التي يستخدمها مجرمو الإنترنت:

1. 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 الخبيثةWannaCry ، 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 الفديةWannaCry ، تأثر 230 ألف جهاز كمبيوتر في 150دولة به! تعذر على المستخدمين الوصول إلى ملفاتهم، وتلقى كل مستخدم رسالة تطلب منه دفع فدية بعملة البتكوين 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.

2. التصيد الاحتيالي

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 لتقريرنا احتيال 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 الشخصيةِ الخاصة بالأشخاص الذين فتحوا رسائل البريد الإلكتروني هذه والضغط على الروابط الواردة فيها .

هناك نوع آخر من حملات التصيد الاحتيالي معروف باسم التصيد بالحربة .هذه هي حملات التصيد الاحتيالي المستهدفة التي تحاول خداع أفراد معيّنين لتعريض أمن المؤسسة التي يعملون فيها للخطر .

على عكس حملات التصيد الاحتيالي العادية التي تعتبر عامة جدًا من حيث الأسلوب، يتم في العادة تصميم رسائل التصيد بالحربة لتبدو وكأنها رسائل من مصدر موثوق. على سبيل المثال: يتم تصميمها لتبدو كأنها من المدير التنفيذي أو مدير تكنولوجيا المعلومات، وقد لا تحتوي على أي دلالة بصرية على كونها زائفة.

3.هجمات الحرمان من الخدمات الموزَّعة

هجمات الحرمان من الخدمات الموزَّعة (DDoS) هي إحدى أنواع هجمات الجرائم الإلكترونية التي يستخدمها المجرمون الإلكترونيون في إسقاط نظام أو شبكة. يتم أحيانًا استخدام أجهزة إنترنت الأشياء المتصلة (IoT) في شن هجمات الحرمان من الخدمات.

يتسبب هجوم الحرمان من الخدمات في إرباك النظام باستخدام أحد بروتوكولات الاتصال القياسية التي يستخدمها لإرسال البريد العشوائي إلى النظام بطلبات الاتصال. وقد يستخدم المجرمون الإلكترونيون الذين ينفّذون الابتزاز الإلكتروني التهديد بهجوم الحرمان من الخدمات للمطالبة بالمال. بدلاً من ذلك، يمكن استخدام هجوم الحرمان من الخدمات كأسلوب إلهاء أثناء وقوع نوع آخر من الجرائم الإلكترونية.

من الأمثلة الشهيرة لهذا النوع من الهجمات هو هجوم الحرمان من الخدمات لعام 2017 على موقع UK National Lotteryأدى هذا الهجوم إلى قطع اتصال موقع اليانصيب على الإنترنت وتطبيق الجوال بالإنترنت، مما منع مواطني المملكة المتحدة من اللعب. لا يزال سبب الهجوم غير معروف، إلا أنه يُشتبه في أن الهجوم كان محاولة لابتزاز اليانصيب الوطني.

تأثير الجرائم الإلكترونية

سرقة الهوية في ازدياد عام لا يتوقف، فوفقًا تقرير حالة مرونة الأمن السيبراني لعام 2021 منAccenture ، زادت الهجمات الأمنية بنسبة 31٪ من 2020 إلى 2021، وزاد عدد الهجمات لكل شركة من 206 إلى 270 على أساس سنوي. الهجمات على الشركات تؤثر على الأفراد أيضًا لأن العديد منهم يخزنون بيانات حساسة ومعلومات شخصية من العملاء.

يمكن لهجوم واحد –سواء كان خرقًا للبيانات أو برمجيات خبيثة أو برنامج طلب فدية أو هجوم حرمان من الخدمات– يكلف الشركات من جميع الأحجام ما متوسطه 200 ألف دولار، وتخرج العديد من الشركات المتضررة من العمل في غضون ستة أشهر من الهجوم، وذلك وفقًا شركة التأمين.Hiscox

نشرت Javelin Strategy & Research دراسة عن احتيال الهوية في عام 2021 وجدت فيها أن خسائر الاحتيال في الهوية لذلك العام بلغت 56 مليار دولار.

بالنسبة للأفراد والشركات، يمكن أن يكون تأثير الجريمة الإلكترونية عميقًا: ضررًا ماليًا في المقام الأول، ولكن أيضًا فقدان الثقة والإضرار بالسمعة.

كيفية حماية نفسك عبر الإنترنت من الجرائم الإلكترونية

نظرًا لانتشار الجرائم الإلكترونية، قد تتساءل عن وقاية نفسك منها. إليك بعض النصائح البسيطة لحماية جهاز الكمبيوتر الخاص بك وبياناتك الشخصية من الجرائم الإلكترونية:

1.إبقاء البرنامج ونظام التشغيل محدّثَين

يضمن إبقاء البرنامج ونظام التشغيل لديك محدّثَين استفادتك من أحدث تصحيحات الأمن لحماية جهاز الكمبيوتر الخاص بك.

2.استخدام برنامج مكافحة الفيروسات وإبقائه محدّثًا

يشكّل استخدام برنامج لمكافحة الفيروسات أو حل شامل لأمن الإنترنت مثل Kaspersky Premium طريقة ذكية لحماية النظام من الهجمات. يتيح لك برنامج مكافحة الفيروسات إمكانية فحص التهديدات واكتشافها وإزالتها قبل أن تصبح مشكلة. وجود هذه الحماية يساعد في حماية جهاز الكمبيوتر الخاص بك وبياناتك من الجرائم الإلكترونية، مما يمنحك راحة البال. أبقِ برنامج مكافحة الفيروسات محدَّثًا للحصول على أفضل مستوى من الحماية.

3.استخدام كلمات مرور قوية

تأكد من استخدام كلمات مرور قوية لا يمكن للأشخاص معرفتها ولا تقم بتسجيلها في أي مكان. يمكنك كذلك استخدم تطبيق مدير كلمات مرور حسن السمعة لإنشاء كلمات مرور قوية بشكل عشوائي لتسهيل الأمر عليك.

.4عدم فتح المرفقات في رسائل البريد الإلكتروني العشوائية أبدًا

تشكّل مرفقات البريد الإلكتروني في رسائل البريد الإلكتروني العشوائية طريقة تقليدية لإصابة جهاز الكمبيوتر ببرامج ضارة وغيرها من أشكال الجرائم الإلكترونية. لا تفتح أبدًا مرفقًا من مرسِل لا تعرفه.

.5عدم فتح الروابط في رسائل البريد الإلكتروني العشوائية أو على مواقع الويب غير الموثوق بها

توجد طريقة أخرى يصبح بها الأشخاص ضحايا للجرائم الإلكترونية، وهي فتح الروابط الموجودة في رسائل البريد الإلكتروني العشوائية أو الرسائل الأخرى أو المواقع الإلكترونية غير المألوفة. تجنّب القيام بهذا الأمر للحفاظ على أمنك على الإنترنت.

.6عدم تقديم المعلومات الشخصية إلا إذا كنت آمنًا

لا تقدم أبدًا بيانات شخصية عبر الهاتف أو عبر البريد الإلكتروني إلى أي جهة ما لم تكن متأكدًا تمامًا من أمان الخط أو البريد الإلكتروني. تأكد من أنك تتحدث إلى الشخص الذي تعتقد أنك تتحدث معه .

.7الاتصال بالشركات مباشرةً بشأن الطلبات المشبوهة

إذا اتصلت بك شركة وطلبت منك معلومات شخصية أو بيانات، أنه المكالمة بدون إعطائهم شيء، ثم أعد الاتصال بهم مرة أخرى باستخدام الرقم الموجود على الموقع الإلكتروني الرسمي الخاص بهم للتأكد من أنك تتحدث إليهم وليس مع مجرمي الإنترنت. الأفضل كذلك استخدام رقم هاتف مختلف لأن مجرمي الإنترنت يمكنهم إبقاء الخط مفتوحًا. عندما تعتقد أنك اتصلت بالشركة مجددًا، يمكنهم الادّعاء بأنهم من المصرف أو مؤسسة أخرى تعتقد أنك تتحدث معها.

.8التنبّه لعناوين مواقع URL التي تزورها

راقب عناوين مواقع URL التي تفتحها. هل تبدو مشروعة؟ تجنب الضغط على الروابط التي تحتوي على عناوين URLغير مألوفة أو التي تبدو كرسالة غير مرغوب فيها. إذا كان منتج أمن الإنترنت لديك يشمل وظائف لضمان أمن المعاملات عبر الإنترنت، فتأكد من تمكينها قبل تنفيذ المعاملات المالية عبر الإنترنت.

.9مراقبة بياناتك المصرفية

من المهم اكتشاف أنك وقعت ضحية جريمة إلكترونية بسرعة. راقب بياناتك المصرفية واستفسر عن أي معاملات غير مألوفة مع المصرف، ويمكن للمصرف التحقيق فيما إذا كانت احتيالية أم لا.