بحث عن الجرائم الإلكترونية

مقدمة البحث

تشكل الجرائم الإلكترونية تهديدًا خطيرًا للأفراد والشركات والهيئات الحكومية ويمكن أن تؤدي إلى خسائر مالية كبيرة وإلحاق الضرر بالسمعة وتعريض الضحية لخطر كبير، ومع تقدم التكنولوجيا وتزايد اعتماد الأشخاص على الأجهزة والشبكات الرقمية، يستمر تهديد الجرائم الإلكترونية في التزايد، مما يجعل اتخاذ خطوات للحماية منها أكثر أهمية من أي وقت مضى، وفيما يأتي نقدم لكم بحثاً عن الجرائم الإلكترونية.

بحث عن الجرائم الإلكترونية

وفيما يأتي تجدون فقرات بحث عن الجرائم الإلكترونية:

مفهوم الجرائم الإلكترونية

الجريمة الإلكترونية أو ما يسمى الجريمة السيبرانية هي مصطلح عام يصف عددًا لا يحصى من الأنشطة الإجرامية التي يتم تنفيذها باستخدام جهاز كمبيوتر أو شبكة أو مجموعة أخرى من الأجهزة الرقمية. تعدّ الجريمة السيبرانية المظلة التي تغطي نطاقًا واسعًا من الأنشطة غير القانونية التي يرتكبها مجرمو الإنترنت، وتشمل هذه الهجمات القرصنة والتصيد الاحتيالي وسرقة الهوية وبرامج الفدية وهجمات البرامج الضارة، وغيرها من الأعمال المؤذية.
يتخطى نطاق الجريمة السيبرانية جميع الحدود المادية، حيث ينتشر المجرمون والضحايا والبنية التحتية التقنية في جميع أنحاء العالم. تتخذ الجريمة السيبرانية أشكالًا عديدة وتتطور باستمرار مع استخدام التكنولوجيا لاستغلال الثغرات الأمنية على المستوى الشخصي وعلى مستوى المؤسسات، وفي المقابل، فإن القدرة على التحقيق بشكل فعال في الجرائم الإلكترونية ومحاكمتها ومنعها هي معركة مستمرة تواجهها الكثير من التحديات.

تصنيفات الجرائم الإلكترونية

يمكن تصنيف الجرائم الإلكترونية بشكل عام إلى أربع فئات:

- **الجرائم الإلكترونية الفردية**: هذا النوع يستهدف الأفراد. ويشمل التصيد الاحتيالي والانتحال والبريد العشوائي والمطاردة عبر الإنترنت والمزيد.
- **الجرائم الإلكترونية المنظمة**: الهدف الرئيسي هنا هو المنظمات. عادة، يتم تنفيذ هذا النوع من الجرائم من قبل فرق من المجرمين بما في ذلك هجمات البرامج الضارة وهجمات تعطيل الخدمة.
- **الجرائم الإلكترونية العقارية**: يستهدف هذا النوع الملكية مثل بطاقات الائتمان أو حتى حقوق الملكية الفكرية.
- **الجرائم الإلكترونية المجتمعية**: وهذا هو أخطر أشكال الجرائم السيبرانية لأنه يشمل الإرهاب السيبراني.

أنواع الجرائم الإلكترونية

تغطي الجريمة السيبرانية مجموعة واسعة من الأنشطة الإجرامية التي تنطوي على منصات وتقنيات رقمية مختلفة. ويوجد العديد من أنواع الجرائم الإلكترونية التي تستحق المناقشة، بدءًا من رسائل البريد الإلكتروني الاحتيالية وأنشطة وسائل التواصل الاجتماعي وحتى عمليات التصيد الاحتيالي وهجمات برامج الفدية. وأكثر أنواع هذه الجرائم شيوعاً هي:

عمليات الاحتيال عبر البريد الإلكتروني: وهي عبارة عن رسائل مضللة تأخذ أشكالاً عديدة. تعمل رسائل البريد الإلكتروني المزيفة على تضليل المستلمين، بينما تخدع تقنيات الهندسة الاجتماعية الأشخاص لإفشاء معلومات، مثل أرقام بطاقات الائتمان، أو تحويل الأموال إلى المهاجم، ومن أشهر أشكال عمليات الاحتيال عبر البريد الإلكتروني مخططات التصيد الاحتيالي، حيث يحاكي المحتالون العلامات التجارية المشروعة، وينتحلون شخصياتها.

الاحتيال عبر وسائل التواصل الاجتماعي: عمليات الاحتيال التي تستخدم منصات التواصل الاجتماعي مثل Facebook وTwitter وInstagram وTikTok لخداع الضحايا والاحتيال عليهم. تشمل الأمثلة المتاجر الوهمية عبر الإنترنت، أو عمليات الاحتيال، أو هجمات الهندسة الاجتماعية، أو عمليات الاحتيال لانتحال الشخصية. غالبًا ما تستغل عمليات الاحتيال عبر وسائل التواصل الاجتماعي ثقة المستخدم، والسذاجة، والميل إلى الإفراط في مشاركة المعلومات الشخصية عبر الإنترنت.

الاحتيال المصرفي: وهي الأنشطة الاحتيالية التي تستهدف المؤسسات المالية أو عملائها وأصحاب المصلحة. تؤدي عمليات الاحتيال المصرفي في أغلب الأحيان إلى خسارة مالية كبيرة أو سرقة الهوية، وغالبًا ما تتضمن استراتيجيات المهاجم أساليب قرصنة وهندسة اجتماعية متطورة. تشمل الأمثلة الاحتيال على بطاقات الائتمان، وعمليات الاحتيال على أجهزة الصراف الآلي، وعمليات الاحتيال المصرفية عبر الإنترنت.

الاحتيال في التجارة الإلكترونية: يستغل المهاجم نقاط الضعف والمزالق في تقنيات التسوق عبر الإنترنت، مثل المتاجر الاصطناعية أو الملفقة عبر الإنترنت، أو حسابات البائعين المزيفة، أو سرقة معلومات بطاقة الائتمان. عادةً ما تؤدي حالات الاحتيال في التجارة الإلكترونية إلى خسائر مالية لكل من المستهلكين وتجار التجزئة عبر الإنترنت.

البرامج الضارة: هجوم برمجي واسع الانتشار مبرمج لإتلاف أنظمة الكمبيوتر والتلاعب بها عن طريق إدخال الفيروسات أو أحصنة طروادة أو برامج التجسس إلى النظام. تعد البرامج الضارة مشكلة متكررة في العديد من الحالات لأنها تستهدف كلاً من أجهزة الكمبيوتر الفردية وشبكات الكمبيوتر على مستوى المؤسسة. يتم استخدام هذا النوع من الهجمات بشكل شائع لتعطيل الشبكات وسرقة البيانات من المستخدمين.

فيروس الفدية: وهو نوع من هجمات البرمجيات الخبيثة التي تقوم بتشفير البيانات الهامة للضحايا ويطلب المهاجم فدية مقابل الحصول على مفتاح فك التشفير لاستعادة البيانات المشفرة. غالبًا ما تؤدي هجمات برامج الفدية، التي تسبب شللًا ماليًا للأفراد والمؤسسات على حد سواء، إلى فقدان البيانات والأصول، والدمار المالي، وتعطيل الإنتاجية، تم استخدام هذا النوع من على حكومة كوستاريكا وتحولت إلى حالة طوارئ وطنية.

فيروسات الكمبيوتر: ربما يكون هذا هو النوع الأكثر شيوعًا من البرامج الضارة التي يمكنها النسخ ذاتيًا والانتشار إلى أنظمة أخرى، وغالبًا ما تتسبب في تلف ملفات الكمبيوتر أو برامجه. تتضمن أمثلة فيروسات الكمبيوتر فيروسات Melissa وILOVEYOU وNimda - والتي تنتشر جميعها بسرعة لإصابة الملفات وإتلاف أنظمة الكمبيوتر.

قرصنة البرمجيات: شكل من أشكال سرقة الملكية الفكرية يتضمن الاستخدام غير المصرح به أو توزيع المواد المحمية بحقوق الطبع والنشر، مثل البرامج أو الموسيقى أو الأفلام. تتضمن أمثلة قرصنة البرامج استخدام مولدات المفاتيح أو برامج الكراك لتنشيط البرامج المدفوعة دون ترخيص.

هجمات DDoS: تتم برمجة هجمات تعطيل الخدمة الموزعة، أو هجمات DDoS، لإغراق الشبكة أو موقع الويب بحركة المرور (عن طريق إرسال عدد هائل من الرسائل في نفس الوقت)، مما يؤدي إلى إبطائها أو تعطلها بالكامل. كانت هجمات DDoS واحدة من العديد من الأنشطة السيبرانية المدمرة التي قامت بها روسيا ضد أوكرانيا، إلى جانب الهجمات الأخرى المصممة لحذف بيانات الكمبيوتر التابعة لجهات حكومية وخاصة.

الإرهاب الإلكتروني: وتشمل بشكل عام، أعمال التدمير الكبرى عبر الإنترنت باستخدام الإنترنت أو تكنولوجيا المعلومات لتنفيذ أعمال إرهابية، مثل التسبب في تدمير البنية التحتية والأعطال الكارثية للدول أو المنظمات الكبرى، أو سرقة المعلومات السرية، أو نشر الدعاية ذات الآثار السياسية أو الثقافية. أصبحت حالات الإرهاب السيبراني معقدة بشكل متزايد، مما يفرض متطلبات أكبر على الأمن والحماية السيبرانية.

تأثير الجرائم الإلكترونية

مع تزايد تطور أنواع الجرائم الإلكترونية، يتزايد أيضًا الحجم الهائل للتهديدات والخسائر المالية المرتبطة بها. وفقًا لتقارير مكتب التحقيقات الفيدرالي، سلط وزير الأمن الداخلي مايوركاس الضوء على الخسائر المتعلقة بالجرائم الإلكترونية التي تجاوزت 4.1 مليار دولار في عام 2020.
تُظهر التقارير الأحدث الصادرة عن قسم مركز شكاوى جرائم الإنترنت (IC3) التابع لمكتب التحقيقات الفيدرالي خسائر تتجاوز 6.9 مليار دولار في عام 2021. واستنادًا إلى تقرير IC3، يعزو مكتب التحقيقات الفيدرالي هذا الارتفاع الحاد في خسائر الجرائم الإلكترونية إلى المزيد من هجمات برامج الفدية وعمليات الاحتيال عبر البريد الإلكتروني التجاري والعملات المشفرة. ويسلط التقرير الضوء أيضًا على المشهد المتطور للهجمات السيبرانية التي أصبحت مرتبطة بشكل متزايد بالعلاقات الدولية وتهديدات الاستخبارات الأجنبية.
تتفشى الجرائم الإلكترونية في منازل العديد من الأشخاص وأجهزة الكمبيوتر الشخصية. وفقًا للإحصائيات التي نشرتها وكالة الأمن السيبراني والبنية التحتية (CISA)، كشف 47% من الأمريكيين عن معلوماتهم الشخصية للمجرمين عبر الإنترنت، وأصابت البرامج الضارة ثلث أجهزة الكمبيوتر المنزلية.
ويبدو أن التأثير المستقبلي للجريمة السيبرانية هو محرك اقتصادي محوري ودعوة ضخمة للعمل من أجل شركات الأمن السيبراني والبلدان التي تستضيفها. وتتوقع شركة Cybersecurity Ventures أن تستمر التكاليف العالمية للجرائم الإلكترونية في النمو بنسبة 15% سنويًا على مدى السنوات الخمس المقبلة، لتصل إلى 10.5 تريليون دولار من الأضرار السنوية بحلول عام 2025.

أشهر الجرائم الإلكترونية الكبيرة

لا يمكن عد وإحصاء الجرائم الإلكترونية التي تعرضت لها مختلف الكثير من الجهات حول العالم، وفي هذا البحث سنكتفي بذكر شركة Yahoo محرك البحث الشهير على الإنترنت التي كانت ضحية للعديد من الهجمات الإلكترونية عبر تاريخها. في عام 2013، أدى الهجوم إلى اختراق ثلاثة مليارات حساب على Yahoo، بما في ذلك الأسماء وأسئلة الأمان وكلمات المرور وتفاصيل الاتصال. ومما زاد الأمر سوءاً أن الاختراق تكرر في عام 2014، حيث تم اختراق 500 مليون حساب آخر. فازت شركة ياهو بلقب أكبر كيان منفرد يتم اختراقه في تاريخ الإنترنت.
وقد تم مؤخراً التعرف على مجموعة من المتسللين الروس الذين يقفون وراء الهجوم. لقد استهدفوا قاعدة بيانات Yahoo لسرقة السجلات ومعلومات المستخدم من خلال رسائل البريد الإلكتروني التصيدية المرسلة إلى موظفي شركة Yahoo والتي خدعتهم للنقر على الرابط. في حين أنه من غير الواضح عدد رسائل البريد الإلكتروني التي تم إرسالها، إلا أنه بمجرد دخول المتسللين إلى الشبكة، استهدفوا قاعدة بيانات مستخدمي Yahoo وأداة إدارة الحساب، والتي تم استخدامها لتحرير قاعدة البيانات. لسوء الحظ بالنسبة لشركة ياهو، فشلت الشركة في الكشف عن الاختراق السيبراني لعام 2014 للمستخدمين، مما أدى إلى غرامة قدرها 35 مليون دولار وسلسلة من الدعاوى القضائية الجماعية.

كيفية منع الجرائم الإلكترونية

هناك العديد من النصائح والإرشادات لحماية نفسك وبيئتك من مخاطر الجرائم الإلكترونية مثل:

- تأكد من أنك تستخدم برامج أمان محدثة مثل برامج مكافحة الفيروسات وجدران الحماية.
- قم بتنفيذ أفضل إعدادات وتطبيقات الأمان الممكنة لبيئتك.
- لا تتصفح المواقع غير الموثوقة وكن حذرًا عند تنزيل الملفات غير المعروفة، وكن حذرًا أيضًا عند عرض مرفقات البريد الإلكتروني.
- استخدم أساليب مصادقة قوية واحتفظ بكلمات المرور الخاصة بك قوية قدر الإمكان.
- لا تشارك معلومات حساسة عبر الإنترنت أو على حساباتك على وسائل التواصل الاجتماعي.
- ثقف أطفالك حول مخاطر استخدام الإنترنت واستمر في مراقبة أنشطتهم.

- كن مستعداً دائماً للقيام برد فعل فوري إذا تعرضت للجرائم الإلكترونية من خلال مراجعة الشرطة.

خاتمة البحث

إذاً الجرائم الإلكترونية هي الاستخدام غير القانوني لأي جهاز اتصال لارتكاب أو تسهيل ارتكاب أي عمل غير قانوني، ويوجد الكثير من الأشكال التي يمكن من خلالها ممارسة الجريمة الإلكترونية بدءاً من هجمات الهندسة الاجتماعية التي تعتمد على التواصل المباشر مع الضحية وخداعه بالكلام أو التصرفات وصولاً إلى الحروب الإلكترونية بين الدول وأجهزة الاستخبارات العالمية.