**¿Qué es la ciberseguridad?**

El término "ciberseguridad" se refiere a todas las salvaguardias y medidas implementadas para reducir la probabilidad de una violación de seguridad digital. La ciberseguridad afecta a todas las computadoras y dispositivos móviles en general, todos los cuales pueden ser objeto de ataques por parte de delincuentes cibernéticos. La ciberseguridad se centra en gran medida en la privacidad y la confidencialidad, así como en la integridad de los datos y la protección de la identidad. Las violaciones de seguridad en general no son algo nuevo, pero se han vuelto más frecuentes y problemáticas en la era digital actual. Cuanto más dependiente se vuelve el mundo de la tecnología conectada, mayor es la amenaza planteada por los ciberdelincuentes en todo el mundo.

Desde el daño a la reputación hasta la caída del sistema y las pérdidas financieras, los problemas de ciberseguridad pueden ser extremadamente costosos. Según un estudio reciente, casi la mitad de todas las empresas que operaban en 2017 experimentaron al menos un ciberataque o intento de violación de seguridad. Esta es precisamente la razón por la cual las empresas en todo el mundo han comenzado a priorizar la ciberseguridad, implementando sólidas medidas de protección y contratando expertos en ciberseguridad para supervisar sus operaciones.

**Importancia**

Internet ha transformado la vida cotidiana de miles de millones de personas en todo el mundo. Los volúmenes diarios de tráfico web, ya enormes, están creciendo a un ritmo exponencial. Hasta tal punto que la gran mayoría de las comunicaciones y actividades comerciales en todo el mundo dependen fundamentalmente de Internet. Desde simples compras minoristas hasta las actividades comerciales más sensibles y de alto perfil, todo ocurre en línea. Todo esto representa una oportunidad casi irresistible para los ciberdelincuentes del siglo XXI.

Ignorar la ciberseguridad ya no es una opción. Las empresas que no se protegen adecuadamente se enfrentan a la posibilidad de consecuencias catastróficas. Independientemente del tamaño, naturaleza o propósito de la empresa, los efectos de un ciberataque pueden ser devastadores. Además, algunos de los ataques más destacados en los últimos años han demostrado que incluso las empresas más grandes del mundo no siempre están tan bien protegidas como creen. Incluso cuando sus sistemas vuelven en línea y el negocio continúa como de costumbre, el daño a la reputación incurrido puede ser mucho más difícil de superar.

Por supuesto, no se trata simplemente de proteger proactivamente su empresa y sus intereses generales de los ciberataques. También es necesario pensar detenidamente en la medida en que sus clientes están protegidos. A menudo, una violación de seguridad que tiene consecuencias negativas para uno o más clientes puede ser mucho más perjudicial que un ataque a la propia empresa. Las empresas no solo tienen la expectativa de proteger a sus clientes en línea, tienen una obligación legal de hacerlo. Todo esto implica otra responsabilidad que requiere la contribución y experiencia de talentosos especialistas en ciberseguridad.

**Insiders y Outsiders**

En lo que respecta a la seguridad general de los datos, existen dos clasificaciones de personas: los insiders (internos) y los outsiders (externos) (también conocidos como empleados y no empleados). La Figura 1 muestra las tres clases de seguridad informática y los delitos causados por cada una de ellas.

**Las siete clases individuales son las siguientes:**

**1. Insiders overt (Insiders manifiestos)**: Las acciones manifiestas por parte de los insiders suelen ser obra de empleados insatisfechos, lo que a menudo resulta en el compromiso de datos y la destrucción de equipos.

**2. Insiders covert (Insiders encubiertos)**: Los empleados dentro de una empresa pueden infligir daños más graves que los outsiders debido a sus privilegios de acceso y un amplio conocimiento de la organización en general.

**3. Insiders unintended (Insiders no intencionados)**: Muchos problemas de seguridad o amenazas que ocurren internamente son el resultado de simples errores humanos genuinos. Esta es una de las clases de amenazas más comunes.

**4. Outsiders overt (Outsiders manifiestos)**: Ataques directos a sistemas de red e instalaciones informáticas por parte de outsiders, lo que también incluye ataques de denegación de servicio (DoS).

**5. Outsiders covert (Outsiders encubiertos)**: Esto se refiere al tipo de ataque que implica la transmisión de software malicioso a una o más computadoras o sistemas desde fuera del negocio.

**6. Outsiders unintended (Outsiders no intencionados)**: Es bastante raro que un outsider dañe una computadora o acceda a datos sensibles de manera no intencionada.

**7. Accidents (Accidentes):** Los problemas relacionados con la integridad o seguridad de los datos pueden surgir debido a accidentes imprevisibles que no se pueden prevenir, como desastres naturales, incendios en el lugar de trabajo, entre otros.

Existen diversas clasificaciones de problemas y amenazas de seguridad informática, aunque la gran mayoría puede agruparse bajo tres categorías principales, como se detalla a continuación:

1. Seguridad Física: Ejemplos de problemas de seguridad física incluyen el robo de equipos informáticos, el acceso físico no autorizado a sistemas informáticos y daños físicos generales causados a hardware.

**2. Software Malicioso (Rogue Software)**: Esta categoría incluye todos los ejemplos de virus informáticos y malware. Más ampliamente, cualquier software introducido en un sistema (ya sea accidentalmente o de otra manera) que represente o cree una amenaza de seguridad se considera software malicioso.

**3. Seguridad de Red**: La gran mayoría de las computadoras en la actualidad están conectadas a una o más redes, que pueden ser vulneradas por insiders (personas internas a la organización) o outsiders (personas externas). Cuando una red se accede o se compromete de alguna manera sin autorización, se considera un problema de seguridad de red.

Es sorprendente pensar que un campo tan complejo e importante como la seguridad informática prácticamente no existía hace tres décadas. La evolución de la ciberseguridad en general en los últimos años ha sido nada menos que fenomenal.

Si bien es cierto que casi cualquier vulnerabilidad o amenaza de seguridad puede gestionarse y controlarse, no existe una protección 100% infalible contra ataques. Esto se debe a que los ciberdelincuentes están constantemente perfeccionando y adaptando sus técnicas, lo que crea una especie de juego continuo de "gato y ratón" con los expertos en ciberseguridad. Ambas partes hacen todo lo posible para estar un paso por delante de la otra.

Las "10 Leyes de la Ciberseguridad de Microsoft"

Empresas líderes en software como Microsoft emplean equipos enormes de expertos en ciberseguridad para salvaguardar sus sistemas y software. A lo largo de los años, Microsoft ha publicado un extenso archivo de valiosas pautas de ciberseguridad para empresas de todas las formas y tamaños. También han producido y publicado sus propias "10 leyes de la ciberseguridad", que pueden y deben implementarse en todos los niveles de la empresa.

**Las 10 reglas establecidas por Microsoft son las siguientes**:

1. Si alguien puede persuadirte para que ejecute su programa en tu computadora, ya no es tu computadora.

2. Si alguien puede alterar el sistema operativo de tu computadora, ya no es tu computadora.

3. Si alguien tiene acceso físico sin restricciones a tu computadora, ya no es tu computadora.

4. Si permites que alguien cargue cualquier cosa en tu sitio web, ya no es tu sitio web.

5. Contraseñas débiles derrotan una seguridad fuerte.

6. Una computadora solo es tan segura como confiable sea su propietario/usuario.

7. Los datos encriptados solo son tan seguros como la clave de desencriptación.

8. Un escáner de virus desactualizado es apenas un poco mejor que no tener ninguno en absoluto.

9. El anonimato absoluto no es práctico, ni en la vida real ni en la web.

10. La tecnología no es una panacea.

**Seguridad Física**

La gran mayoría de las amenazas y ataques de ciberseguridad son de naturaleza "virtual". En otras palabras, quienes son responsables de estos ataques no obtienen acceso físico a las redes y sistemas informáticos que son su objetivo. Sin embargo, junto con virus, robo de identidad, violaciones generales de la seguridad de datos, y otros, existe otro aspecto de la ciberseguridad igual de importante que la seguridad virtual. Se trata de la protección física del equipo informático contra cualquier eventualidad. Ejemplos de estas eventualidades incluyen incendios, inundaciones, robos y daños accidentales.

**Amenazas Físicas**

Una de las amenazas físicas más comunes para la ciberseguridad es también una de las más pasadas por alto y subestimadas. Las sobretensiones eléctricas, que pueden ocurrir en cualquier momento sin previo aviso, pueden destruir eficazmente dispositivos electrónicos como computadoras en cuestión de segundos. Es por eso que los expertos en ciberseguridad consideran obligatorio el uso de protectores contra sobretensiones y fuentes de alimentación ininterrumpida. Cuanto más importante sea la computadora o el sistema de TI, mayores deben ser las medidas para protegerlos.

La seguridad física de las computadoras y los sistemas de red a menudo comienza y termina con la seguridad de la instalación en sí. Si la oficina o el lugar de negocio no están suficientemente protegidos contra el acceso no autorizado, aumenta el riesgo de robo o daño a su propiedad. Cuanto más difícil se lo ponga a los posibles delincuentes para acceder a sus computadoras y tecnología relacionada, menor será la probabilidad de convertirse en víctima de un ataque. La seguridad física de la instalación en sí también puede desempeñar un papel en la minimización de la amenaza que representan incendios, inundaciones y eventualidades impredecibles similares.

Por lo tanto, vale la pena retroceder de vez en cuando para considerar hasta qué punto están protegidos sus sistemas informáticos y tecnología relacionada. ¿Está su edificio asegurado con cerraduras impenetrables? ¿Tiene un sistema de alarma y/o vigilancia de alta calidad? ¿Ha configurado un sistema para recibir alertas automáticas en caso de acceso no autorizado? ¿Cuánto daño podría causar un empleado descontento si lograra acceder sin autorización a su edificio?

Todas estas preguntas forman parte de la evaluación esencial de riesgos de ciberseguridad, que debe realizarse de manera regular.

**Seguimiento de Usuarios**

La responsabilidad es fundamental en cada marco exitoso de ciberseguridad. En otras palabras, debe mantener un registro preciso de quién está accediendo a sus sistemas, cuándo lo están haciendo, desde dónde y qué tipo de actividades están realizando. Cuanto más siga las actividades de cada usuario, más fácil será identificar a las partes responsables en caso de un problema de ciberseguridad.

Un buen ejemplo es el de un equipo de administradores que trabajan en una clínica médica. Cada uno de estos trabajadores tendrá sus propias credenciales de inicio de sesión únicas, junto con una tarjeta que debe usarse para activar el sistema informático. A partir de ese momento, se mantiene un registro detallado de sus actividades hasta el momento en que cierran sesión. Cada página que visitan en la intranet, cada cita que reservan, cada nota que toman y cada registro al que acceden. Toda esta información se almacena de manera segura para futuros accesos y no puede ser editada ni eliminada por nadie en la instalación.

De esta manera, cualquier error u omisión identificados en una fecha posterior pueden rastrearse hasta su origen. La mayoría de los cuales, por supuesto, resultarán ser errores humanos, pero la importancia de la responsabilidad no puede ser exagerada. Estos sistemas de seguimiento de usuarios también sirven como disuasivos útiles, disuadiendo a posibles atacantes de participar en actividades maliciosas mientras están conectados. Es decir, a menos que puedan iniciar sesión utilizando las credenciales de otra persona, de ahí la importancia de contraseñas sólidas y actualizadas regularmente.

**Protección Física de Datos**

Uno de los mayores problemas con los dispositivos de almacenamiento físico de datos es que la mayoría de ellos pueden dañarse o destruirse fácilmente. Discos duros, DVD, unidades USB, y otros medios de almacenamiento físico son relativamente simples de comprometer. Tanto de manera accidental como maliciosa, estos y otros dispositivos/medios de almacenamiento físico a menudo sufren daños.

Es por eso que es de suma importancia asegurarse de que todos los datos importantes se respalden de manera regular. Los dispositivos de almacenamiento de datos en general deben considerarse frágiles e imperfectos. Debe asumirse que en cualquier momento y sin previo aviso, cualquier dispositivo dado podría ser destruido. En ese caso, estará contento de haber hecho una copia de seguridad que ahora puede utilizar en su lugar. Idealmente, los datos que respalde deben mantenerse en una ubicación separada, lejos del dispositivo de almacenamiento original. La razón es que, en caso de incendio, inundación, robo o daño accidental, no correrá el riesgo de que ambas copias se dañen o destruyan al mismo tiempo.

Hacer copias de seguridad de datos utilizando instalaciones de almacenamiento en línea es una opción, pero nuevamente no se puede confiar en ellas como infalibles. Es importante recordar que cualquier cosa que exista en el espacio virtual de la web tiene el potencial de ser comprometida en cualquier momento. Incluso si la probabilidad es mínima, aún existe. Cuando los datos son importantes y simplemente no puede arriesgarse a perderlos por completo, se deben realizar copias de seguridad físicas de manera regular y almacenarse en un lugar seguro.

**Planificación de la Recuperación**

Armado con estos respaldos actualizados regularmente, una empresa proactiva puede formular un plan efectivo de recuperación ante desastres. Su plan de recuperación debe incluir un resumen completo y detallado de qué hacer en caso de que su instalación (total o parcialmente) sea destruida o quede inoperable. La información típica contenida en un plan de recuperación puede incluir la ubicación de las copias de seguridad de datos, instrucciones para la adquisición de nuevos sistemas informáticos, las responsabilidades individuales de cada miembro de la fuerza laboral, dónde se deben establecer nuevas instalaciones físicas, y así sucesivamente.

Además de las copias de seguridad actualizadas regularmente, también puede ser útil mantener copias impresas de documentos importantes. Esto es precisamente por qué algunos de los documentos más importantes en los negocios y en la vida cotidiana aún no se han digitalizado. Contratos, facturas, recibos de compra, y otros documentos se consideran demasiado importantes como para no tener una copia impresa. De esta manera, incluso si sus sistemas principales y copias de seguridad son destruidos, aún tendrá una copia impresa con la que trabajar. Sin embargo, si mantiene copias impresas, deberá asegurarse de que estén adecuadamente protegidas y destruidas cuando ya no sean necesarias.

¿Qué es el Ciberdelito?

El término "ciberdelito" se refiere a cualquier actividad ilegal que involucre una computadora o un dispositivo conectado de cualquier tipo. Los incidentes resultantes de errores humanos o accidentes no se consideran ciberdelitos, pero aun así pueden constituir un grave riesgo de seguridad cibernética. Para que se cometa un ciberdelito, la persona debe tener el deseo expreso de llevar a cabo una o más acciones no autorizadas, que pueden tener consecuencias catastróficas para la víctima. Los ciberdelincuentes suelen llevar a cabo sus ataques por motivos de codicia, venganza o simplemente por diversión.

**Ciberdelitos por Insiders (Personas Internas) y Outsiders (Personas Externas)**

Los ciberdelincuentes pueden ser conocidos por la organización o entidad que atacan, o pueden ser un desconocido con el que nunca han tenido contacto. Como resultado, existen dos categorías distintas de ataques cibernéticos realizados por entidades criminales en todo el mundo:

**Ataque Interno**: Un ataque interno ocurre cuando una persona se involucra en alguna actividad maliciosa a través de su acceso autorizado al sistema. En la gran mayoría de los casos, los ataques internos son llevados a cabo por empleados descontentos, contratistas insatisfechos, ex empleados que aún tienen acceso a los sistemas de la organización, y otros. Los ataques internos pueden ser particularmente devastadores, ya que el usuario puede tener privilegios de acceso de alto nivel. Sin embargo, los ataques internos también son comparativamente fáciles de rastrear hasta su origen, lo que asegura que se identifique y responsabilice a las partes responsables.

**Ataque Externo**: En cambio, los ataques externos ocurren cuando cualquier persona que no tenga acceso autorizado a los sistemas de la empresa lanza un ataque. Cualquier empresa que opere computadoras y sistemas de TI conectados a Internet es técnicamente un objetivo viable para los atacantes externos en todo el mundo. La mayoría de los ataques externos son detenidos por firewalls y medidas de seguridad similares, aunque no se pueden descartar por completo. Los ataques externos están motivados predominantemente por codicia o en base a una disputa/desacuerdo con la organización en cuestión.

**Ataques Estructurados y No Estructurados**

Los ciberataques también se pueden dividir en otras dos categorías: ataques estructurados y ataques no estructurados. Esto es básicamente una referencia a la madurez y sofisticación del atacante en el momento del incidente.

**Ataque No Estructurado**:

Un ataque no estructurado generalmente es llevado a cabo por una persona con poco conocimiento y experiencia. También pueden no tener un motivo específico para el ataque o una noción de la gravedad del delito que están cometiendo. Los ataques no estructurados a menudo se realizan de manera aleatoria y, por lo tanto, pueden ser altamente impredecibles.

**Ataque Estructurado:**

La diferencia radica en que, con un ataque estructurado, el perpetrador sabe exactamente lo que está haciendo y comprende completamente las consecuencias de sus acciones. Están familiarizados con herramientas y tecnologías de piratería sofisticadas, tienen un objetivo específico en mente. Esencialmente, los ataques estructurados son realizados por criminales profesionales que saben exactamente lo que quieren y no tienen interés en las posibles consecuencias.

El atractivo del ciberdelito entre las entidades criminales en todo el mundo está en crecimiento. Esto se debe a que el ciberdelito tiene el potencial de generar enormes ganancias a través de una "empresa" de bajo riesgo y baja inversión.

No solo eso, sino que cuando los ciberdelitos son perpetrados por delincuentes de una nación lejana, es casi imposible llevarlos ante la justicia. Incluso si son identificados, la probabilidad de que sean responsables por sus acciones es baja. El creciente atractivo del ciberdelito representa uno de los muchos desafíos que enfrentan los expertos en ciberseguridad y las empresas para las que trabajan en todo el mundo.

**Troyanos**

El término "troyano" se refiere a un tipo de software malicioso o malware que se disfraza de programa legítimo para engañar a los usuarios y luego infectar sus sistemas sin su conocimiento. Los troyanos obtienen su nombre de la historia del caballo de Troya en la mitología griega, donde los griegos se escondieron dentro de un gran caballo de madera para infiltrarse en la ciudad de Troya de manera engañosa.

Los troyanos suelen realizar funciones dañinas una vez que infectan un sistema, como robar información confidencial, tomar el control de la computadora, habilitar el acceso remoto no autorizado o permitir la descarga de más malware en el sistema. Son una forma común de ataque cibernético y se propagan a menudo a través de descargas de software no confiable, correos electrónicos de phishing o sitios web comprometidos.

Lo anterior representa la estructura organizativa jerárquica típica de una empresa de ciberdelincuencia. Sin embargo, la jerarquía se mantiene en un estado constante de cambio y se basa puramente en la oportunidad. Por ejemplo, si un hacker tiene el conocimiento y la experiencia para vender datos sensibles directamente a un comprador a un precio lucrativo, es poco probable que involucre intermediarios. En cambio, si el hacker no tiene los contactos necesarios para realizar una venta, es posible que solo pueda operar como parte de una pandilla criminal.

**Motivaciones para el Ciberdelito**

Tanto la prevalencia como la magnitud de la amenaza que representa el ciberdelito han crecido exponencialmente en los últimos años. En cuanto a las motivaciones, algunas de las razones más comunes para participar en este tipo de actividades criminales incluyen las siguientes:

a. Dinero: La gran mayoría de las personas que cometen ciberdelitos están motivadas por la perspectiva de ganar mucho dinero en poco tiempo.

b. Venganza: También es común que las personas cometan ciberdelitos como forma de venganza. Un ejemplo de esto es un ex empleado descontento que lanza un ataque contra su antiguo empleador.

c. Terrorismo: Los ataques motivados por la religión o creencias personales se están volviendo cada vez más comunes, lo que puede llevar a enormes pérdidas físicas o económicas para las víctimas.

d. Diversión: A menudo no hay una motivación específica para un ataque cibernético, aparte del entretenimiento de los responsables. Simplemente quieren ver de lo que son capaces.

e. Reconocimiento: Hackear una red supuestamente impenetrable puede ser una fuente enorme de orgullo y reconocimiento para aquellos que operan en redes de ciberdelincuencia conocidas en todo el mundo.

f. Anonimato: Individuos que normalmente se abstendrían de cometer crímenes pueden participar en actividades de ciberdelito, atraídos por la perspectiva de un anonimato casi total.

g. Espionaje: Los sistemas informáticos de todo el mundo son regularmente pirateados y/o monitoreados por agencias internacionales y gobiernos, una forma de ciberespionaje.

Dado que a menudo es difícil identificar a las partes responsables de un ciberdelito, no siempre es posible determinar una motivación específica para el acto.

**Diferentes Tipos de Ciberdelitos**

A medida que los ciberdelincuentes continúan evolucionando y mejorando la sofisticación de sus ataques, se están identificando constantemente nuevos tipos de ciberdelitos. Hasta el momento, algunos de los tipos más comunes de ciberdelitos cometidos a nivel mundial son los siguientes:

Ciberacoso

El término "ciberacoso" se refiere a cualquier tipo de acoso o comportamiento amenazante perpetrado en línea. Las redes sociales en particular han proporcionado una plataforma abierta para que los ciberdelincuentes acosen a sus víctimas en línea, con poco riesgo de ser identificados o responsabilizados. Los efectos del ciberacoso en las personas que son blanco pueden ser devastadores.

Pornografía Infantil

Cualquier tipo de posesión, distribución o acceso a imágenes o videos sexuales de menores (menores de 18 años) es un delito grave.

Falsificación y Contrabando

La creciente sofisticación de la tecnología informática está facilitando más que nunca la falsificación de documentos y la creación de falsificaciones. Hasta el punto en que puede ser casi imposible diferenciar un documento falsificado de uno original, sin el uso de extensas técnicas forenses.

Piratería de Software y Delitos relacionados con los DPI (Derechos de Propiedad Intelectual)

La reproducción y/o distribución no autorizada de software se conoce como piratería de software. Las mayores compañías de software del mundo invierten mucho en el desarrollo de sólidas medidas de prevención de la piratería, pero los ciberdelincuentes sofisticados están siempre a solo un par de pasos detrás.

Ciberterrorismo

Definido como el uso de recursos informáticos para intimidar o coaccionar al gobierno, la población civil o cualquier segmento de la misma en aras de objetivos políticos o sociales.

Phishing

El término "phishing" se utiliza en referencia a cualquier intento de adquirir la información personal de una o varias partes, mediante el envío de correos electrónicos que parecen haber sido enviados desde una fuente de confianza. Ejemplos comunes de phishing incluyen correos electrónicos que se parecen casi idénticos a los enviados por eBay, Amazon y Netflix, pero que en realidad son enviados por entidades fraudulentas con el propósito de robar la información privada del destinatario. Otra forma de phishing es el "Smishing", en el cual se utilizan mensajes de texto SMS para atraer a los clientes.

Vandalismo Informático

Cualquier intento de dañar o destruir una computadora o un sistema informático, ya sea mediante software malicioso o fuerza física, se considera vandalismo informático.

**Hacking Informático**

El hacking informático ocurre cuando un individuo o un grupo obtiene acceso no autorizado a una computadora, dispositivo o sistema informático de cualquier tipo. El hacking informático puede ocurrir de forma local o remota, motivado por el deseo de robar datos sensibles, destruir la información almacenada en el sistema o simplemente hacer un punto político. Los hackers a menudo bloquean a individuos y empresas fuera de sus sistemas por completo, exigiendo pagos de rescate para "desbloquear" sus computadoras.

Existen cuatro clasificaciones principales de hackers, como se describe a continuación:

**White Hat (Sombrero Blanco):** Estos son los hackers "éticos" profesionales, contratados por empresas para encontrar problemas y vulnerabilidades en sus defensas. En lugar de participar en actividades maliciosas, simplemente señalan los tipos de problemas que podrían abrir la puerta a ciberdelincuentes. Algunos son empleados a tiempo completo por empresas, otros ofrecen sus servicios como autónomos.

**Black Hat (Sombrero Negro):** Por el contrario, el hacker de sombrero negro solo tiene intenciones criminales en mente. Pueden estar motivados por cualquiera de los factores mencionados anteriormente y no tienen en cuenta las consecuencias de quienes son blanco de sus ataques. La mayoría de los hackers de sombrero negro establecidos tienen acceso a hardware y software sofisticados, junto con los recursos físicos y virtuales necesarios para orquestar ataques ambiciosos.

**Grey Hat (Sombrero Gris):** El hacker de sombrero gris identifica vulnerabilidades de seguridad y proporciona los servicios necesarios para abordarlas, generalmente por una tarifa predeterminada.

**Blue Hat (Sombrero Azul):** Antes del lanzamiento de un nuevo sistema o una actualización de sistema, una organización puede contratar a un hacker de sombrero azul para identificar posibles problemas con anticipación. La prevención en la etapa más temprana posible es preferible a abordar problemas solo cuando se identifican en una fecha posterior.

**Crear y distribuir virus a través de Internet**

La gran mayoría de los virus informáticos no sirven para nada más que para causar problemas a quienes se ven afectados. Algunos hackers invierten incansablemente en el desarrollo de virus de vanguardia con el potencial de afectar (o causar daño a millones de sistemas informáticos en todo el mundo. Como resultado, los virus rara vez se crean o distribuyen con el propósito de ganar dinero.

**Spam**

Poco a poco, el spam se reconoce cada vez más como una forma de ciberdelito por derecho propio. Para que un mensaje se considere spam, generalmente debe formar parte de una campaña de envío masivo, ser enviado por una entidad con identidad desconocida y haber sido enviado sin el permiso expreso del destinatario. Los correos electrónicos de spam generalmente no son 'peligrosos' en sí, pero pueden ser molestos e irritantes en el mejor de los casos.

**Fraude en subastas en línea**

La popularidad de sitios de subastas en línea como eBay ha desencadenado una nueva ola de actividades fraudulentas por parte de ciberdelincuentes. En pocas palabras, se enumeran artículos en venta que o bien no existen o nunca llegarán al ganador de la subasta. En cambio, el 'vendedor' simplemente se queda con el dinero y desaparece por completo.

**Cyber Squatting (Apropiación de dominios)**

Definido como un acto de reservar los nombres de dominio de la marca registrada de otra persona, con la intención de venderlo posteriormente a la organización que es dueña de la marca registrada a un precio elevado.

**Bombas lógicas**

Una bomba lógica se define formalmente como un fragmento de código que se inserta intencionalmente en un sistema de software y se activará automáticamente cuando se cumplan ciertas condiciones. En un ejemplo de funcionamiento, un empleador puede insertar un fragmento de código en un sistema que comenzará a eliminar información y causar estragos en general si se termina su contrato.

**Secuestro de sitios web**

Esto es una forma de secuestro digital, en la que el hacker obtiene acceso a un sitio web sin autorización y posteriormente impide que su legítimo propietario lo acceda. Pueden hacerlo para exigir un rescate para desbloquear el sitio o por motivos políticos o sociales.

**Robo de Tiempo en Internet**

Hackear el nombre de usuario y la contraseña del ISP de un individuo y realizar actividades en línea a su costa se llama Robo de Tiempo en Internet.

**Ataque de Denegación de Servicio**

Un ataque de Denegación de Servicio (DoS) ocurre cuando un ciberdelincuente (o un grupo de ellos) intenta inundar un sitio web con un flujo de tráfico no deseado, creando una congestión que impide su correcto funcionamiento. Por eso a menudo es necesario marcar la casilla de 'No soy un robot' antes de obtener acceso a un sitio web.

**Suplantación de Correo Electrónico**

Esto es cuando se cambia la información del encabezado de un correo electrónico para ocultar la identidad de la fuente real, haciendo que parezca que el correo electrónico fue enviado desde una fuente que en realidad no era el remitente real.