Desde ‘Antivirus’ hasta ‘Ataque del día cero’:

20 términos de ciberseguridad que debes conocer

NordVPN®

“

La ciberseguridad abarca todo lo que hacemos online y, ahora más que nunca, nuestra vida online es nuestra vida cotidiana. Por extensión, las amenazas de ciberseguridad son amenazas a nuestros sustentos, y educarnos al respecto es esencial para proteger nuestro bienestar. Todas las personas pueden beneficiarse al entender sus conceptos esenciales, y por eso es importante que todos comprendamos el ABC de los términos de ciberseguridad.

Troy Hunt

Troy Hunt – Miembro del Consejo de NordVPN, Director Regional de Microsoft y ganador del premio al Profesional Más Valioso para el Desarrollo de la Seguridad, blogger en troyhunt.com, conferenciante internacional en materia de seguridad web, y autor de muchos cursos de seguridad de primera categoría para los desarrolladores web en Pluralsight.

Prólogo

Si estás dando tus primeros pasos en el ámbito de la ciberseguridad, este es el lugar donde comenzar. Para entender por qué, veamos cómo funcionan normalmente las cosas.

Te encuentras con la palabra ‘ spyware’, y quieres saber qué significa. En cuanto empiezas tu búsqueda, te asaltan términos que no habías visto nunca antes. Puede que te encuentres con una definición como esta:

> “El spyware es un tipo de malware que monitoriza el dispositivo de la víctima para extraer datos sensibles sin que la víctima lo sepa. Ejemplos de spyware: adware, keyloggers y troyanos”.

Esta es una definición precisa, pero no es de gran ayuda. Ahora tienes más preguntas. ¿Cómo funciona el spyware? ¿Qué se consideran datos sensibles, y hasta qué punto deberías preocuparte por su seguridad? ¿Qué es un keylogger? ¿Acaso es una palabra de verdad?

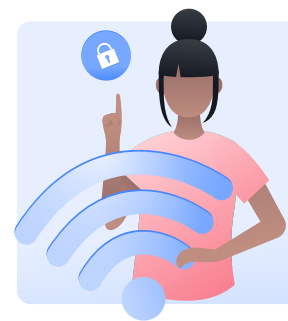
Vamos a tomar un enfoque diferente.

Más que dar definiciones técnicas, vamos a mostrarte cómo la ciberseguridad influye en tu vida, y a ofrecerte comparaciones sencillas. Este no es un glosario exhaustivo, y no pretende serlo. Está pensado para abrirte el apetito de aprender más.

Si buscas explicaciones técnicas más detalladas sobre todo lo referente a la seguridad online, visita nuestro blog en NordVPN.com/blog, donde encontrarás contenidos de interés explicados en mayor profundidad.

Tabla de contenidos:

3 Antivirus
4 Botnet
5 Texto cifrado
6 Filtración de datos
7 Encriptación de extremo a extremo
8 Firewall
9 Hacker
11 Dirección IP
12 Cryptojacking
13 Keylogger
14 Bomba lógica
15 Ataque de intermediario
16 Network
17 Phishing
18 Ransomware
19 Ingeniería social
21 Verificación en dos pasos
22 VPN
23 Wi-Fi
24 Ataque del día cero



A

Antivirus

Recibes un nuevo correo electrónico. Asunto: **Te quiero.**

En él, encuentras una preciosa confesión de amor de alguien que te admira desde el anonimato. Y también hay una foto. Sientes curiosidad, haces clic en el archivo adjunto... y descargas un virus.

Tu antivirus lo pone en cuarentena de inmediato. Has tenido suerte: era un virus antiguo, y su firma ya estaba en la base de datos.

Si el virus es nuevo y no está registrado en la base de datos, el antivirus dispone de otras herramientas para detectarlo. Tu antivirus siempre analiza tu equipo en busca de actividad sospechosa. Si un programa trata de saltarse esta monitorización, se ejecuta en el arranque de tu equipo sin tu permiso o descarga otras formas de malware, el antivirus reacciona.

Y no solo se trata de virus. Hay toda clase de programas maliciosos como troyanos, ransomware, keyloggers, etc., que pueden tratar de comprometer tus dispositivos o aprovecharse de ellos.

En la actualidad, la palabra 'antivirus' define a una amplia variedad de herramientas anti-malware que protegen a tu dispositivo frente al malware.

Términos relacionados vírus, malware, software anti-malware, troyano, gusano, adware.

B

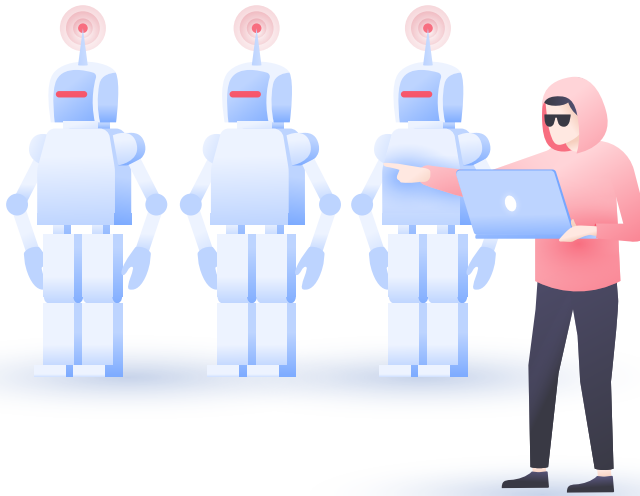
Botnet

Abres tu navegador, introduces la dirección de tu web favorita para ver memes. Oooh, está caída. Y nunca sabrás por qué.
Son los zombis.

Bots, para ser exactos. Un enjambre de dispositivos infectados, sin mente, han enviado cientos de miles de peticiones a la web y la han saturado.

Este ataque se denomina DDoS, que significa 'denegación del servicio'. Hay personas que usan botnets para este y otros propósitos maliciosos, como enviar spam por correo electrónico o crear tráfico de internet falso.

Tus dispositivos quizá sean parte de una botnet y respondan en secreto a las órdenes de un cibercriminal. Es difícil de saber si tu equipo es un bot: el único indicio puede ser un rendimiento ligeramente peor, o su sobrecalentamiento.



Términos relacionados: bot, zumbie, ataque DDoS.

C

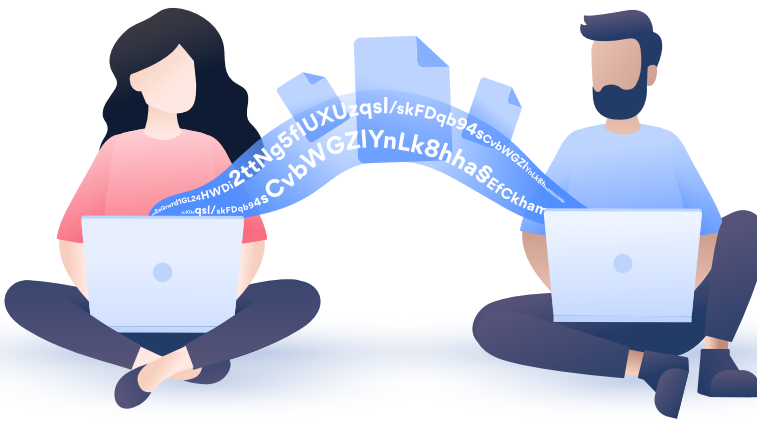
Texto Cifrado

Abres una app de mensajería y escribes “LO SIENTO, no voy a poder ir esta noche. Estoy un poco mal del estómago”.

Esto se llama ‘texto plano’. Es un texto sin encriptar que puede ser interceptado y leído por un espia online. También se llama ‘mentira’: te sientes bien, pero prefieres quedarte en casa y ver una película. Al menos, estás usando una app de mensajería segura. Esta app aplica un algoritmo para transformar tu mentira en un texto cifrado:

“ueEeQrwrd1GL24HWDi2ttNg5fIUXUzqsIFqb94^Ef2NU1NBrD
rPb84wbReVnclTP2AgnMCkhaHC3UrfR8VWxh3jWWh+0WE”

Aquí tienes la encriptación en acción. El texto plano se transforma en texto cifrado mediante una clave segura (un código). Las apps de mensajería que usan tus amigos tienen la clave que descifra tus mensajes. Los espías online no la tienen, así que no pueden leer tus comunicaciones.



Términos relacionados: encriptación, código, texto plano, descifrar

D

Filtración de datos

Tienes un grupo de chat con un montón de tus amigos cercanos. Un día, descubres capturas de pantalla del chat en todas las redes sociales. Has sufrido una filtración de datos. Una filtración de datos ocurre cuando datos sensibles caen en manos de alguien que no debería tener acceso a ellos.

¿Cómo ha ocurrido esto? ¿Un hacker ha interceptado tus comunicaciones? ¿O ha sido una filtración interna? Quizá el compañero de piso de Marc accedió al chat mientras Marc estaba en el baño. Él siempre pareció sospechoso. Probablemente nunca lo descubras.

Esto es lo que ocurre también con las filtraciones de datos de las grandes empresas.

Las empresas reúnen grandes cantidades de datos —a veces, datos de usuarios como tú—, y algunas de estas empresas sufren filtraciones, los datos se hacen públicos, y entonces ves tus nombres de usuario y contraseñas dando vueltas por la web.

Comprueba periódicamente cuáles de tus cuentas han sufrido filtraciones de datos en haveibeenpwned.com.

Términos relacionados: facilitación no intencional de información, escape de datos, vulneración de datos.

E

Encriptación de extremo a extremo

Lo has oído decir en tono de broma: "¡Vamos a implementar una encriptación de extremo a extremo!". ¿Qué es tan extremo sobre ella? La encriptación de extremo a extremo elimina al intermediario. Solo tú y la persona a la que le estás enviando tu mensaje pueden ver su contenido.Imagina que tus datos son una nota de papel. Antes de enviarla, la pones en un sobre que protege su contenido ante los curiosos. Eso es la encriptación.

En algún punto del camino, un tercero (por ejemplo, el servicio de mensajería que usas) abre ese sobre, extrae tus datos y los envía a su destinatario final. Simplemente, internet funciona así: hay intermediarios por todas partes.

La encriptación de extremo a extremo elimina al intermediario. Solo tú y la persona a la que le envías la nota pueden ver su contenido.

Términos relacionados: texto cifrado, texto plano.

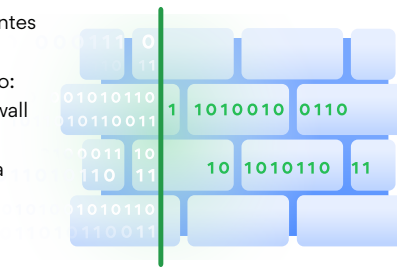
F

Firewall

Estás en una cola. Cuando llegas hasta el portero, te dice: “No puedes entrar”. Te das la vuelta y te marchas a casa. No habrá discoteca hoy.

El portero aplica la regla de quién puede entrar en la discoteca y quién no. Estas reglas son arbitrarias: dependen de las normas de la discoteca y de circunstancias externas. Por ejemplo, quizá el club esté lleno, o se esté celebrando una fiesta privada.

De la misma forma, un firewall se alza entre tu red local e internet. Como un portero digital, aplica la norma de qué tráfico es lo bastante bueno para acceder a tu red. Un firewall permite el tráfico de fuentes o direcciones IP confiables. ¿No estás en la lista? Lo siento, tráfico: vete a casa. Así es como un firewall protege tu red frente al tráfico malicioso de internet que podría comprometer tu sistema.



H

Hacker

Los has visto en las películas. Son misteriosos, antisociales, incluso peligrosos. Son los forajidos digitales que viven al margen de las normas. Hackean el Pentágono en menos de 5 minutos.

Así ocurre en la ficción, claro. Los hackers son personas, y cada persona tiene sus motivos. A algunos les gusta el desafío intelectual de acceder a redes. Otros, los llamados hackers de guante negro, actúan con malicia. Comprometen sistemas para su propio beneficio, roban datos valiosos o dinero, interfieren en las redes y causan toda clase de daños.

Muchas empresas y gobiernos contratan a hackers de guante blanco para que traten de acceder a sus sistemas para comprobar su seguridad. Esto se denomina test de penetración, y puede tener muchas formas: incluso físicas.

Por ejemplo, un hacker de guante blanco puede entrar en el edificio de una empresa siguiendo a un empleado. Las personas son educadas y normalmente sostienen la puerta abierta para otros, incluso para los desconocidos. Una vez dentro, el hacker puede robar discos duros con datos sensibles, acceder a equipos informáticos sin supervisión, o comprometerlos (por ejemplo con keyloggers).

¿Pueden hackearte a ti?

Depende de tus medidas de seguridad. Sin embargo, los hackers extremadamente habilidosos suelen encontrar una forma de acceder incluso a las redes más seguras. La buena noticia es que probablemente estén interesados en objetivos más apetecibles que tu cuenta de Steam.

Normalmente sufrirás hackeos indirectos: por ejemplo, filtraciones de datos.

Más bien deberías tomar precauciones ante los estafadores que crean webs falsas o envían enlaces maliciosos, es decir, ante el phishing. Si introduces tu contraseña en una web falsa, se la estarás dando directamente a un estafador.

Términos relacionados: hacker de guante gris, hacker de guante negro, hacker de guante blanco, penetración, test de penetración.

Dirección IP

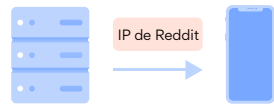
Tu teléfono tiene una dirección IP (abreviatura de Protocolo de Internet) asignada por tu red. Lo mismo ocurre con tu portátil, tu Smart TV y cualquier otro gadget que se conecte a internet. Ningún dispositivo puede funcionar online sin contar con una. ¿Por qué?

Digamos que quieres entretenerte un rato. Sacas tu teléfono y escribes 'Reddit.com' en la barra de direcciones.

Pero tu teléfono no sabe lo que significa 'Reddit.com'. Su idioma nativo está compuesto por números, no por palabras. Para acceder a Reddit, tu teléfono envía una pregunta: "¿Cuál es la dirección IP de Reddit.com?".

¿Cuál es la dirección IP de Reddit.com?

Esta pregunta es remitida a un servidor especial: una base de datos de direcciones IP. El servidor encuentra la dirección IP de Reddit y se la envía a tu teléfono.



Solicitud

Tu teléfono entonces envía una solicitud a la dirección IP de Reddit. Y Reddit envía la información de vuelta a la IP de tu teléfono.

Información de la IP de Reddit

Pasa un segundo, y Reddit aparece en tu pantalla. Meh, hoy no encuentras nada interesante, así que le das al botón de 'cerrar'.

J

Cryptojacking

Tu equipo está caliente y zumba, el ventilador está girando como un loco. Pero funciona muy despacio. Tienes que esperar mucho para que cargue cualquier cosa.

¿La razón? Un hacker ha secuestrado tu equipo para minar criptomone-das.

Probablemente has oído hablar del minado de criptomonedas. Para explicarlo de forma sencilla, es cuando recibes criptomonedas como recompensa por realizar cálculos complejos en tu dispositivo. Pero estos cálculos necesitan de mucha potencia computacional: normalmente, demasiada potencia como para que resulte rentable hacerlo.

Para resolver este problema, los hackers secuestran dispositivos y los hacen minar criptomonedas para ellos. Realizan este ataque —llamado cryptojacking— utilizando malware o códigos maliciosos en páginas webs. Las víctimas quedan preguntándose por qué su equipo se sobrecalienta tanto.

P.S. Sí, sabemos que poner cryptoJacking en la letra J es hacer trampas. Pero la letra J es un desierto en términos de ciberseguridad, así que teníamos que aprovechar.

Términos relacionados: criptominado, criptominado malicioso.

K

Keylogger

Estás en la biblioteca escribiendo un ensayo para tu clase de economía. Lo tenías que haber entregado ayer. La batería de tu portátil se agota, y te has dejado el cargador en casa.

Una chica de aspecto amistoso está sentada cerca.

Le pides prestado su portátil: sólo necesitas 5 minutos para terminar de escribir tu idea mientras aún te sigue rondando la cabeza. Ella acepta ayudarte. Tomas su portátil, accedes a tu nube y terminas tu crítica sobre las leyes antimonopolio durante la era de la Gran Depresión.

Cuando vuelves a casa, descubres que tu correo electrónico y muchas de tus cuentas online han sido hackeadas. ¿Cómo?

La chica tenía un keylogger instalado en su portátil. Se trata de una herramienta que registra las pulsaciones de las teclas. Grabó todo lo que habías escrito, incluyendo el nombre de usuario y la clave de tu almacenamiento en la nube.

Como usas la misma contraseña para tu nube y tu correo, un hacker accedió a tu cuenta de correo primaria (por eso no deberías reutilizar las contraseñas). Y, desde allí, pudo resetear las contraseñas de tus otras cuentas.

Los keyloggers no suelen provenir de chicas de apariencia amistosa. Normalmente tienen forma de dispositivos de hardware que los hackers conectan a ordenadores sin supervisión. También pueden ser herramientas de software usadas de forma legal o ilegal. Por ejemplo, algunas empresas instalan keyloggers en sus equipos para monitorizar a sus empleados.

Términos relacionados: spyware.

L

Bomba lógica

Estás en el trabajo, y han pasado cinco minutos de la hora de una entrega. Estás tecleando rápidamente, pero entonces todo se desconecta. Ya no puedes acceder a la red interna ni a ningún archivo remoto. Hoy no habrá más trabajo.

Al día siguiente oyes rumores. Fue un antiguo empleado, un informático disgustado: él desactivó la red interna. ¿Pero cómo puede ser? A él lo echaron hace medio año, y no ha tenido acceso a los sistemas de la empresa desde entonces.

Bueno, en su último día de trabajo, dejó una bomba lógica. Se trata de una pieza de código malicioso que se activa cuando se cumplen ciertas condiciones. Por ejemplo, cuando el CEO accede a un sistema sensible. Una bomba lógica puede activarse en una fecha específica, como ocurrió en nuestra historia, cuando explotó medio año después de quedar establecida.

Términos relacionados: bomba lógica, amenaza interna

M

Ataque de intermediario

Estás en una cafetería, usando su Wi-Fi pública. Has enviado un correo electrónico a tu contratista pidiéndole su número de cuenta bancaria. Te da su número, realizas tu pago, te bebes tu café con leche.

Dos días después, el contratista te llama y te pregunta: "¿Cuándo recibiré el pago?"

¿Qué?

Volvamos a la cafetería. Un hacker llegó a la cafetería antes que tú, estableció un hotspot malvado y lo llamó "Cafetería Wi-Fi Gratis". Al creer que era una red legítima, tú te conectaste a su hotspot. Desde ese momento, el hacker pudo monitorizar tu tráfico de internet.

Eso es un ataque de intermediario.

El hacker interceptó tu correo y te envió su propio número de cuenta bancaria. Él recibió tu dinero, mientras que el contratista sigue esperando su pago.

Ten presente que las redes Wi-Fi públicas nunca son seguras. Incluso si no han sido establecidas por un hacker, nunca sabes hasta qué punto están bien configuradas. Alguien podría estar rodando en medio de tus comunicaciones. Asegúrate de que usas una VPN antes de conectarte a una.

Términos relacionados: ataque del gemelo malvado, jarro de miel de Wi-Fi

N

Network

Tus dispositivos son parte de una red, que es parte de una red mayor, que es parte de una red todavía mayor, que... ya pillas la idea. Eso es internet, una red de redes informáticas, grandes y pequeñas. Y tú estás en ella.

La red más cercana a ti se llama LAN: red de área local. Se refiere a un grupo de dispositivos interconectados en una ubicación física. Así que, cuando te conectas al router de tu casa, te estás conectando a tu LAN.

La red de tu casa probablemente es bastante pequeña, de unos 10 dispositivos conectados (o, si te encantan los gadgets, posiblemente algunos más, pero no te juzgamos por eso: ¡la tecnología es genial!). Una LAN también puede tener el tamaño de una empresa, o abarcar toda una escuela con miles de dispositivos interconectados.

Términos relacionados: internet, LAN.

P

Phishing

Recibes un correo electrónico de tu banco. Es un aviso: alguien ha tratado de retirar dinero de tu cuenta. “Por favor, envíe su nombre de usuario y contraseña INMEDIATAMENTE para confirmar su identidad”, dice el banco.

Suena espeluznante, pero no deberías responder a este miedo.

Comprueba el remitente con atención, y probablemente te darás cuenta de que no se trata de tu banco, sino de alguien que se está haciendo pasar por él. No respondas, y no hagas clic en ningún enlace del correo. Llama directamente a tu banco y pregúntales por este mensaje.

Esta estafa se denomina phishing, y puede adoptar muchas formas. Mensajes o correos que usan el miedo y la urgencia para obtener detalles confidenciales. Una web falsa que se ve casi idéntica a la de tu universidad. Si introduces tu nombre de usuario y contraseña en ella, se los estarás dando a un estafador.

La forma de defenderte es simple: ten cuidado. Presta atención a los mensajes sospechosos que juegan con tus miedos, o, todavía peor, que te prometen algo demasiado bueno para ser cierto. Solo tienes que hacer clique aquí para recibirlo.

Detente, piensa, y revisa. No hagas clic en un enlace si la URL no parece legítima. Como regla general, nunca introduzcas ni facilites tu contraseña salvo que tengas la completa certeza de que se trata de un sitio seguro.

R

Ransomware

Enciendes tu ordenador y... espera, ¿qué es esto? La pantalla no carga. Pero hay un mensaje: “Tus archivos han sido encriptados por el Grupo Hacker NarutoRun. Tienes una semana para transferir 500 dólares en Bitcoin a nuestra billetera, o tus archivos habrán desaparecido para siempre. ¡Rasengan!”.

Suena como una trama de una comedia pobremente escrita, pero no es algo para reírse. El ransomware es un tipo de malware que encripta a la fuerza los datos de su víctima. Nadie, salvo los hackers, puede deshacer la encriptación, porque solo ellos tienen la clave. (Hay muchos protocolos de encriptación que son prácticamente irrompibles sin la clave que los desencripta: ve a ‘texto cifrado’ y a ‘encriptación de extremo a extremo’.)

No deberías pagar la fianza porque tus dólares (o, más probablemente, tus criptomonedas, que es lo que los hackers suelen pedir) ayudarían a financiar a criminales. En lugar de esto, aprende a combatir el ransomware:

- No descargues nada desde webs sospechosas. No abras enlaces, correos electrónicos o mensajes extraños. Ver: phishing.
- Haz regularmente una copia de seguridad de tus archivos más sensibles.
- Actualiza tus apps y tu software, sobre todo tu software de seguridad.
- Usa contraseñas robustas.

S

Ingeniería social

Tu teléfono te despierta a primera hora de la mañana. La persona que te llama te explica cordialmente que es un técnico de LiteNet, tu proveedor de servicios de internet. Han tenido un problema en la red que puede haberles causado una pequeña pérdida de datos.

¿Podrías facilitarle los últimos cuatro dígitos de tu tarjeta de crédito, para que puedan comprobar si se corresponde con los registros de su servidor?

Cómo estás medio dormido, lo haces y continúas durmiendo. Te despiertas del todo dos horas después, desayunas y descubres que te han hackeado.

La persona que te llamó no era un técnico, sino un ingeniero social: un estafador que usa la manipulación psicológica para que hagas una acción específica o reveles detalles sensibles.

Repasémoslo paso a paso. El estafador te pilló temprano en la mañana, se presentó para aliviar tus sospechas (LiteNet es el principal proveedor de la zona, era fácil de adivinar) y te soltó algo de jerga técnica para parecer legítimo.

Luego llamó a LiteNet haciéndose pasar por ti, y dijo que había olvidado su contraseña. Proporcionó los últimos cuatro dígitos de tu tarjeta de crédito para confirmar su identidad (es decir, tu identidad) y reseteó tu contraseña de LiteNet, incluyendo la de tu correo electrónico de LiteNet.

LiteNet es un proveedor de internet falso que hemos creado para esta historia. Pero muchas empresas reales pueden resetear tus contraseñas por teléfono basándose solo en los últimos cuatro dígitos de tu tarjeta de crédito. Deberías dar solo la mínima información sensible posible al suscribirte, y no facilitar nunca ningún detalle por teléfono.

Los ingenieros sociales utilizan muchas técnicas diferentes para manipular a los usuarios: algunas muy sofisticadas, y otras más básicas. Un estafador puede enviar mil correos falsos para encontrar unas pocas víctimas lo bastante inocentes como para responder facilitando sus contraseñas o la información de su tarjeta de crédito.
Ver también: phishing.

T

Verificación en dos pasos

Intentas acceder a Twitter desde el teléfono de tu amigo, porque te has dejado el tuyo en casa. Como es un nuevo dispositivo, debes confirmar tu acceso en una app especial de verificación. Que está en tu teléfono. Que está en casa.

¡Aargh, es lo peor de la ciberseguridad!

Sí, puede que te cause algún inconveniente, pero la verificación en dos pasos (2FA) te protege con una segunda capa de seguridad. Si tienes problemas para acceder a tu cuenta sin tu teléfono, también los tendrán los hackers.

Los dos factores suelen ser:

Algo que sabes tú (una contraseña o un código pin). O algo que tienes (un teléfono, un libro de claves, o tu biométrica).

Ningún sistema es impenetrable, pero la 2FA mejora la seguridad de tus cuentas a un nivel superior al de la mayoría de los usuarios. Los ciberdelincuentes suelen ser oportunistas, así que, en lugar de tratar de superar tu 2FA, buscarán objetivos más sencillos, preferiblemente alguien que use ABCDEFG como su contraseña.

Deberías activar la 2FA en todos los servicios que cuenten con ella. Es una forma sencilla para estar mucho más seguro online, a cambio de una incomodidad mínima.

Términos relacionados: autentificación en dos pasos.

V

VPN

Navegas, haces scroll, surfeas. Y, siempre que estás online, dejas un rastro de datos sobre ti. Tu proveedor de servicios de internet tiene acceso a tu tráfico online. Todas las webs que visitas pueden ver tu dirección IP.

No se trata solo de tu privacidad: tu seguridad online también está en juego. Muchas webs siguen sin usar un protocolo de comunicación seguro. Muchas apps no explican qué clases de prácticas de ciberseguridad utilizan. Solo puedes confiar en ellas, sin tener motivos reales para hacerlo.

Una VPN (red privada virtual) es una herramienta que redirige todo tu tráfico a través de un servidor seguro, lo encripta en el proceso, y cambia tu IP y tu ubicación virtual. Aunque puede sonar muy técnico, una VPN es una herramienta popular que es muy accesible para cualquiera.

Esto no significa que todas las VPNs sean igualmente buenas. Una VPN redirige todo tu tráfico a través de sus servidores, así que puede reunir tus datos y venderlos al mejor postor. La buena noticia es que la mayoría de las grandes VPNs son transparentes en cuanto a sus prácticas, no mantienen registros de los datos de sus usuarios, y no venden ni revelan ninguna información a terceros.

Por ejemplo, en NordVPN tenemos una política de cero registros, y nuestros servicios son auditados regularmente auditados regularmente por una de las cuatro principales empresas especializadas.

Términos relacionados: bomba de tiempo, amenaza interna.

W

Wi-Fi

Estás en la habitación de tu hotel usando Wi-Fi gratuito. Varios pisos más abajo, un hacker está espiando tu actividad online. ¿Cómo?

El Wi-Fi público es poco seguro de forma inherente: los ciberdelincuentes pueden usar muchos métodos para aprovecharlo o comprometerlo.

Si el router está mal configurado, un hacker puede observar el tráfico de internet de cualquiera que lo utilice. O puede encontrar la forma de introducir malware en la red y en tu dispositivo.

Un hacker puede configurar un hotspot falso —un gemelo malvado— y engañarte para que te conectes a él. Ver también: ataque de intermediario.

Tu seguridad dependerá de:

La configuración y las medidas de seguridad en el Wi-Fi del hotel. Las prácticas de seguridad de las webs que visites y de las apps que uses. Tus prácticas personales de ciberseguridad.

Normalmente no puedes saber hasta qué punto es segura una red pública, así que evita acceder a datos sensibles cuando te conectes a ellas. ¿Por qué no usar tus datos móviles en su lugar? ¿O activar una VPN?

P.S. Si estás organizando un evento, no dependas del Wi-Fi proporcionado por el recinto, porque raramente es seguro. Establecer adecuadamente una red Wi-Fi no es sencillo, y requiere de un conocimiento técnico preciso. Si no tienes las habilidades técnicas necesarias, es mejor que contrates a profesionales.

Pero tu trabajo es igual de importante. ¡Necesitas comunicarte! Informa a las personas asistentes al evento sobre cuáles son las redes oficiales, y avísales de que no se conecten a ninguna otra, incluso si parecen legítimas.

Términos relacionados: inyección de malware, sniffing de Wi-Fi.

Z

Ataque del día cero

Has actualizado tu software, has instalado un antivirus, has activado tu firewall. En este momento, ningún hacker podría acceder a tu sistema, ¿verdad?

Si tan solo fuera tan simple.

Las redes informáticas, el software y el hardware son creados por personas. Las personas cometen errores, no piensan en todos los posibles escenarios, dejan vulnerabilidades.

Los hackers explotan esto. Buscan los puntos más débiles del sistema, y los rompen.En cuanto se descubre una vulnerabilidad, se parchea. Las actualizaciones que instalas para tus apps o sistemas operativos suelen ser simplemente eso: parches para vulnerabilidades que han sido recientemente descubiertas.

(Por supuesto, algunas vulnerabilidades nunca pueden parchearse. Las personas, y no las máquinas, suelen ser el punto más débil en materia de ciberseguridad. Ver: ingeniería social).

Una vulnerabilidad del día cero no es conocida por el fabricante, así que no ha sido parcheada. El nombre hace referencia al número de días que el fabricante ha tenido para solucionar la vulnerabilidad: cero. Un ataque basado en esta vulnerabilidad se denomina ataque del día cero o explotación del día cero.

Así que, incluso si mantienes tu sistema asegurado, parcheado y actualizado, una actualización del día cero puede comprometerlo a través de una vulnerabilidad anteriormente desconocida. La solución es la vigilancia constante. Muévete con inteligencia cuando estés online, utiliza contraseñas robustas, no hagas clic en enlaces si no tienes la certeza de que son seguros.

De esta forma minimizarás tus riesgos y harás que los ciberdelincuentes busquen objetivos más fáciles.

Términos relacionados: vulnerabilidad del día cero, ataque del día cero.