Día de una Internet más segura: los expertos en ciberseguridad opinan

Expertos en ciberseguridad de toda la industria han analizado cómo podemos utilizar Internet de una manera más segura, tanto a nivel profesional como personal, en una era de crecientes ataques y nuevos vectores de ataque.

por Guru Writer 6 de febrero de 2024 en Características

Día de una Internet más segura: los expertos en ciberseguridad opinan

Compartir en Facebook

Compartir en Twitter

¡Feliz Día de una Internet más segura a todos los que lo celebran! Expertos en ciberseguridad de toda la industria han analizado cómo podemos utilizar Internet de una manera más segura, tanto a nivel profesional como personal, en una era de crecientes ataques y nuevos vectores de ataque. Una cosa es segura: nuestros expertos dicen que la IA y los deepfakes dominarán las preocupaciones en Internet en 2024. MFA y la importancia de una buena seguridad de las contraseñas siguen siendo un buen punto de partida en lo que respecta a la seguridad en línea.

Chris Dimitriadis, director de estrategia global de ISACA, dice:

“El Día de una Internet más segura tiene como objetivo crear conciencia sobre una Internet mejor y más segura para todos. En un mundo en constante transformación digital, la Inteligencia Artificial (IA) será parte del trabajo que la fuerza laboral del futuro realizará y, en última instancia, formará parte de nuestra vida cotidiana.

“Además de aprender a aprovechar sus beneficios, los usuarios deben ser conscientes de sus riesgos y aprender a mitigarlos. Por ejemplo, a medida que la IA se vuelve más sofisticada, los malos actores pueden utilizarla para poner en peligro a los usuarios de Internet.

“Los reguladores de todo el mundo están tomando la iniciativa para establecer nuevas reglas en esta dirección (por ejemplo, desde EE. UU. hasta la UE y el Reino Unido), diseñando leyes para proteger a los usuarios de contenido malicioso e ilegal. Es alentador que los gobiernos estén a la vanguardia cuando se trata de mantener Internet seguro, pero la legislación sólo puede llegar hasta cierto punto: necesitamos personas calificadas y con experiencia para implementar los cambios regulatorios. Las empresas deben dotar a su personal de formación y habilidades para utilizar, gestionar y comprender datos para evitar que los descubran infringiendo la ley. De esta manera, los usuarios pueden sentirse capacitados para utilizar Internet de una manera más segura, ahora y en el futuro”.

Nick Rago, CTO de campo de Salt Security, dice:

“A medida que la digitalización se infiltra en casi todos los aspectos de nuestras vidas, Internet ha cambiado irrevocablemente la forma en que accedemos a cosas como servicios financieros, educativos o médicos, compramos bienes o realizamos nuestro trabajo diario. Y en el centro de garantizar que estos sistemas puedan comunicarse entre sí, acceder a información pertinente o realizar transacciones sin problemas se encuentran las interfaces de programación de aplicaciones (API). El uso de API, los proverbiales componentes básicos de la Internet moderna, se ha disparado en los últimos años, y algunos expertos incluso sugieren que el mercado de API crecerá más que toda la economía del Reino Unido para 2027.

En este Día de una Internet más segura, se debe recordar a las organizaciones que los atacantes buscan cada vez más aprovechar las inseguridades de las API para violar bases de datos, robar información y causar ramificaciones financieras considerables al abusar de las API. Como parte tan crucial de lo que constituye Internet y cómo la usamos, las empresas que buscan innovar mediante la digitalización de servicios y procesos internos deben evaluar el riesgo que plantean las API y asegurarse de que se gobiernen adecuadamente”.

Darren Guccione, director ejecutivo y cofundador de Keeper Security, añade:

“Una Internet fundamentalmente “segura” simplemente no es factible con el aluvión de amenazas que enfrentan las personas y las organizaciones en el mundo actual. En un nuevo estudio realizado por Keeper Security, el 92% de los líderes de seguridad de TI encuestados revelan que los ciberataques son más frecuentes ahora que hace un año y cada vez son más sofisticados. Los ataques impulsados por IA, los deepfakes, el cloud jacking y los ataques sin archivos encabezan la lista de vectores de ataque emergentes contra los que se sienten menos preparados para defenderse.

Aunque Internet en sí siempre planteará riesgos, las organizaciones pueden estar seguras en línea desarrollando un enfoque proactivo de la ciberseguridad, combinando mecanismos de defensa avanzados y mejores prácticas básicas para mitigar y combatir los vectores de ataque existentes y las amenazas crecientes. Los pasos específicos incluyen:

Aprovechar contraseñas seguras y únicas para cada cuenta y permitir una autenticación multifactor (MFA) sólida. El robo de credenciales ha sido durante mucho tiempo una de las principales causas de infracciones y ciberataques. Es esencial utilizar un administrador de contraseñas para crear contraseñas aleatorias de alta seguridad para cada sitio web, aplicación y sistema.

Tener mucha precaución al abrir archivos adjuntos de correo electrónico y hacer clic en hipervínculos. Los malos actores utilizan cada vez más la IA generativa para crear correos electrónicos y URL de phishing realistas para sitios web falsificados y generan variantes lo más rápido posible para eludir los detectores de spam.

Implementación de una solución de gestión de acceso privilegiado (PAM). PAM ayuda a los administradores de TI y al personal de seguridad a administrar y proteger credenciales privilegiadas y garantizar el acceso con privilegios mínimos. Esto, combinado con un acceso y una actividad estrechamente monitoreados, puede reducir en gran medida los riesgos cibernéticos. En caso de que un ciberdelincuente pueda acceder a una organización En las redes de la explosión, PAM puede minimizar el radio de la explosión evitando el movimiento lateral".

Camellia Chan, directora ejecutiva y cofundadora de Flexxon:

"En el Día de una Internet Segura, es vital comprender los cambios transformadores en la tecnología y cómo esto afecta la seguridad en línea. En particular, las herramientas de IA generativa como ChatGPT, DALL-E y Bard han ganado popularidad y se han arraigado en la vida cotidiana. Sin embargo, si bien han impulsado la creatividad y la productividad, no han sido adoptadas simplemente por quienes tienen buenas intenciones.

Las herramientas de IA de generación han bajado considerablemente el listón para los ciberdelincuentes. No es necesario ser un codificador técnico experto ni un experto en palabras para producir correos electrónicos de phishing que parezcan auténticos. De hecho, existe una herramienta tipo ChatGPT para ciberdelincuentes (WormGPT), lo que significa que los delincuentes pueden ejecutar campañas de forma sencilla y económica.

En consecuencia, la gente tiene que estar aún más atenta a posibles correos electrónicos poco fiables, ya que las tradicionales señales de alerta a las que hay que prestar atención (errores ortográficos y mala gramática) no existen. Cuanto más difícil sea reconocer los correos electrónicos de phishing, más empresas serán víctimas de ciberataques como el ransomware, por lo que deben buscar ampliar las posturas de ciberseguridad para incluir la seguridad del hardware. De esa manera, cuando la línea de defensa humana inevitablemente falla y los ataques avanzados logran superar las soluciones basadas en software, los datos están protegidos desde cero".

Steve Bradford, vicepresidente sénior de EMEA, SailPoint, dice:

"El Día de una Internet Segura sirve como recordatorio para todos nosotros (jóvenes, mayores, estudiantes, expertos, empleados) de que debemos permanecer alerta en línea. Los ciberdelincuentes se están volviendo más sofisticados y aprovechan la inteligencia artificial para

hacerse pasar por figuras confiables mediante phishing o deepfakes, y hacer que los sitios web o correos electrónicos falsos parezcan aún más convincentes.

Un consejo para mantenerse seguro en Internet es darle la misma importancia a su identidad digital que a su identidad personal: no entregaría información confidencial a un extraño, por lo que se debe aplicar el mismo espíritu en línea.

Considere siempre formas de bloquear digitalmente su cuenta y observe cualquier interacción en línea con ojo escéptico. Procesos como la autenticación multifactor, códigos de acceso de un solo uso de los bancos para autorizar transacciones más grandes y contraseñas de inicio de sesión complejas y únicas para cada cuenta son cruciales para mantener la seguridad de la identidad.

Además, a nivel empresarial, las empresas necesitan capacitar al personal para reconocer solicitudes sospechosas o fuera de lo común. Por eso, ya sea dentro o fuera de la oficina, en el correo electrónico o en los sitios de redes sociales, siempre aplicamos las mejores prácticas y nos mantenemos alerta ante las amenazas cibernéticas".

Niall McConachie, director regional (Reino Unido e Irlanda) de Yubico, dice:

"El Día de una Internet más segura es una oportunidad ideal para crear conciencia sobre la necesidad de mejores prácticas de ciberseguridad. Según una encuesta de 2023 realizada por Yubico y OnePoll, la Generación Z ha adoptado peores hábitos cibernéticos que los Boomers, lo que pone sus cuentas en línea en un riesgo significativo de sufrir ataques cibernéticos. A pesar de esto, la encuesta encontró que el 90 por ciento de los encuestados de la Generación Z están preocupados por la ciberseguridad de sus cuentas en línea y, si bien una mayor concientización es un gran primer paso, se necesita un cambio para mantenerse a salvo de cada vez más ataques cibernéticos como el phishing.

El primer paso es mejorar las prácticas básicas de higiene cibernética; por ejemplo, la encuesta encontró que es más probable que la Generación Z use la misma contraseña para varias cuentas en comparación con los Boomers. Aunque las políticas que exigen que las contraseñas sean cada vez más complejas y se actualicen con más frecuencia han exigido más tiempo y memoria de los usuarios, las contraseñas simples se adivinan fácilmente. Una vez robada una contraseña, los ciberdelincuentes pueden eludir con éxito otros métodos de inicio de sesión, como un código enviado por mensaje de texto. Una forma efectiva de abordar esto es con tecnología moderna sin contraseña, como la autenticación de clave de acceso basada en hardware resistente al phishing, como las claves de seguridad.

La mayoría de las veces, la Generación Z puede adaptarse fácilmente a las nuevas tecnologías, lo que significa que tecnologías como las llaves de seguridad de hardware podrían ser un gran paso adelante para garantizar la seguridad en línea. A diferencia de las contraseñas, las claves de acceso se almacenan físicamente en los dispositivos de los usuarios, como teléfonos, computadoras o llaves de seguridad, y no pueden ser interceptadas ni robadas por atacantes remotos. Este Día de una Internet Segura arroja luz sobre la ineficacia de las contraseñas y sobre cómo más plataformas y servicios deberían permitir claves de acceso para crear una Internet segura para todos".

Christopher Budd, director de investigación de amenazas de Sophos, dice: "También es importante recordar el poder del 'no'. La mejor manera de proteger sus datos e información es, en primer lugar, no revelarlos. El hecho de que un sitio te pregunte por tu cumpleaños, por ejemplo, no significa que lo necesite o que tenga derecho a recibirlo. Si un sitio o servicio no tiene su información, no puede perderla ni revelarla accidentalmente".

Alex Laurie, vicepresidente senior de Ping Identity, concluye: "Internet es un arma de doble filo. Ofrece comodidad, productividad, accesibilidad y escala mundial, mientras que los delincuentes lo aprovechan para lanzar ciberataques a individuos y empresas por igual, destinadas a robar información personal para obtener beneficios económicos. El Día de una Internet Segura sirve como recordatorio para estar atentos a qué y cómo se comparten, recopilan y almacenan datos de identidad digital, especialmente dada la creciente prevalencia de las herramientas de inteligencia artificial (IA).

"El día también subraya el valor de confiar en métodos de autenticación que brinden más seguridad y conveniencia, como la autenticación multifactor (MFA) y sin contraseña al acceder a información en línea. De hecho, el 50% de los consumidores dice que MFA los hace sentir mejor con el servicio que utilizan, y el 65% cambiaría a una marca comparable si ofreciera autenticación sin contraseña. Nunca ha sido tan fácil para las empresas satisfacer las demandas de los consumidores y al mismo tiempo hacer de Internet un lugar más seguro".