La ciberseguridad es responsabilidad de todos

En nuestro mundo siempre conectado, donde la información privada de individuos y organizaciones es vulnerable a la exposición y mal uso, la ciberseguridad es responsabilidad de todos porque a los hackers maliciosos o actores de amenazas que roban información propietaria no les importa la edad, género, raza, cultura, creencias o nacionalidad. Ellos investigan tu huella digital y tus computadoras conectadas a Internet basándose en la oportunidad, buscando a menudo beneficio económico.

Apuntando a los Humanos

Las personas son el principal objetivo y causa de fallos en la ciberseguridad porque la mayoría son individuos confiados que desean ayudar o contribuir como parte de la naturaleza humana y sus trabajos. Hackers maliciosos y personas internas aprovechan esa confianza pareciendo hacer solicitudes de negocios legítimas de jefes o compartiendo elementos sociales de naturaleza más personalizada. Ellos cuentan con la curiosidad de las personas y su disposición a cooperar para hacerlos "hacer clic en el enlace" en un correo electrónico de negocios o personal.

Un solo clic en un enlace malicioso, sin embargo, puede descargar malware en tu computadora que puede bloquear inmediatamente datos en un ataque de "ransomware" y, a menudo, tienes que enviar dinero para recuperar el acceso. O, el malware descargado puede, sin que el usuario lo sepa, comenzar a recolectar información instantáneamente con el objetivo de obtener credenciales y contraseñas para explotar más tarde. Aunque muchas de estas acciones humanas son accidentales o no tienen la intención de ser dañinas, el resultado puede causar daño considerable a ellos mismos, su familia, sus compañeros de trabajo, su empresa y su comunidad.

Los hackers maliciosos quieren robar tu identidad y credenciales

A medida que el uso de Internet y las redes sociales ha crecido, los cibercriminales han cambiado las técnicas que usan para apuntar a las personas. El correo electrónico sigue siendo el arma número uno de elección, seguido por sitios web infectados, estafas en redes sociales y robo de identidades digitales y contraseñas.

Investigaciones recientes muestran que hasta el 80 por ciento de todas las brechas de datos involucran la compromisión de las credenciales de un empleado. En una encuesta, los hackers afirman que robar la contraseña de un empleado es la forma más rápida (y preferida) de violar y eludir los controles de ciberseguridad de una empresa.

A medida que te conectas a servicios en línea para obtener las últimas noticias, buscar las mejores ofertas, chatear con amigos, transmitir música y videos, y realizar transacciones bancarias, rápidamente te conviertes en un objetivo de los cibercriminales. Usando redes sociales, por ejemplo, típicamente compartes mucha información personal identificable sobre tus identidades físicas y digitales. Esta información incluye nombre completo, dirección de casa, números de teléfono, dirección IP, detalles biométricos, detalles de ubicación, fecha de nacimiento, lugar de nacimiento e información sobre otros miembros de la familia. Los cibercriminales saben esto y pueden pasar hasta el 90 por ciento de su tiempo realizando reconocimiento usando fuentes de redes sociales en línea para aplicar técnicas de

búsqueda avanzadas y parámetros de motores de búsqueda especializados para descubrir información confidencial de empresas e individuos que típicamente no aparece durante búsquedas web normales.

Los hackers maliciosos buscan específicamente robar tus credenciales de nombre de usuario y contraseña para poder acceder a tu información e impersonarte. Y, cuando tu identidad es robada, un atacante puede fácilmente eludir los controles de seguridad técnica tradicionales sin ser detectado. Una vez dentro de la red informática, los cibercriminales pueden llevar a cabo ataques maliciosos o acceder y robar información confidencial haciéndose pasar por un usuario legítimo.

Tu información de trabajo y personal están todas vinculadas en el ciberespacio

La protección de la información sobre tu vida laboral y personal ya no puede separarse. El uso frecuente y generalizado de redes sociales, trabajar desde casa o al viajar, y el Internet de

las Cosas (IoT) conectando todo tipo de dispositivos domésticos significa que la ciberseguridad ya no es solo responsabilidad del departamento de TI de tu empresa. Una cuenta personal comprometida puede fácilmente llevar a un cibercriminal a descubrir suficiente información sobre ti para hacer que hackear tu correo electrónico de negocios sea mucho más fácil.

A medida que la línea entre el uso de Internet de negocios y personal continúa difuminándose, cada empleado debe contribuir en proteger los activos de información en el trabajo y en casa.

Estar en la Primera Línea

Muchas personas en el trabajo y en casa sufren de fatiga cibernética, que describe la frustración experimentada al manejar decenas de cuentas en línea con múltiples contraseñas necesarias para acceder a la información que usas diaria o horariamente. En algunos casos, los individuos se sienten tan frustrados que renuncian a intentar manejar las cosas de manera segura y recurren a usar las mismas contraseñas para múltiples cuentas, compartiendo contraseñas con miembros de la familia e iniciando sesión en Internet usando sus cuentas de redes sociales.

Eres la primera línea en la batalla para mantener la información segura. Los ataques confían en tu buena voluntad y confianza para tener éxito, por lo que debes volverte más personalmente responsable en cómo manejas tu información, y esto puede ser agotador.

Para superar la fatiga cibernética (o evitarla por completo), sugiero seguir estos consejos:

- Simplifica tu experiencia de inicio de sesión usando un gestor de contraseñas que te ayudará a reducir el dolor de seleccionar contraseñas largas y complejas, recordar demasiadas contraseñas y elegir contraseñas únicas para cada cuenta. Un gestor de contraseñas hará esto por ti.

- Configura tus programas, aplicaciones y software de seguridad para que se actualicen automáticamente para que no tengas que hacerlo manualmente. Uno de los pasos más importantes en la ciberseguridad es mantenerse actualizado, y habilitar actualizaciones automáticas te ayuda para que no tengas que preocuparte por obtener los últimos parches de seguridad.

- Programa copias de seguridad de datos para asegurarte de que cuando ocurran cosas malas siempre tengas una copia de seguridad sólida para volver a la normalidad y no estresarte por perder datos importantes.

- Mantente educado sobre las últimas tendencias de seguridad para que sepas qué es importante y puedas ayudar a evitar la sobrecarga de información sobre no saber qué está pasando en el ciberespacio.