Cybersecurity at Work Meeting Kit – Spanish

QUÉ ESTÁ EN RIESGO

Un solo clic en un enlace malicioso puede costarle millones a su empresa. Desde el ransomware hasta las estafas de phishing, los ciberataques no solo se dirigen a los departamentos de TI, sino también a las personas. Es decir, a usted. Si maneja el correo electrónico, inicia sesión en sistemas, accede a datos de clientes o incluso utiliza la red Wi-Fi en el trabajo, forma parte de la primera línea de defensa. Las amenazas cibernéticas pueden paralizar las operaciones, filtrar datos confidenciales y arruinar reputaciones. Y no solo son un riesgo para la empresa, sino que también pueden poner en peligro su trabajo, su identidad y la seguridad de sus compañeros. Mantener la seguridad cibernética no es opcional. Es parte de su trabajo, todos los días.

CUÁL ES EL PELIGRO

Las amenazas a la ciberseguridad no siempre parecen amenazas. A menudo parecen correos electrónicos inofensivos, ventanas emergentes amigables o pantallas de inicio de sesión rutinarias. Pero, entre bastidores, pueden abrir la puerta a daños graves, y solo hace falta un error.

Phishing y estafas por correo electrónico: disfrazadas y peligrosas

Los correos electrónicos de phishing están diseñados para engañarle. A menudo parecen provenir de su jefe, su banco o un proveedor de confianza, pero contienen enlaces o archivos adjuntos que, una vez pulsados, permiten a los piratas informáticos robar información o instalar malware.

- Algunos correos electrónicos de phishing se hacen pasar por contactos internos y solicitan transferencias urgentes o contraseñas.
- Otros incluyen facturas falsas o notificaciones de envío con archivos adjuntos maliciosos.

Contraseñas débiles y nombres de usuario reutilizados: un blanco fácil.

Usar la misma contraseña en varios sistemas o elegir algo como «123456» o el nombre de su mascota facilita el acceso a los piratas informáticos. Una vez que un sistema se ve comprometido, a menudo pueden acceder a otros, especialmente si no se ha habilitado la autenticación multifactorial.

Ransomware y malware: modo de bloqueo

Los ataques de ransomware pueden bloquear todo su sistema: archivos, redes e incluso sistemas de seguridad. Es posible que aparezca una pantalla exigiendo un pago en criptomoneda para recuperar sus datos. Estos ataques suelen comenzar con un solo archivo o enlace infectado.

Dispositivos y redes no seguros: la amenaza silenciosa

¿Trabaja a distancia o utiliza dispositivos personales para el trabajo de la empresa? Si esos dispositivos no son seguros o no están actualizados, son un punto de acceso fácil para los ciberdelincuentes.

- Incluso conectarse a una red Wi-Fi pública sin una VPN puede exponer datos confidenciales de la empresa.
- Violaciones de datos: las consecuencias son reales

COMO PROTEGERSE

La ciberseguridad no tiene por qué ser complicada, pero sí requiere concienciación. La mayoría de los ataques no comienzan con un hacker experto que rompe un cortafuegos, sino con alguien que hace clic en un enlace malicioso, reutiliza una contraseña u omite una actualización. ¿La buena noticia? Unos pocos hábitos sólidos pueden marcar una gran diferencia.

Piensa antes de hacer clic

Aquí es donde comienzan la mayoría de los problemas, y donde normalmente se pueden detener. A los hackers les encanta enviar correos electrónicos que parecen legítimos. Tal vez sea «RR. HH.» o tal vez sea «TI» quien le diga que «actualice su contraseña ahora». Cuentan con que usted haga clic primero y pregunte después. No les dé esa satisfacción. Tómese su tiempo. Observe con atención. Si algo le parece extraño, confíe en su instinto. Es mejor reenviarlo a su equipo de TI que caer en una trampa.

Utiliza contraseñas seguras y únicas.

Este es uno de los pasos más fáciles que puedes dar, y uno de los más ignorados. Piensa en tu contraseña como la cerradura de la puerta de tu casa: ¿utilizarías la misma llave para tu casa, tu coche y tu oficina?

- Cree contraseñas con una combinación de letras, números y caracteres especiales.
- No utilice fechas de cumpleaños, nombres de mascotas o «123456», ya que se descifran rápidamente.
- Utilice un gestor de contraseñas para llevar un control (la mayoría de los lugares de trabajo ofrecen o recomiendan uno).
- Cambie sus contraseñas con regularidad y nunca las comparta, ni siquiera con sus compañeros de trabajo.

Mantenga sus dispositivos actualizados

Sí, esas ventanas emergentes de actualización de software son molestas, pero ignorarlas deja la puerta abierta a las amenazas cibernéticas. Las actualizaciones no solo le proporcionan nuevas funciones, sino que también corrigen los agujeros de seguridad que los hackers saben encontrar. Ya sea su ordenador portátil, de sobremesa o su teléfono móvil, manténgalos actualizados. Cuanto más espere, más riesgo correrá.

Trabajo remoto seguro y acceso móvil

¿Trabaja de forma remota o revisa sus correos electrónicos desde su teléfono? Esa flexibilidad es excelente, hasta que sus datos terminan en manos equivocadas. Nunca se conecte a una red Wi-Fi pública sin una VPN y siempre bloquee su pantalla cuando se aleje. Si su empresa le proporciona herramientas de seguridad, utilícelas, no son opcionales. Y si utiliza dispositivos personales para trabajar, asegúrese de que también estén protegidos.

Sea inteligente con los datos de la empresa

Del mismo modo que no dejaría documentos confidenciales en la sala de descanso, tampoco deje archivos digitales sin protección. Piense detenidamente cómo y dónde accede, envía y guarda la información.

- No guarde archivos de trabajo en USB o unidades personales.
- Nunca envíe documentos confidenciales a su correo electrónico personal.
- Utilice solo aplicaciones o plataformas aprobadas para almacenar y compartir archivos.

CONCLUSIÓN

La ciberseguridad no es solo un problema del departamento de TI, es responsabilidad de todos. Un clic, una contraseña reutilizada o una actualización omitida pueden abrir la puerta a una filtración de datos que afecte a toda su organización.