



5 de los peores hábitos de seguridad en Sistemas de Información

Reparar los malos hábitos de seguridad cibernética puede ser tan fácil o tan difícil como corregir malos hábitos personales.

1) Actitud desprecupada

"Las posibilidades de ser pirateado son tan bajas que no necesito molestarme en aprender sobre la ciberprotección".

Incorrecto. El *hackeo* a Equifax (empresa crediticia de Estados Unidos) puede haber afectado a más del 55 por ciento de los estadounidenses mayores de 18 años. El *hackeo* a Yahoo puso en riesgo a 3 mil millones de sus usuarios. El crimen cibernético se está disparando. Un ataque *ransomware* ocurre cada 45 segundos.

"Mi empleador se encargará de eso por mí".

Nuevamente incorrecto. Conectarse a la red corporativa solo aumenta el riesgo cibernético y expone al usuario a más perpetradores. Los usuarios deben tomarse la seguridad en serio y aprender algo al respecto. Si no, están descuidando su seguridad cibernética y lo pagarán.

2) Sin protección de correo electrónico

El robo de correo electrónico es uno de los crímenes cibernéticos más grandes. Para proteger a los usuarios de los piratas informáticos que tienen acceso a identidades robadas, **la mayoría de las aplicaciones de correo electrónico, incluyendo Gmail, Yahoo Mail, AOL Mail y Outlook, ofrecen verificación en dos pasos.** Con la verificación en dos pasos activada, una aplicación de correo electrónico requiere un código adicional cuando el usuario inicia sesión. Cada vez que un usuario ingresa su nombre de usuario y contraseña, la aplicación de correo electrónico le envía un código secreto que debe ingresar para acceder a su correo electrónico. Cuando un pirata informático intenta iniciar sesión en la cuenta de correo electrónico del usuario, se detiene en seco porque no tiene el código secreto. **El problema con la verificación en dos pasos es que requiere que el usuario lo active.** La mayoría de los usuarios desconoce esto o son demasiado perezosos para pasar 5 minutos para activar el interruptor de dos pasos de su cuenta de correo electrónico. Como resultado, sus cuentas de correo electrónico están abiertas a los piratas informáticos.

3) Hacer clic en hipervínculos en correos electrónicos

El 91% de los ciberataques y las violaciones de datos resultantes comienzan con un correo electrónico de *phishing*: un correo electrónico falso que puede pretender ser un representante de atención al cliente pidiéndole a un usuario que haga clic en un enlace para cambiar su contraseña por seguridad. Puede parecer que un correo electrónico de aspecto auténtico proviene del VISA, solicitando a un usuario que haga clic en un enlace para recibir su reembolso. ¿El remedio? **No hacer clic en ningún hipervínculo sospechoso contenido en los correos electrónicos.** Las consecuencias de hacer clic en un enlace fraudulento pueden ser trágicas.

4) Prácticas de contraseña pobres

Las contraseñas débiles facilitan que los hackers adivinen correctamente o usen herramientas sencillas de descifrado de contraseñas para acceder al correo electrónico y a otras cuentas de usuario. La gente sabe esto pero, de todos modos, **la contraseña más popular en uso hoy en día es 123456.** Las personas suelen usar la misma contraseña fácil de descifrar para todas sus aplicaciones. La fatiga cibernética está creciendo a un ritmo alarmante y los piratas informáticos están sacando provecho de este fenómeno. Una vez que un ladrón cibernético descubre que la contraseña de un usuario para todas sus cuentas es "admin" (una de las contraseñas más populares para los usuarios de Equifax que fueron pirateados), se acabó el juego. Si eso no es suficientemente malo, los usuarios tienden a compartir sus contraseñas. Compartir contraseñas multiplica los problemas de las contraseñas débiles y reutilizadas.

5) Sin copias de seguridad de datos

Ransomware, un *malware* que infecta las computadoras y restringe su acceso a los archivos, a menudo amenaza con la destrucción permanente de datos a menos que se pague un rescate y ha alcanzado proporciones epidémicas. Un ataque de *ransomware* puede resultar en la pérdida permanente de datos personales y comerciales importantes: la mejor manera de frustrarlo es hacer una copia de seguridad de los archivos. **"Realizar copia de seguridad de datos regularmente y verificar la integridad de esas. Las copias de seguridad son fundamentales en los incidentes de ransomware; si está infectado, las copias de seguridad pueden ser la única manera de recuperar sus datos críticos"**, afirma el FBI en un anuncio de servicio público de 2016. A pesar del *ransomware* y otras amenazas cibernéticas, la mayoría de los usuarios de computadoras todavía no están respaldando sus datos, y la pérdida puede ser devastadora y costosa.

