OUCH! Septiembre 2021

El Boletín Mensual de Concientización en Seguridad para ti

Un simple paso para asegurar tus cuentas

¿Parece que los ciberdelincuentes tienen una varita mágica para ingresar a tu correo electrónico o cuentas bancarias y no hay nada que puedas hacer para detenerlos? ¿No sería genial si hubiera un solo paso que te ayudara a protegerte de los ciberdelincuentes y te permitiera aprovechar al máximo la tecnología de manera segura? Si bien ningún paso detendrá a todos los delincuentes cibernéticos, uno de los pasos más importantes que puedes tomar es habilitar algo llamado autenticación de dos factores (a veces llamado 2FA, verificación de dos pasos o autenticación de múltiples factores) en tus cuentas más importantes.

El problema con las contraseñas

Cuando se trata de proteger tus cuentas, lo más probable es que ya estés utilizando algún tipo de contraseña. Hay varias formas de autenticarse en una cuenta: algo que tienes, algo que sabes, algo que eres, algún lugar en el que estás. Cuando empleas más de un método de autenticación, estás agregando una capa adicional de protección contra los ciberdelincuentes; incluso si descifran un método, aún tendrían que eludir los factores adicionales para acceder a tu cuenta. Las contraseñas prueban quién eres en función de algo que sabes. El peligro de las contraseñas es que son un único punto de falla. Si un ciberdelincuente puede adivinar o comprometer tu contraseña, puede obtener acceso a tus cuentas más importantes. Además, los ciberdelincuentes están desarrollando técnicas mejores y más rápidas para adivinar, comprometer o eludir contraseñas. Afortunadamente, puedes contraatacar con la autenticación de dos factores.

Autenticación de dos factores

Agregar autenticación de dos factores es una solución mucho más segura que depender solo de contraseñas. Funciona al requerir no uno, sino dos métodos diferentes para autenticarse. De esta manera, si tu contraseña se ve comprometida, tu cuenta seguirá estando protegida. Un ejemplo es tu tarjeta de cajero automático; cuando retiras dinero de un cajero automático, en realidad estás utilizando una forma de autenticación de dos factores. Para acceder a tu dinero, necesitarás dos cosas: tu tarjeta de cajero automático (algo que tienes) y tu número PIN (algo que sabes). Si pierdes tu tarjeta de cajero automático, cualquier persona que encuentre tu tarjeta no podrá retirar tu dinero, ya que no conoce su PIN. lo mismo ocurre si solo tienen tu PIN y no la tarjeta. Un atacante debe tener ambos para comprometer tu cuenta de cajero automático.

El concepto es similar para la autenticación de dos factores; tienes dos capas de seguridad.

Usar la autenticación de dos factores en línea

La autenticación de dos factores es algo que configuras individualmente para cada una de tus cuentas.
En realidad, es bastante simple: por lo general, no necesitas hacer nada más que sincronizar tu teléfono móvil con tu cuenta. De esta manera, cuando necesites iniciar sesión en tu cuenta, no solo iniciarás sesión con el nombre de usuario y la contraseña de tu cuenta, sino que también utilizarás un código único que obtienes de tu teléfono. La idea es que se requiera la combinación de tu contraseña y código único para iniciar sesión. Por lo general, este código único se enviará mediante un mensaje de texto a tu dispositivo móvil o correo electrónico. Tu teléfono también puede tener una aplicación móvil (como la aplicación Google o Microsoft Authenticator) que generará el código único para ti. Cuando es posible, las aplicaciones móviles se consideran la opción más segura para obtener tu código único.

Lo que hace que esto sea tan simple es que, por lo general, solo tienes que hacer esto una vez desde cualquier computadora o dispositivo que estés utilizando para iniciar sesión. Una vez que el sitio web o tu cuenta reconocen tu dispositivo, solo necesitarás tu contraseña para iniciar sesión. Cada vez que intentes (o alguien más lo intente) iniciar sesión con tu cuenta, pero desde una computadora o dispositivo diferente, tendrá que usar la autenticación de dos factores nuevamente. Esto significa que si un ciberdelincuente obtiene tu contraseña, aún no puede acceder a tu cuenta, ya que cuenta con el código único.

Recuerda, la autenticación de dos factores generalmente no está habilitada de manera predeterminada, por lo que deberás habilitarla tú mismo para cada una de tus cuentas más importantes, como banca, inversiones, jubilación o correo electrónico personal. Si bien esto puede parecer más trabajo al principio, una vez configurado, es muy fácil de usar.

Editor invitado

Lysandra Capella tiene más de 15 años de experiencia trabajando en Seguridad y Tecnología de la Información. Ella es instructora del Instituto SANS del curso AUD507, enfocado en medir y gestionar el riesgo. Cuando no está enseñando, Lysandra apoya a equipos de dirección ejecutiva con la formulación de estrategias, la garantía de seguridad y el gobierno de TI.
https://www.linkedin.com/in/lysandracapella/.

Recursos

Creando contraseñas simples: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Gestores de contraseñas: https://www.sans.org/newsletters/ouch/password-managers/

Traducido para la comunidad por: Célica Martínez Aponte, UNAM-CER