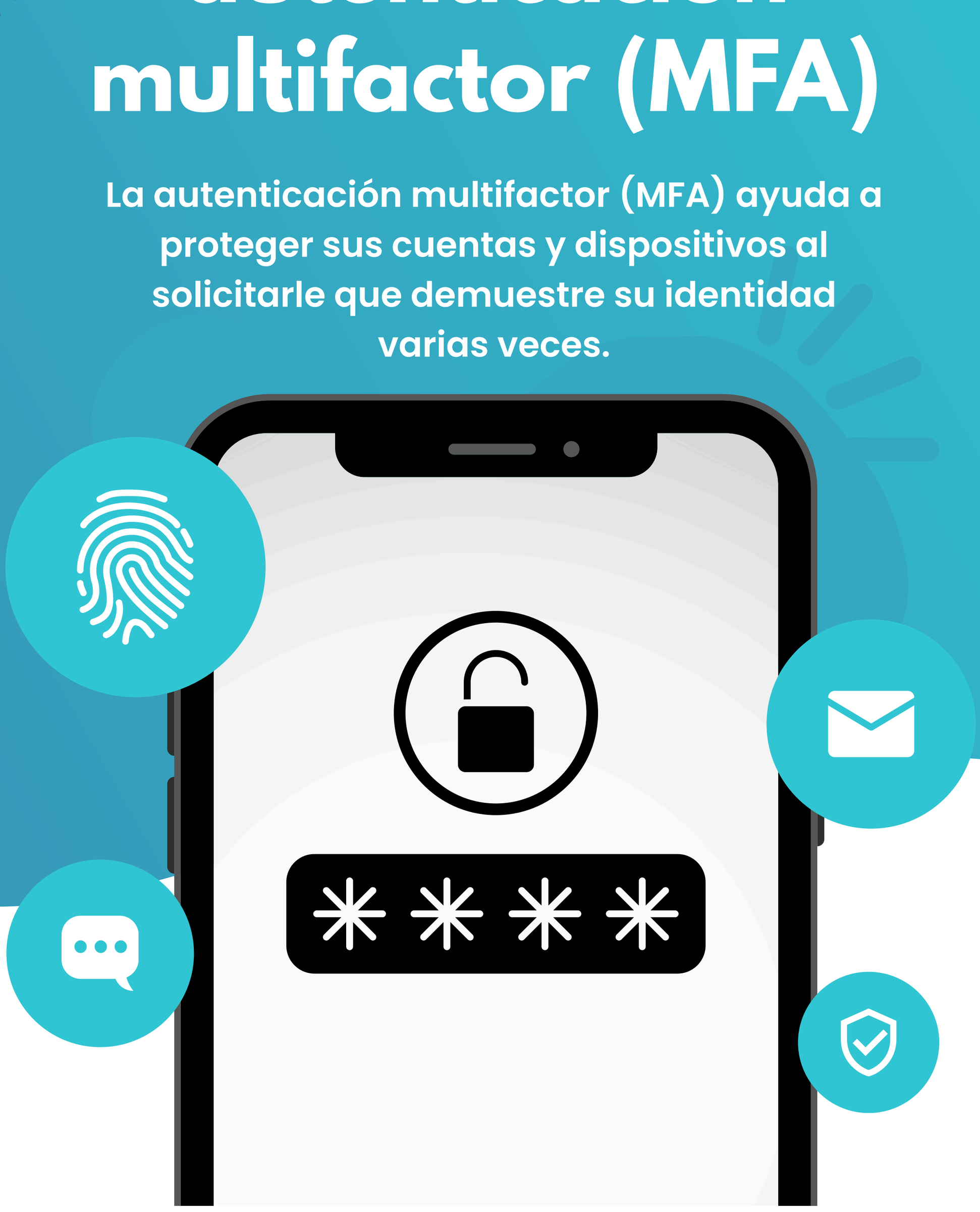
Mantenga sus aplicaciones y software actualizados.

Los parches son importantes porque corrigen vulnerabilidades conocidas del producto que los atacantes pueden explotar para comprometer sus dispositivos.

Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.

Habilitar la autenticación multifactor (MFA)

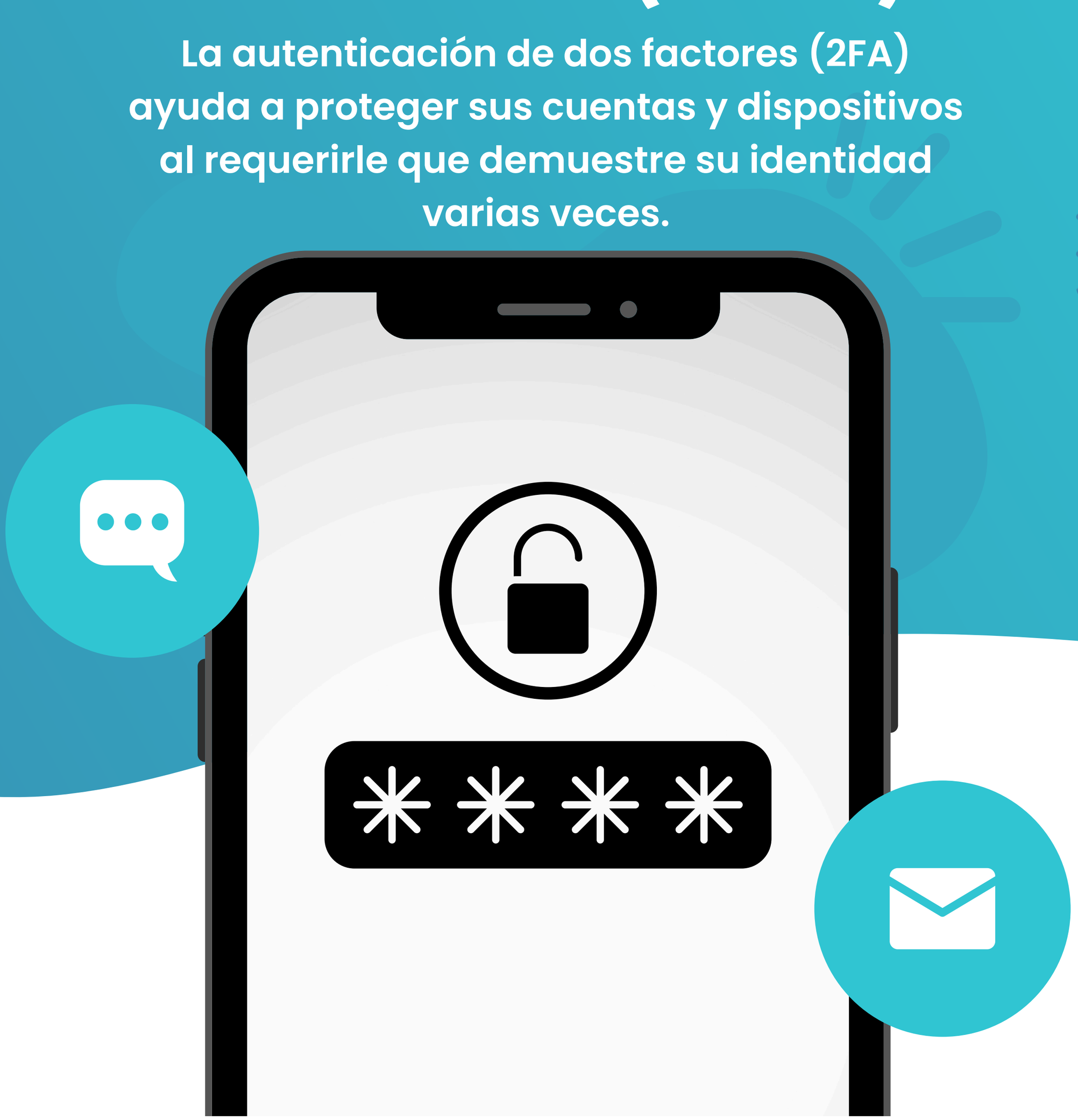
La autenticación multifactor (MFA) ayuda a proteger sus cuentas y dispositivos al solicitarle que demuestre su identidad varias veces.



Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.

Habilitar la autenticación de dos factores (2FA)

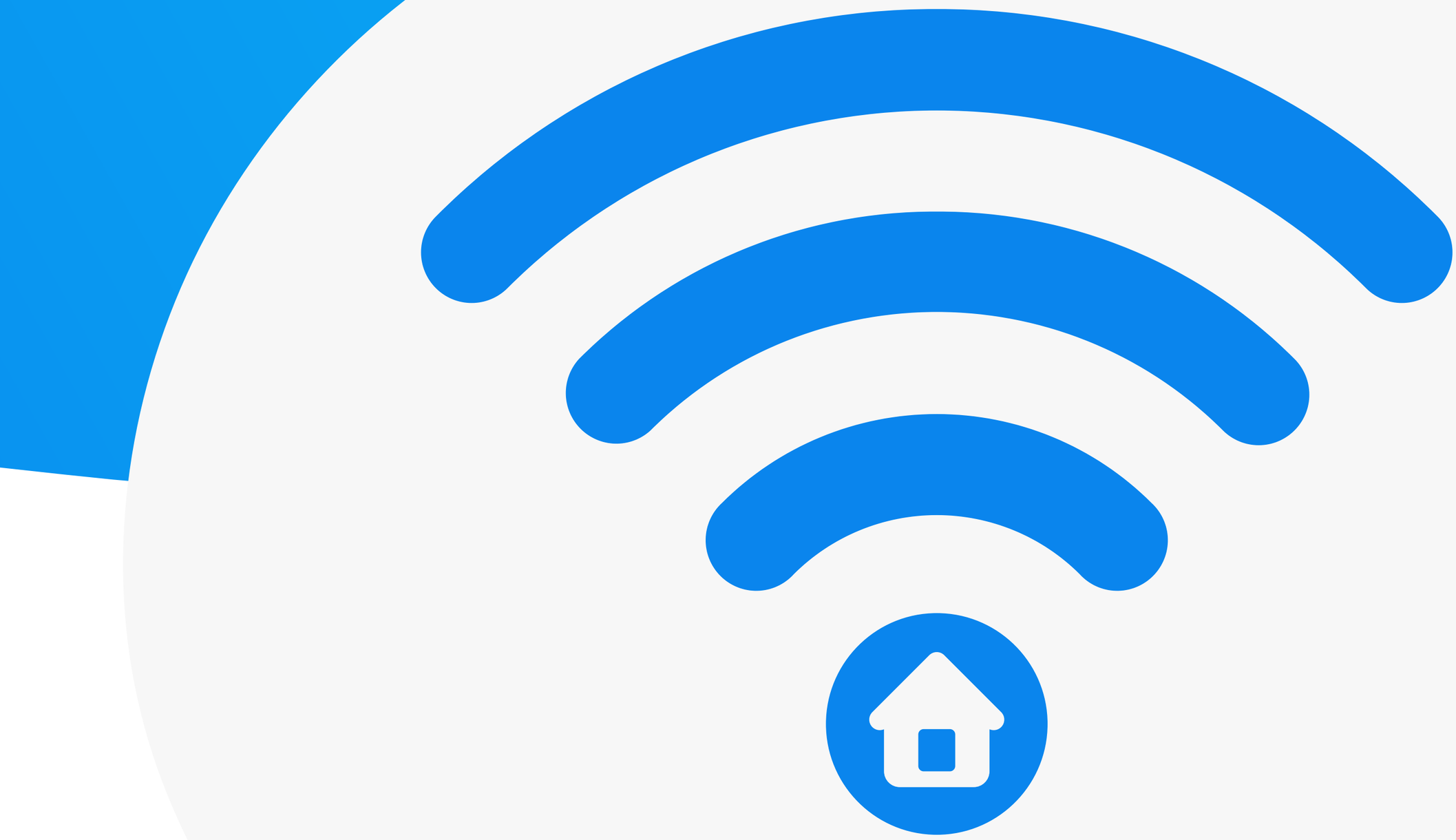
La autenticación de dos factores (2FA) ayuda a proteger sus cuentas y dispositivos al requerirle que demuestre su identidad varias veces.



Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.

Asegúrese de que su red doméstica sea segura.

Cambiar la contraseña predeterminada de su enrutador y asegurarse de que su firmware esté actualizado ayudará a reducir el riesgo de piratería.



Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.

¿Por qué utilizar una VPN para mejorar la seguridad?

Una conexión a una red privada virtual (VPN) enmascara su tráfico de datos en línea y lo protege del acceso externo.

Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.

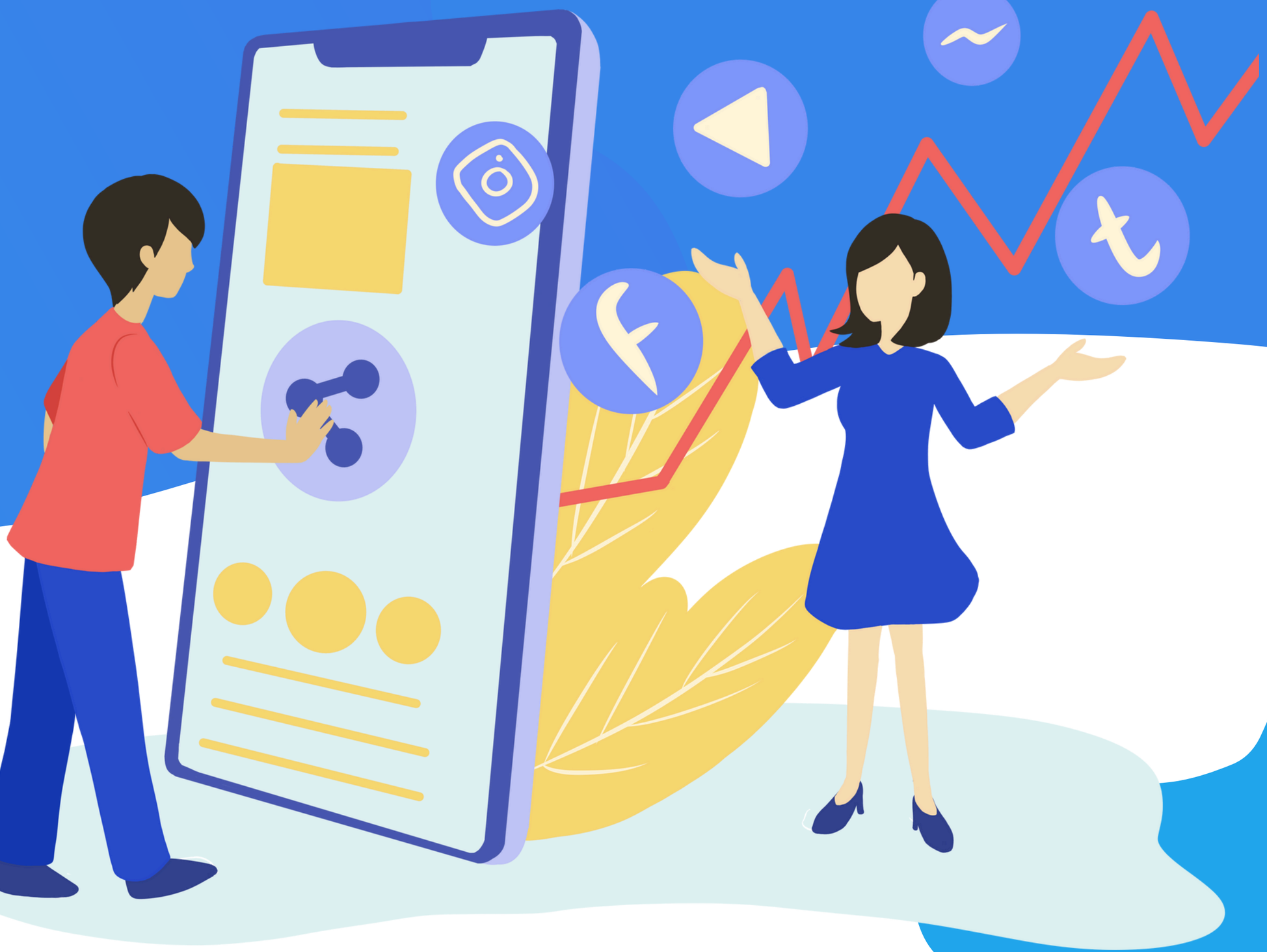
No olvides la seguridad física

Asegúrese de bloquear su computadora cuando salga de la oficina y guarde bajo llave todos los documentos en papel que contengan información confidencial.

Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.

¿Compartes información confidencial en las redes sociales?

Los ciberdelincuentes pueden usar la información que usted publica en las redes sociales para obtener información personal sobre usted (PII) que puede usarse en su contra.



Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.

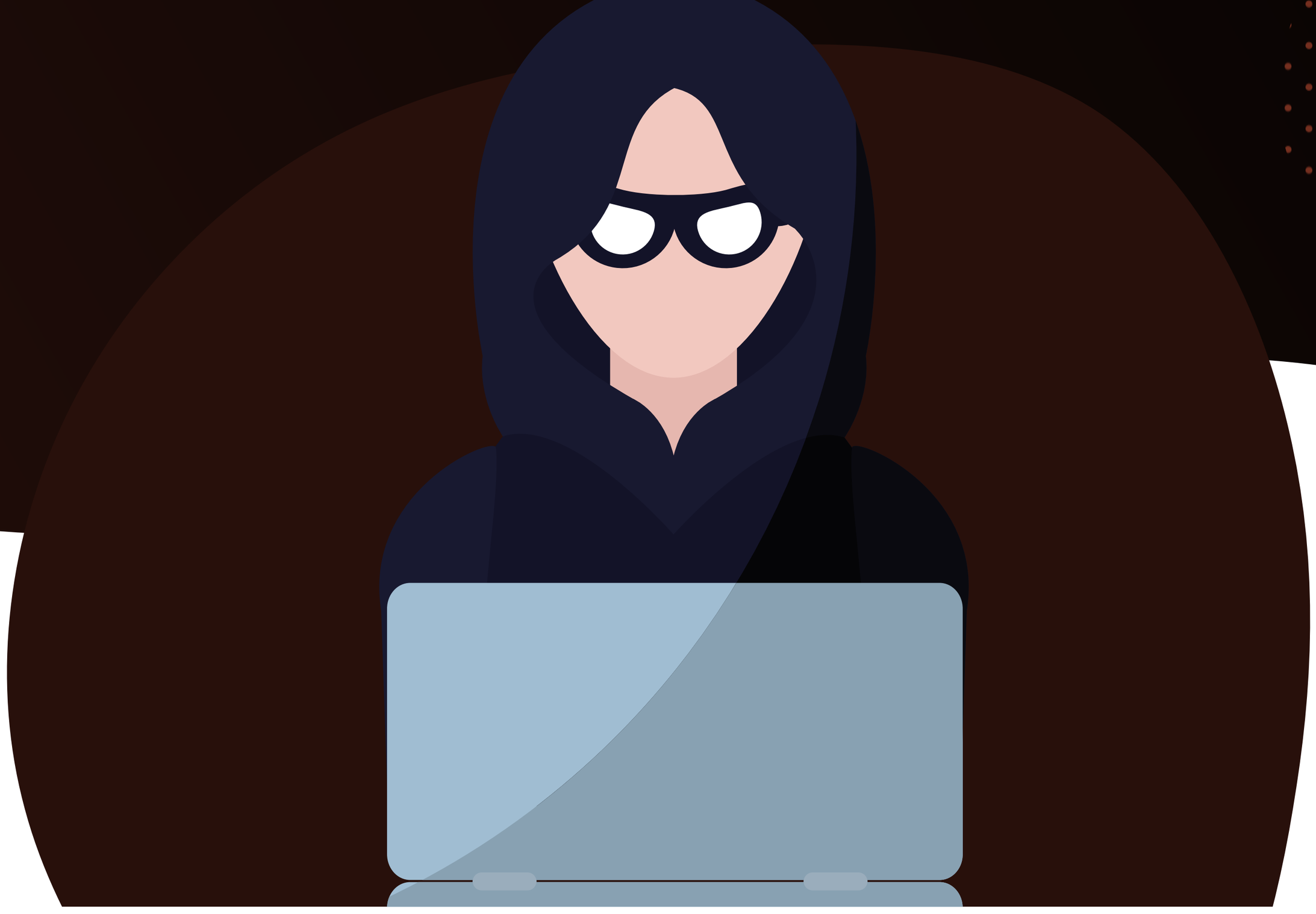
Respete siempre las políticas y procedimientos de la empresa.

Las políticas y procedimientos de seguridad brindan orientación esencial que nos ayuda a proteger nuestro negocio, colegas y clientes de los ciberataques y la pérdida de datos.

Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.

Cuidado con la ingeniería social

La ingeniería social es un vector de ataque que se basa en la interacción humana y que a menudo implica manipular a las personas para que violen los procedimientos de seguridad con el fin de obtener acceso a sistemas, redes o ubicaciones físicas.



Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.

5 señales reveladoras de un ataque de ingeniería social

El mensaje llega inesperadamente

Esta es una característica clave de la ingeniería social, aunque los atacantes también pueden usar cuentas de correo electrónico comprometidas para secuestrar conversaciones.

La acción solicitada parece inusual.

Tenga cuidado si le piden que haga algo que normalmente no haría (por ejemplo, enviar dinero, instalar algo, compartir información de clientes, etc.).

La acción solicitada parece arriesgada.

Si se lleva a cabo esta acción, ¿podría perjudicar al destinatario o a la empresa? De ser así, piénselo dos veces.

Un archivo adjunto o URL inusual

Muchas estafas de ingeniería social incluyen un enlace fraudulento en el que se le pide al usuario que haga clic o un documento/programa para descargar.

Hay un sentido de urgencia.

Muchas estafas se basan en un gran sentido de urgencia y el estafador intenta comunicar una amenaza de daño.

Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.

¡No caigas en estafas de phishing!

Los correos electrónicos de phishing parecen solicitudes legítimas de entidades conocidas y a menudo le piden que haga clic en enlaces, descargue archivos adjuntos o proporcione información confidencial.

Piensa antes de hacer clic

Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.

Consejos para concienciar sobre el phishing

Enlaces sospechosos en el correo electrónico

Tenga cuidado si la dirección web que aparece cuando pasa el cursor sobre el enlace no parece coincidir con el remitente o si el correo electrónico lo redirecciona a una página que le solicita que inicie sesión.

Mala ortografía y gramática

Los correos electrónicos y mensajes de texto de phishing a veces pueden estar plagados de errores ortográficos y gramaticales, así que preste atención a estas señales.

Solicitud de información sensible

Si le piden que comparta información confidencial que normalmente no compartiría por correo electrónico, llame a un número conocido para verificar la solicitud.

Emergencia o amenazas subyacentes

Los atacantes a menudo recurren a un sentido de urgencia para presionarte a actuar rápidamente sin darte tiempo para detenerte y pensar.

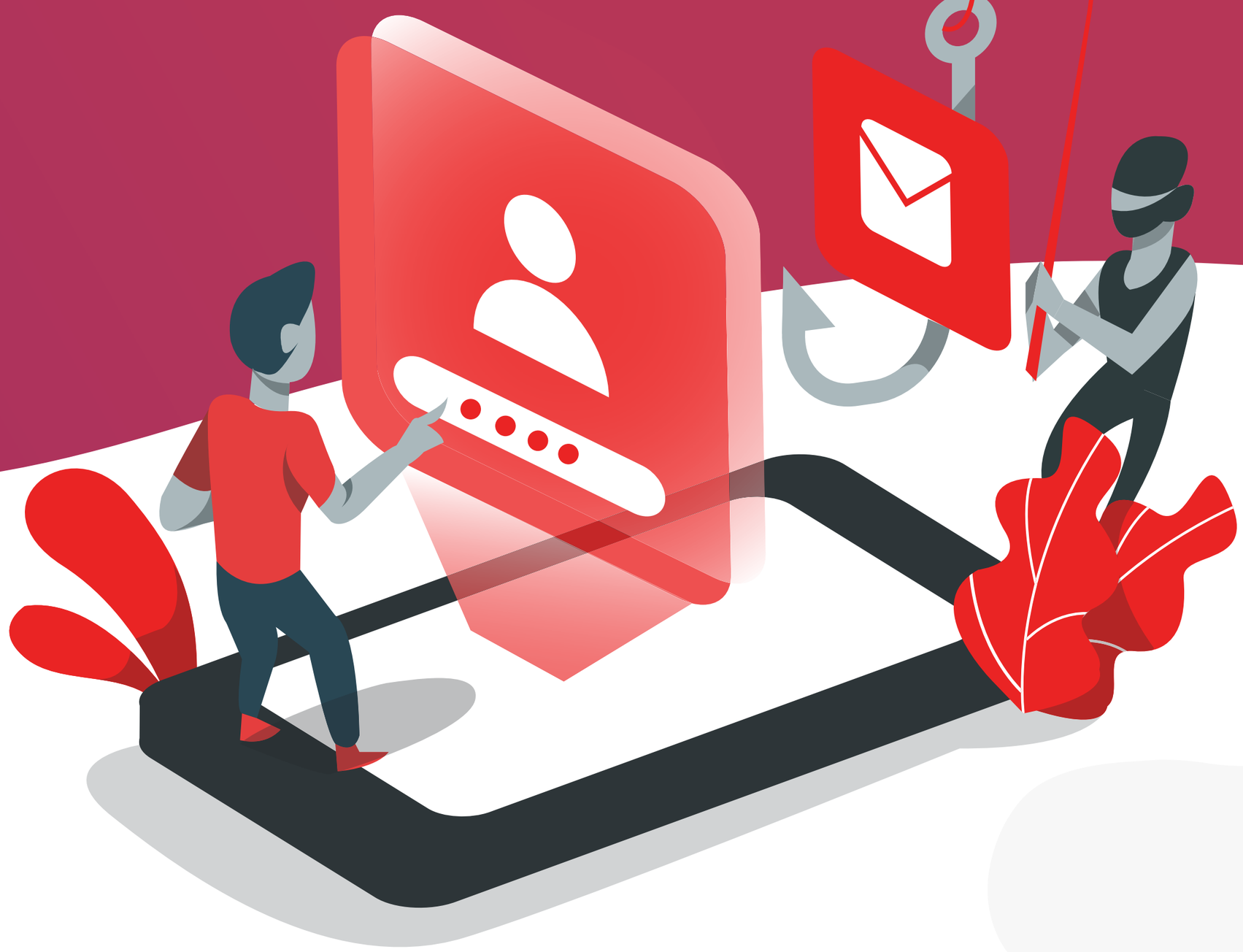
Dominios sospechosos

Muchos correos electrónicos maliciosos utilizan un dominio que parece legítimo, pero con ligeras diferencias.

Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.

Utilice siempre contraseñas seguras, únicas y confidenciales.

Sus contraseñas deben ser únicas, privadas y fáciles de recordar para usted, pero no fáciles de adivinar para un hacker.



Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.

Consejos de seguridad para contraseñas

No reutilice sus contraseñas.

Si una violación de datos compromete una de sus cuentas, el atacante podría acceder a otras cuentas utilizando sus contraseñas reutilizadas.

No dejes tus contraseñas a la vista.

No deje sus contraseñas en un lugar inseguro, como una nota adhesiva, una agenda o un archivo de texto sin cifrar.

No compartas tus contraseñas.

Nunca compartas tus contraseñas o cuentas con nadie, ni siquiera con tus colegas.

Crea contraseñas largas y sencillas

Utilice una serie de palabras aparentemente no relacionadas para crear contraseñas largas y simples en lugar de cortas y complejas.

Utilice métodos de autenticación multifactor

Utilice el método de autenticación multifactor más seguro disponible, como una aplicación de autenticación.

Manténgase alerta.
Manténgase al tanto de los riesgos cibernéticos.