DENUNCIE LOS CIBERATAQUES Y CIBERINCIDENTES PARA MANTENER A AUSTRALIA SEGURA.

INSCRÍBASE

En nuestro servicio de alerta gratuito
cyber.gov.au

DENUNCIE

La ciberdelincuencia a REPORTCYBER:
cyber.gov.au/report

CONTACTO

Llame al 1300 CYBER1 o
visite cyber.gov.au

Este número es para llamadas en Australia únicamente.

SÍGANOS

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

5. CUIDADO CON LAS ESTAFAS

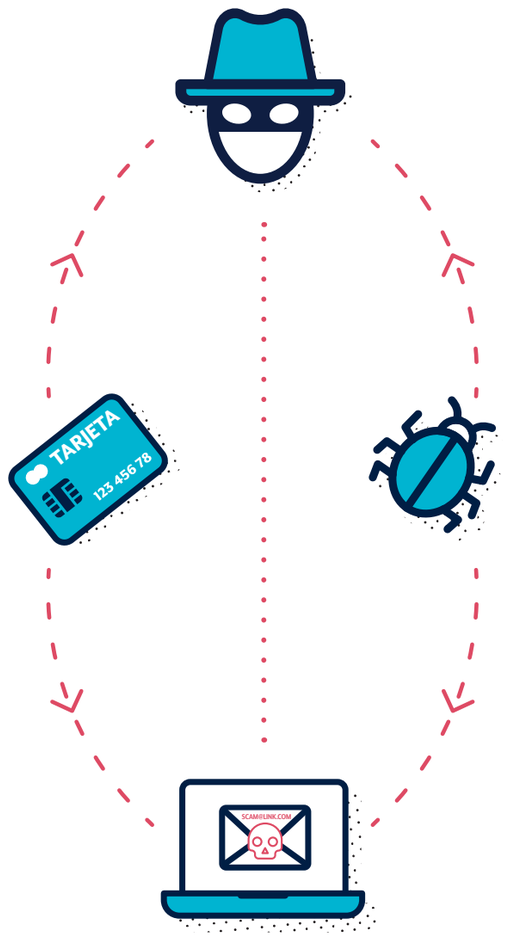
Los ciberdelincuentes usan e-mail, SMS, llamadas telefónicas y medios sociales para engañar y lograr que la persona abra un archivo adjunto, visite una página web, revele los datos de conexión a una cuenta, revele información confidencial o transfiera dinero o tarjetas de regalo. Presentan estos mensajes de modo que parezcan haber sido enviados por personas u organizaciones que uno cree conocer, o en las que uno cree que puede confiar.

Para detectar los mensajes fraudulentos, deténgase y reflexione:

- **Autoridad:** ¿Dice el mensaje que viene de un funcionario oficial?
- **Urgencia:** ¿Le dicen que tiene un tiempo limitado para responder?
- **Emoción:** ¿Despierta el mensaje en usted sensaciones de pánico, temor, esperanza o curiosidad?
- **Escasez:** ¿Le ofrece el mensaje algo que escasea?
- **Actualidades:** ¿Está el mensaje relacionado con noticias de actualidad, grandes eventos o momentos específicos del año (por ejemplo, la declaración de impuestos)?

Para comprobar si un mensaje es legítimo:

- Vaya a algo de confianza. Visite la página web oficial, conéctese a su cuenta o llame por teléfono al número del aviso. No use los enlaces o datos de contacto del mensaje que recibió o que le dieron por teléfono.
- Compruebe si la fuente oficial ya le ha dicho qué datos no le pedirá nunca. Por ejemplo, posiblemente su banco le haya dicho que jamás le pedirá su contraseña.



Para obtener más información sobre la detección de mensajes fraudulentos, vea la publicación Detección de los mensajes de ingeniería social del Centro australiano de ciberseguridad (ACSC), y manténgase informado: inscríbase en el Servicio de alerta del ACSC en **cyber.gov.au.**

PASOS SENCILLOS

PARA LA SEGURIDAD DE SUS DISPOSITIVOS Y CUENTAS

SIGA ESTOS PASOS PARA REDUCIR EL RIESGO DE ATAQUE POR CIBERDELINCUENTES

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1. ACTUALICE SUS DISPOSITIVOS

Los ciberdelincuentes atacan los dispositivos mediante debilidades conocidas de los sistemas o aplicaciones. Las puestas al día tienen actualizaciones de seguridad para corregir estas debilidades. Active las actualizaciones automáticas para que esto suceda sin su intervención.

Active las actualizaciones automáticas en todos sus dispositivos:

- Teléfono celular
- Computadora portátil
- Computadora de escritorio

Compruebe periódicamente si hay actualizaciones para sus:

- Aplicaciones
- Programas
- Dispositivos inteligentes

2. ACTIVE LA AUTENTICACIÓN MULTIFACTORIAL (MFA)

La MFA mejora la seguridad pues aumenta la dificultad de los ciberdelincuentes para acceder a sus archivos o cuentas.

Active la MFA, empezando por sus cuentas más importantes:

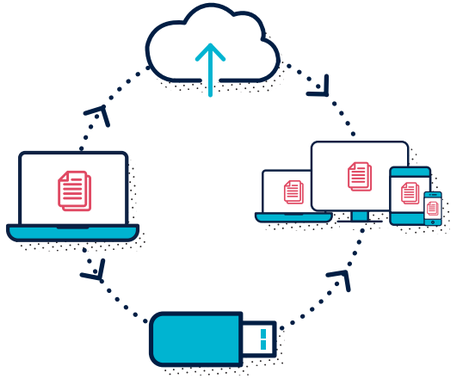
- Cuentas de correo electrónico
- Servicios bancarios en línea y cuentas con datos de pago guardados
- Medios sociales

3. CREE COPIAS DE SEGURIDAD DE SUS DISPOSITIVOS

La copia de seguridad es una copia digital de la información guardada en su dispositivo, como fotos, documentos, videos y datos de las aplicaciones. Se la puede guardar en un dispositivo de almacenamiento externo o en la nube. La copia de seguridad significa que podrá recuperar sus archivos en caso de que su dispositivo se pierda o se dañe.

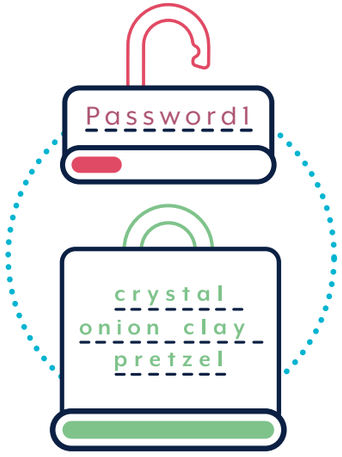
Haga copias de seguridad regularmente de sus dispositivos:

- Teléfono celular
- Computadora portátil
- Computadora de escritorio
- Tableta



4. DEFINA FRASES DE CONTRASEÑA SEGURAS

Cuando no fuera posible usar la autenticación multifactorial, una frase de contraseña segura suele ser lo único que protege su información y sus cuentas de los delincuentes.

Las frases de contraseña usan cuatro o más palabras al azar como contraseña. Cambie sus contraseñas a frases de contraseña, y asegúrese de que sean:

- Largas: Cuanto más larga la frase de contraseña, mejor. Use por lo menos 14 caracteres
- Imprevisibles: Use una mezcla al azar de palabras no relacionadas
- Únicas: No use las mismas frases de contraseña en varias cuentas