5 Reglas de ciber para una vida digital sana

Ahora puedes tomar el control de tu vida digital con estos sencillos consejos:

1 Protege tu información y tu equipo

- **Mantén tu software y aplicaciones actualizados** en todos tus dispositivos a través de fuentes fiables
- Asegúrate que el **bloqueo automático está activado**

2 Sé discreto online y en público

- **Busca tu nombre en Google** para comprobar qué información está disponible en la red
- Comprueba los **ajustes de privacidad** en tus redes sociales

3 Piensa antes de hacer clic o responder

- **Sé cuidadoso a la hora de abrir links**, archivos adjuntos o descargar carpetas desde emails sospechosos
- **Si no estás seguro, llama/envía un mensaje o un email** al remitente utilizando los datos de contacto que ya tengas o estén disponibles públicamente, no los reflejados en el email sospechoso

4 Mantén tus contraseñas seguras

- **Utiliza passphrases** (3 o más palabras) como contraseñas, son más fáciles de recordar
- Cuando sea posible, utiliza **Autenticación de Múltiples Factores** (AMF) para que tus cuentas sean aún más seguras

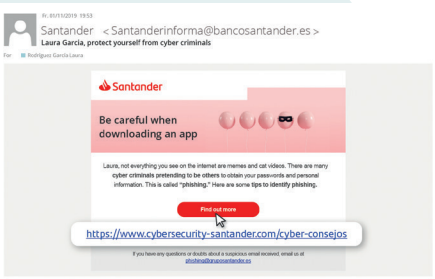
5 Si sospechas, repórtalo

- Cuando recibas una llamada, mensaje o email que te haga desconfiar, **repórtalo a la empresa o individuo**. Podrán comprobar si es legítimo.
- Cuando contactes con la empresa o individuo, utiliza información que ya tengas o esté disponible públicamente, **no la que esté reflejada en el email sospechoso**.

Mantente seguro online y comparte estos consejos con otras personas para que también lleven una vida digital segura.

Recuerda, ¡cada clic cuenta!

Santander



Phishing

Un intento fraudulento de conseguir información personal utilizando técnicas de ingeniería social o haciéndose pasar por entidades fiables en una comunicación digital.

Malware

Se trata de un tipo de software que afecta o daña un dispositivo accediendo a él sin que el usuario sea consciente.

Virus

Un virus informático es un programa utilizado para provocar alteraciones en el funcionamiento de un dispositivo sin el permiso o conocimiento del usuario.

AMF

Autenticación de Múltiples Factores (AMF) es una manera especialmente segura de iniciar sesión que no solo requiere una contraseña, sino que también utiliza otros pasos adicionales de verificación como un código de confirmación o tu huella.

Web segura

HTTPS (HyperText Transfer Protocol Secure, Protocolo de transferencia de hipertexto en español) es un protocolo de comunicación que protege los datos de los usuarios cuando se transmiten entre sus ordenadores y el sitio web. Tiene una capa más de seguridad que el sistema HTTP.

Copia de seguridad

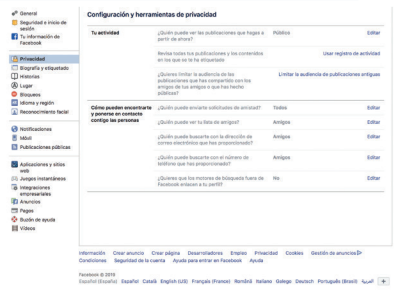
Es una copia de información que se realiza en un dispositivo distinto al inicial. El objetivo es poder recuperar los datos en caso de la pérdida de información.

Ingeniería Social

Es la práctica de obtener información confidencial a través de la manipulación y suplantación de identidad de usuarios.

Passphrase

Es una contraseña de 3 o más palabras (como una frase) que aumenta la seguridad por ser más difícil de descifrar que una contraseña de una sola palabra.



Ajustes de privacidad

Una serie de preferencias que el usuario puede gestionar para controlar qué información comparte y con quién.

Encriptado

La encriptación o cifrado de un mensaje consiste en transformar el contenido de este, a través de un algoritmo, para que solo usuarios autorizados (que conozcan el algoritmo) puedan acceder a él.

Santander