

1. **Activá la autenticidad de dos factores**
2. **No brindes ningún dato personal**.
3. **No ingreses datos personales en sitios por medio de enlaces que llegan por correo electrónico.**
4. **Usá contraseñas fuertes**.
5. **Leé cada correo electrónico recibido con cuidado.**
6. **Tené cuidado con los enlaces sospechosos y asegurate siempre de estar en la página legítima.**
7. **No uses equipos públicos o de terceras personas para acceder a aplicaciones, redes sociales o cuentas personales que requieran contraseñas.**

**OTRAS MODALIDADES DE ENGAÑO O ESTAFA FRECUENTES**

**¿Qué es el phishing?**

*Es un correo electrónico que aparenta ser legítimo que se utiliza para que la persona destinataria abra un enlace, complete formularios con información personal o descargue archivos que contienen malware o programas maliciosos. En caso de recibirlo se recomienda eliminarlo*

*.*

**¿Qué es el smishing?**

*Es una modalidad de estafa mediante mensajes de texto o cualquier aplicación de mensajería que tiene como objetivo obtener información privada. Al igual que los casos de phishing la recomendación es eliminar el mensaje.*

**¿Qué es el spoofing?**

*Es el uso de técnicas de suplantación de identidad. Tipos de spoofing, el envío de correos electrónicos o páginas fraudulentas, falsificación de dispositivos o de direcciones IP. Quienes realizan este tipo de fraudes buscan hacerse pasar por otras personas, organizaciones o empresas para acceder a datos personales, distribuir malware o generar algún tipo de perjuicio.*



***QUÉ HACER SI DETECTÁS UN FRAUDE VIRTUAL O UN ENGAÑO:***

*Podés comunicarte con la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI).*

*Dirección: Sarmiento 663, 6° Piso, CABA*

*Teléfono: (+54 11) 5071-0040 / 0041*

***Correo electrónico:*** *denunciasufeci@mpf.gov.ar*

*Si recibís información o mensajes que simulan ser del Banco Central podés reenviarlos a Ayuda en Línea (ayudaenlinea@bcra.gob.ar).inmediatamente.*