Uso seguro de **tarjetas**

Con el uso de las tarjetas de débito y crédito se obtienen muchas ventajas y comodidades. Sin embargo es importante tener en cuenta algunas medidas para protegerse.

¿Cómo usar tus tarjetas de forma segura?

- ✓ Evitá perder de vista tu tarjeta al realizar pagos en locales comerciales.
- ✓ No prestes tu tarjeta ni permitas que otras personas la utilicen en tu nombre.
- ✓ En caso de robo o extravío de tu tarjeta, reportalo a tu banco de inmediato.
- ✓ Evitá que otras personas vean tu PIN al ingresarlo.
- ✓ Evitá dejar tu tarjeta o documentación personal en el automóvil, habitaciones de hotel sin caja fuerte o lugares públicos.
- ✓ Guardá tus comprobantes de operación por lo menos hasta que recibas los estados de cuenta.
- ✓ Si no vas a utilizar tu tarjeta nuevamente, destruila raspando la firma y cortando el plástico en fragmentos pequeños y luego desechala por separado.
- ✓ Al recibir tu tarjeta, asegurate de que el sobre no se encuentre abierto y seguí las indicaciones que figuran dentro de él.

Seguro **te conectás**

CERTuy
CENTRO NACIONAL DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA

agesic
DESARROLLANDO EL URUGUAY DIGITAL

PRESIDENCIA
República Oriental del Uruguay

Seguro te conectás

/seguroteconectas

CERTuy
CENTRO NACIONAL DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA

agesic
DESARROLLANDO EL URUGUAY DIGITAL

PRESIDENCIA
República Oriental del Uruguay

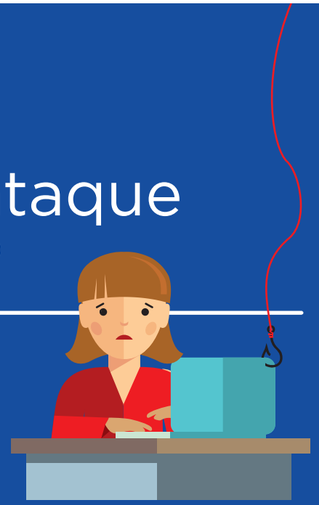
Uso seguro de **contraseñas**

Las contraseñas son las llaves de acceso a los sistemas que usamos (mail, red social, banca electrónica) y, por tanto, deben elegirse y protegerse de forma adecuada.

¿Cómo podés proteger tus cuentas?

- Elegí contraseñas que no contengan palabras relacionadas con el sitio utilizado o con características personales.
- Procurá tener diferentes contraseñas para cada servicio. De esta forma, si se comprometen los datos de una cuenta no se verán afectadas las demás.
- No accedas a tu cuenta bancaria o correo electrónico desde equipos en cibercafés o aeropuertos.
- Cambiá todas tus contraseñas regularmente; de esta forma, en caso de haber sido comprometidas, dejás sin acceso al atacante.
- Utilizá contraseñas complejas, es decir, de más de 8 caracteres, que contengan espacios, símbolos, números, mayúsculas y minúsculas.

¿Qué es un ataque **de phishing?**



El phishing es un tipo de ataque informático con el que se obtiene información personal o financiera de los usuarios como contraseñas, números de tarjetas de crédito o cuentas bancarias.

El ataque de phishing ocurre mediante correos electrónicos que le llegan al usuario y que imitan el formato, el lenguaje y la imagen de los mensajes emitidos por los bancos u otras instituciones. Estos mensajes engañosos siempre solicitan a los usuarios la confirmación de sus datos personales alegando problemas técnicos, cambios en las políticas de seguridad o fraude, entre otros.

¿Qué podés hacer para prevenir un ataque por Phishing?

→ Cuando accedas a tu banco en línea, evitá acceder a través de links, ingresá manualmente la dirección.

→ Antes de iniciar sesión para ingresar a tu cuenta bancaria, confirmá que la dirección web del banco sea la correcta y corroborá si en la barra del navegador aparece el candado que indica la autenticidad del sitio.

→ Tené presente que un banco nunca te solicitará información personal o confidencial por correo electrónico o por teléfono. En caso de recibir una notificación de este tipo, comunicate con tu banco de forma inmediata.

¿Qué es el **ransomware?**

El ransomware es el equivalente informático a un secuestro. Con este tipo de ataque se le bloquea al usuario el acceso a su información o equipos. De esta manera, solo el atacante puede recuperar esa información, por lo que exige un pago al usuario atacado a cambio de sus propios datos.

¿Qué podés hacer para estar preparado ante un ransomware?

Respaldá tu información de forma periódica, de modo que si sos víctima de ransomware puedas recuperarla sin pérdidas significativas.

No abras mensajes de correo electrónico no deseado, ni hagas clic en vínculos de sitios web sospechosos.

Evitá abrir archivos que provienen de fuentes poco fiables (mails con remitentes desconocidos, pendrives perdidos, entre otros).

Instalá un antivirus y mantenelo actualizado.