Departamento de TIC

Capsula informativa

Protege tus datos personales: Toma medidas contra el phishing

¿Qué es el phishing?
El *phishing* es una técnica usada por delincuentes para engañarte y robar tu información personal, como contraseñas, números de tarjetas o datos bancarios. Lo hacen enviándote correos falsos o mensajes que parecen reales.

Paso 1: Aprende a reconocer un intento de phishing

Correos urgentes o alarmantes: Si recibes un correo diciendo que tu cuenta será bloqueada o que ganaste un premio, *desconfía*.

- **Errores de ortografía y redacción rara:** Muchos mensajes falsos tienen faltas o frases extrañas.
- **Direcciones de correo raras:** Si el correo dice venir de tu banco, pero la dirección termina en algo como `@ofertas123.com`, es falso.
- **Enlaces sospechosos:** Coloca el mouse sobre el enlace (¡sin hacer clic!) y mira si la dirección web coincide con la que dice el mensaje.

Paso 2: No hagas clic en enlaces ni descargues archivos

- Si no estás seguro de quién te envió el mensaje, **no abras enlaces ni archivos adjuntos**. Pueden instalar virus o llevarte a páginas falsas.

Paso 3: Verifica siempre por otra vía

- Si te llega un correo del banco o una empresa, llama por teléfono al número oficial o entra tú mismo al sitio web escribiendo la dirección en el navegador. **Nunca uses los enlaces del correo.**

Paso 4: Usa contraseñas seguras y diferentes

- Crea contraseñas largas, con letras, números y símbolos (ejemplo: `Sol@2025segura!`).
- **No uses la misma contraseña en todo.**

Paso 5: Activa la verificación en dos pasos

- Muchos servicios (como Gmail, Facebook, bancos) ofrecen *verificación en dos pasos*. Así, aunque alguien tenga tu contraseña, no podrá entrar sin un código que llega a tu celular.

Gracias.