PHISHING Y VISHING

LA MEJOR PROTECCIÓN ES ESTAR ALERTA E INFORMADOS

Phishing

El Phishing es un tipo de fraude informático que busca suplantar tu identidad. Consiste en tratar de obtener información financiera o personal como datos de tarjetas de crédito o claves de acceso.

Los medios electrónicos que más se utilizan para obtener tus datos son: email, redes sociales, páginas y links falsos o archivos adjuntos, entre otros. En ocasiones, el Phishing también puede ser utilizado para infectar los dispositivos con algún tipo de malware (programa malicioso/virus).

¿Cómo protegerte del Phishing?

- Recordá que las cuentas oficiales de nuestras Redes Sociales tienen este ícono que te dará indicio de que la cuenta está verificada.
- Ingresá a nuestros sitios tipeando la url en el navegador, nunca haciendo una búsqueda online, ni tampoco sobre un hipervínculo incluido en un correo electrónico.
- Escribí siempre la dirección web utilizando HTTPS://... Y verificá que el sitio tenga el candado verde de sitio seguro.
- Mantené actualizados los sistemas operativos, aplicaciones, antimalware y antivirus.
- Prestá atención si el correo solicita información confidencial, personal o financiera. No debés compartir, por ningún medio, claves de acceso como la de tu correo electrónico, tu banco, etc.
- No confíes en mails redactados con sentido de urgencia, grandes premios, regalos, cuentas bancarias bloqueadas, etc. Contactá directamente con la entidad en cuestión.
- Desconfiá de los correos con mala ortografía y otros errores de redacción.

Vishing

Existe otra modalidad llamada Vishing, que se refiere a estafas que se realizan por teléfono con el objetivo de obtener información crucial de carácter financiero o personal. El Vishing opera igual que el Phishing, pero no siempre se realiza a través de Internet, sino que muchas veces se lleva a cabo mediante tecnología de voz. Los estafadores en técnicas de Vishing utilizan una serie de técnicas para dar la apariencia de legitimidad:

- Información correcta: tienen tu nombre, dirección, número telefónico e información bancaria.

PHISHING Y VISHING

- Urgencia: te hacen creer que tu dinero está en peligro, y que tenés que actuar con rapidez.
- Atmósfera empresarial: se escucha mucho ruido de fondo, de modo que da la impresión de ser un Call Center

¿Cómo protegerte del Vishing?

- Nunca llames al número que te dieron, o al que muestra tu identificador de llamadas. Tomate el tiempo para buscar el número legítimo y llamá a ese número.
- Nunca brindes información personal.
- Si recibís una llamada sospechosa, simplemente colgá.