CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS DE SEGURIDAD PARA EVITAR LOS PELIGROS DEL SMISHING

El Smishing

Es una estafa digital enviada a través de **SMS** y **WhatsApp**, para que los usuarios descarguen malware, visiten sitios fraudulentos o llamen a números falsos, y así robar su información personal.

El factor de riesgo en estos casos, aumenta por la distracción producida por el uso constante de tu celular

Características

1. Hablan sobre falsas emergencias, como bloqueo de tarjetas o premios, para que se haga clic sin pensar
2. Piden confirmación para falsas facturas o información de despacho de paquetería.
3. Frecuentemente vienen de números desconocidos, no de contactos.
4. Tienden a aprovecharse de eventos como las vacunas contra el Covid-19 o la Operación Renta.
5. Muchas veces se hacen pasar por bancos o grandes empresas.

Cómo evitar ser víctima

- **DESCONFÍA** de los SMS que provienen de fuentes desconocidas.
- **NUNCA** entregues tus claves, código de recuperación o información financiera por teléfono o mensajería.
- **DUDA** si recibes SMS sospechosos de un contacto, llámalo y pregúntela si realmente lo envió.
- **REVISA** el contenido, que no sea alarmante o tenga faltas de ortografía.

Cómo evitar ser víctima

- **NUNCA** respondas a tu banco a través de SMS o apps de mensajería. Ante dudas, escribe a tu ejecutivo o llama a la mesa central del banco.
- **EVITA** descargar aplicaciones en el enlace de un SMS. Hazlo siempre de la tienda oficial (AppStore o Google Play).
- **CONSIDERA** instalar programas de seguridad anti-malware en su celular.

SI CAES EN EL ENGAÑO

- **BLOQUEAR** la tarjeta o cuenta afectada cuanto antes.
- **CAMBIAR** claves y contraseñas.

Si recibes mensajes falsos o detectas algún sitio fraudulento

DENUNCIA CSIRT 24/7

22486 3850

También a la **PDI**

22708 0658