Seguridad Informática

¿Cómo evitar ser Robado, Engañado y Molestado?

Suplantación de identidad:

Técnica que usan los estafadores para engañar a la gente y así obtener información para su beneficio. Existen diferentes técnicas de suplantación de identidad.

1. Correo electrónico:

Los estafadores envían correos con links a sitios falsos, archivos con virus mediante engaños para conseguir información personal. Son correos no deseados, con remitente desconocido.

Características:

- Demasiado bueno para ser verdad.
- Sentido de urgencia.
- Links extraños y no confiables.
- Archivos adjuntos.
- Remitente inusual.

Recomendaciones:

- No responder a correos no deseados.
- Desconfiar de remitentes desconocidos.
- Evitar abrir links y/o archivos.
- Bloquear remitentes desconfiables.
- Denunciar como intento de suplantación de identidad.
- Marcar correo como no deseado (spam).

2. Páginas falsas:

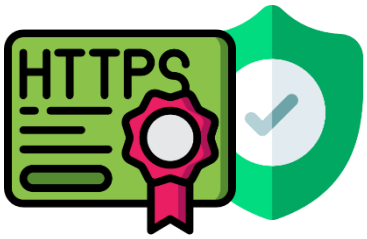
Los estafadores administran una página supuestamente oficial e intenta adquirir información personal haciendo que parezca un sitio de confianza.

Características:

- Por lo general no cuenta con https.
- Pide llenar formularios con información personal.

Recomendaciones:

- Si utilizas tarjeta de crédito o cuentas, revisar que la página comience con https://
- Para páginas en las que no se utilice información personal no es necesario contar con el candado de seguridad.



3. Extorsión telefónica:

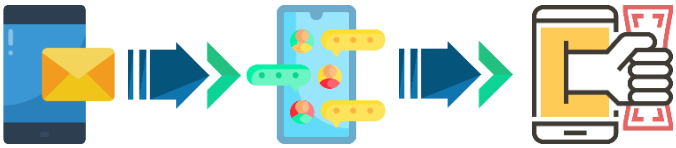
Los extorsionador busca engañar a la gente usando información básica para que se le proporcionen datos confidenciales y así usarlos en su beneficio.

Recomendaciones:

- No des información delicada si te llaman por teléfono.
- Puedes buscar el número en internet para ver si ha tenido reportes.
- Si crees que intentan extorsionarte o es molesto, lo mejor es bloquear el número.

4. Mensajes falsos:

Se mandan mensajes a la victima engañándola para que ingrese en páginas falsas o que llame a algún número para reclamar premio o promoción.



Características:

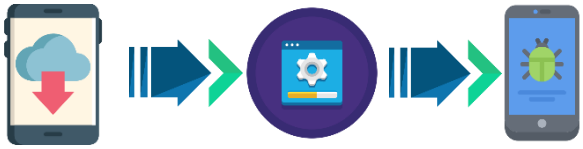
- Links a páginas extrañas.
- Dicen que has ganado un premio.
- Suelen también estar en cadenas de WhatsApp.

Recomendaciones:

- Los operadores de telefonía y bancos no piden contraseñas por mensajes.
- No respondas a estos mensajes.
- Si crees que intentan engañarte, puedes bloquear el número.
- No des click a enlaces extraños que llegan por mensaje.
- Si se hacen pasar por tu banco, llámalos tú directamente.

5. Apps desconocidas:

En internet existen aplicaciones que pueden llegar a tener algún tipo de virus que al descargarlo e instalarlo puede infectar tu celular con él.



Características:

- Estas aplicaciones suelen estar en sitios no autorizados.
- Después de instalada, suelen haber cambios molestos en tu celular.

Recomendaciones:

- Revisa la valoración y comentarios antes de descargar una aplicación.
- Revisa los permisos que solicita la aplicación.
- Mantén tu celular actualizado.
- Puedes buscar la aplicación en su sitio web oficial.
- Si tienes una aplicación molesta, desinstálala.