- Con frecuencia, tienen por objeto captar direcciones de correo electrónico, los datos personales, listas de contactos, tipo de dispositivo utilizado, etc. que utilizan para otros fines lucrativos.

Además, es importante que conozcas cómo funciona el phishing:

Los ciberdelincuentes que ponen en circulación el phishing, utilizan la ingeniería social para intentar obtener nuestra información privada. Captan nuestra atención con alguna excusa con el fin de redirigirnos a páginas web fraudulentas que simulan ser las legítimas de un determinado servicio o empresa.

Cualquier sistema que permita el envío de mensajes puede ser usado como medio para intentar robar nuestra información personal.

En algunos casos pueden llegar intentos de robo de nuestra información personal a través de emails, mensajes SMS (SMiShing), de la misma manera que por cualquier herramienta de mensajería instantánea (como WhatsApp) o red social.

Consejos y recomendaciones

En general:

◆ Cualquier entidad con cierta reputación, se comunica con sus clientes a través de sus páginas web y de sus medios de comunicación oficiales. Si recibes un mensaje de una red social, banco o cualquier otro servicio conocido, etc. no abras el mensaje y accede a su web directamente tecleando la URL desde el navegador.

◆ Si realmente recibes una alerta importante, los medios de comunicación también habrán sido informados, revisa las webs de los principales medios de comunicación.

◆ Si dudas sobre la veracidad de un determinado mensaje, pregunta a la parte implicada directamente.

◆ **No reenvíes cadenas con mensajes alarmistas**, especialmente aquellas que tienen enlaces a sitios web o a descarga de apps que desconocemos. Desconfía de las cadenas de mensajes, no accedas a los enlaces que contienen, ni instales una app para ver una noticia.

◆ Revisa las opciones de configuración de tus apps de mensajería instantánea y redes sociales para tener controlado quién puede contactar contigo.

- Trucos para evitar ser víctima de phishing:

◆ Sé precavido ante los correos que aparentan ser entidades bancarias o servicios conocidos con mensajes del tipo:

- ❖ Problemas de carácter técnico de la entidad.
- ❖ Problemas de seguridad en la cuenta del usuario.
- ❖ Recomendaciones de seguridad para evitar fraudes.
- ❖ Cambios en la política de seguridad de la entidad.
- ❖ Promoción de nuevos productos.
- ❖ Vales descuento, premios o regalos.

- ❖ Inminente cese o desactivación del servicio.

◆ Sospecha si hay errores gramaticales en el texto.

◆ Si recibes comunicaciones anónimas dirigidas a “Estimado cliente”, “Notificación a usuario” o “Querido amigo”, es un indicio que te debe poner en alerta.

◆ Si el mensaje te obliga a tomar una decisión en unas pocas horas, es mala señal. Contrasta directamente si la urgencia es real o no con el servicio a través de otros canales.

◆ Revisa que el texto del enlace coincide con la dirección a la que apunta.

◆ Un servicio con cierto prestigio utilizará sus propios dominios para las direcciones de email corporativas. Si recibes la comunicación desde un buzón de correo tipo @gmail.com o @hotmail. com, no es buena señal.

- ¿Qué debes hacer si detectas un caso de phishing?

◆ No contestes en ningún caso a estos correos. Si tienes dudas pregunta directamente a la empresa o servicio que representa o ponte en contacto con la Oficina de Seguridad del Internauta para hacerles llegar tu consulta.

◆ No accedas a los enlaces facilitados en el mensaje ni descargues ningún documento adjunto.

◆ Elimínalo y, si lo deseas, alerta a tus contactos sobre este fraude.

No hagas clic en enlaces que recibas a través de un mensaje para acceder a un sitio web en el que te tienes que identificar o facilitar información personal.

Bibliografía

Los consejos y recomendaciones provienen de las siguientes fuentes oficiales:

[1] Instituto Nacional de Ciberseguridad de España (INCIBE): https://www.incibe.es/

[2] Oficina de Seguridad del Internauta (OSI): https://www.osi.es/

[3] Agencia Española de Protección de Datos (AEPD): https://www.aepd.es/