20210220, Nota Informativa, cómo actuar ante la suplantación de identidad y secuestro de cuentas.

En virtud de mis compromisos contractuales, seguidamente quiero participaros de la información publicada por la Oficina de Seguridad del Internauta (OSI) el día 5 de este mes sobre cómo actuar ante una suplantación de identidad o el secuestro de cuentas.

Es conocido que cada vez son más los casos de suplantación de identidad a los que se enfrentan los usuarios. Por este motivo, desde la OSI se publican una serie de consejos para ayudar tanto a prevenirlos como a actuar en caso de ser víctima de alguno. Hay muchos tipos de suplantación, por eso, se recomienda seguir todos los consejos y pautas que se detallan a continuación. Y que puedes consultar directamente en la página del OSI mediante este enlace:

https://www.osi.es/es/actualidad/blog/2021/02/05/suplantacion-de-identidad-y-secuestro-de-cuentas-como-actuar

En los últimos meses, en la OSI, canal especializado en ciudadanos de INCIBE, se han recibido un gran número de solicitudes de ayuda y denuncias sobre casos de suplantación de identidad y robo de cuentas. Por ello, se procede a repasar los fundamentos y conceptos básicos en los que se basan este tipo de prácticas fraudulentas, así como varios consejos y recomendaciones para protegernos.

¿Qué es la suplantación de identidad?

Se trata de una actividad malintencionada que busca hacerse pasar por otra persona o entidad por diferentes motivos: robo de datos, fraudes y engaños para obtener información o un beneficio económico, ciberacoso, extorsión, grooming, etc.

Los ataques y fraudes basados en la suplantación de identidad pueden ser muy variados, aunque se distinguen principalmente por dos cosas:

- **Robo o acceso no autorizado a una cuenta**: cuando el atacante ha conseguido acceder a nuestra cuenta haciendo uso de nuestras contraseñas, que ha obtenido a través de distintas técnicas y ataques. En este caso, puede suponer la pérdida del control de nuestra cuenta si el ciberdelincuente cambia la clave de acceso y los métodos de recuperación, aunque en otros casos el atacante puede que solo utilice la cuenta para publicar en nuestro nombre, ver datos almacenados, etc.; todo ello sin nuestro consentimiento.
- **Creación de un perfil falso**: el atacante ha creado una cuenta o perfil muy similar al nuestro o al de otra persona, entidad o empresa. Para ello, utiliza información que ha podido conseguir fácilmente a través de Internet y no implica el robo de nuestra cuenta ni accesos no autorizados.

Os mostramos los **tipos de suplantación de identidad** que más incidencia están teniendo entre los usuarios en este momento:

Robo o secuestro de cuentas de WhatsApp en cadena

Si un atacante instalase WhatsApp en otro dispositivo utilizando nuestro número, nos llegaría por SMS un código de verificación para confirmar que somos nosotros los que estamos configurando la app

en otro dispositivo. Es entonces cuando el ciberdelincuente trataría de engañarnos para que le facilitásemos el código de verificación, haciéndose pasar por un contacto conocido (familia o amigo) que ha cambiado de número y, por seguridad o dudas, prefirió utilizar nuestro teléfono para recibir el SMS.

Si lo compartimos, el atacante nos quitará el control de la cuenta y activará la verificación en dos pasos para evitar que podamos recuperarla fácilmente.

Más detalles sobre cómo funciona este fraude en: ¡Socorro me han secuestrado WhatsApp!

¿Cómo podemos protegernos?

- No compartiendo nunca el código de verificación con nadie. Si alguien nos los solicita, debemos desconfiar.
- Activando la verificación en dos pasos. Incluso si obtienen nuestro código, con esta función no podrán robarnos la cuenta.

Secuestro de nuestras cuentas personales

Mediante ataques a nuestras contraseñas o técnicas basadas en ingeniería social, como el phishing, los atacantes son capaces de hacerse con nuestras credenciales y secuestrar nuestras cuentas. Una vez que están bajo su control, tendrán total libertad para lanzar

fraudes en nuestro nombre, obtener información personal, cambiarnos la contraseña y los datos de recuperación de la cuenta y pedirnos incluso un rescate a cambio de recuperar el control de la misma.

Este tipo de prácticas no se limitan solo a las redes sociales, sino que pueden afectar a nuestras cuentas de correo electrónico o de otros servicios digitales, por lo que conviene revisar detenidamente las opciones de seguridad y privacidad para prevenirlo.

¿Cómo podemos protegernos?

- Configurando correctamente las opciones de privacidad y seguridad de nuestra cuenta.
- Activando la verificación en dos pasos y utilizando contraseñas robustas.
- No aceptando peticiones de amistad de usuarios desconocidos o con perfiles falsos.
- Publicando solo la información que queramos que sea visible y protegiendo los datos más sensibles, como dirección, correo electrónico, DNI, datos bancarios, etc. para que no nos puedan extorsionar a través de otros medios.

Suplantación de identidad y difusión de fraudes entre contactos y seguidores

En este caso, los atacantes tienen como objetivo suplantar aquellas cuentas con muchos seguidores, tanto de usuarios particulares como empresas, como un medio para engañar al mayor número de usuarios posibles y dañar la reputación del perfil legítimo.

Su *modus operandi* es la creación de una cuenta falsa que guarda un gran parecido, casi idéntico, a la cuenta oficial, que en ocasiones solo

se diferencian por un carácter en el alias o *nickname*. De esta forma, los usuarios despistados siguen creyendo que son las cuentas "buenas". Es entonces cuando el atacante aprovechará para lanzar y publicar desde los perfiles fraudulentos sorteos o campañas de publicidad falsas, con enlaces maliciosos o formularios con los que recoger información personal de los usuarios víctimas.

Existe una variante donde la cuenta suplantada es la de un contacto nuestro (familiar o amigo), que el atacante utiliza para solicitarnos ayuda económica o que nos descarguemos algún tipo de *software* malicioso.

¿Cómo podemos protegernos?

- Desconfiando de cualquier petición de amistad por parte de desconocidos.
- Confirmando que estamos siempre siguiendo a un perfil legítimo. Ante la duda, será mejor contrastar la información utilizando otras fuentes de confianza.
- Si un contacto nos solicita ayuda o nos realiza una petición que nos genera dudas, debemos contactar con él por otra vía para verificar que es cierta la información.

SIM *swapping*

Este tipo de ataque de suplantación de identidad se basa en la duplicación de nuestra tarjeta SIM, y para ello, los atacantes necesitan algunos datos personales, como nombre y apellidos, DNI, fecha de nacimiento, los 4 últimos dígitos de nuestra cuenta bancaria, etc., que han podido obtener por otras vías, como el phishing o comprando en tiendas online fraudulentas.

Con estos datos, los atacantes solicitan un duplicado de nuestra SIM, suplantando nuestra identidad con los datos anteriores ante la operadora. Mientras, lo único que notamos es que nuestro dispositivo se queda sin cobertura móvil, y cuando nos conectemos a una red wifi, comenzaremos a recibir notificaciones de movimientos realizados desde nuestro móvil sin nuestro consentimiento, como transferencias bancarias o compras online, entre otras.

¿Cómo podemos protegernos?

- Contactando con nuestra compañía telefónica si nos quedamos permanentemente sin cobertura en sitios donde habitualmente tenemos.
- Utilizando solo servicios de confianza y protegiendo nuestras cuentas con credenciales robustas y la verificación en dos pasos.
- Conociendo las distintas técnicas de ingeniería social que utilizan los ciberdelincuentes para hacerse con nuestros datos.

Phishing, smishing y vishing

Estos ataques basados en ingeniería social se sirven de la suplantación de identidad para hacerse pasar por nuestros contactos o entidades de confianza a través del correo electrónico, SMS o llamadas telefónicas, respectivamente. Su principal objetivo es engañarnos para que realicemos una acción bajo cualquier pretexto: acceder a una web para que facilitemos datos privados, descargar un fichero malicioso, realizar un pago, etc.

¿Cómo podemos protegernos?

- Desconfiando de cualquier mensaje o llamada de desconocidos que intente obtener información personal.

- No descargando ni haciendo clic en ningún archivo o enlace sospechoso.
- Verificando la legitimidad del mensaje utilizando otras vías, por ejemplo, contactando directamente con la empresa o servicio que dice ser.

¿Qué podemos hacer si detectamos una suplantación de identidad o nos han robado el acceso a la cuenta?

Si creemos que estamos sufriendo una suplantación de identidad o somos víctimas de algún fraude donde se ha suplantado la identidad de alguna entidad o persona, debemos seguir las siguientes recomendaciones:

1. **Documentar todo lo ocurrido**, recabando copias de los correos o mensajes con capturas de pantalla, y revisar nuestras cuentas para comprobar cuáles han podido ser afectadas.
2. **Estar alerta y contactar con nuestros contactos, familiares y amigos** para contarles lo ocurrido y evitar que se conviertan en víctimas del fraude a su vez.
3. **Recuperar las cuentas y cambiar las credenciales** de aquellas donde aún podamos acceder con contraseñas robustas, además de activar el factor de autenticación múltiple o verificación en dos pasos.

Es recomendable que revisemos las opciones de recuperación de cuenta cada cierto tiempo para comprobar que no hayan sido modificadas. Un ciberdelincuente que haya robado una cuenta tratará de cambiar estas opciones lo antes posible, como el teléfono o correo alternativo, para impedirnos recuperar el control de nuestra cuenta.

Informar y denunciar al servicio o aplicación de lo ocurrido

La mayoría de servicios online, como redes sociales o correo electrónico, cuentan con mecanismos para recuperar cuentas "hackeadas" y denunciar la existencia de perfiles falsos o casos de suplantación de identidad.

Finalmente, no olvides recopilar todas las pruebas que puedas y presentarlas a los cuerpos y fuerzas de seguridad del Estado para efectuar la denuncia si lo consideras oportuno. Así, en caso de que se produzca algún delito mientras la cuenta no está bajo tu control, podrás demostrar que no has sido tú. También es recomendable hacerlo en caso de que no consigas recuperar el acceso a tu cuenta.

Además, recuerda que desde INCIBE se ha a disposición de todos los usuarios una Línea de Ayuda en Ciberseguridad, **017,** donde podrás encontrar soluciones a cualquier duda o problema relacionados con la ciberseguridad.

En todo caso, y como siempre, quedo a vuestra disposición para aclarar cualquier duda sobre la cuestión comentada.

Hecho conforme a mi leal saber y entender, en Manilva a 19 de febrero de 2021,

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Nombre de reconocimiento (DN): c=ES, serialNumber=IDCES-32028277H, givenName=SALVADOR, sn=ZOTANO SANCHEZ, cn=ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2021.02.19 11:28:01 +01'00'

Salvador Zotano Sánchez

(Delegado de Protección de Datos Certificado 19-ADK0101 conforme al Esquema AEPD-DPD)