Vishing: Cuando los malos no escriben, sino que llaman por teléfono

Descripción: Nivel de Importancia: ALTA (4)

Una vez más la ingeniería social entra en juego salvo que en esta ocasión el despliegue de técnicas para ganarse la confianza del usuario llega a través de la voz mediante llamadas telefónicas.

Vishing es una práctica fraudulenta a través de llamadas telefónicas en las que se produce la suplantación de identidad de una determinada persona, organización o empresa para obtener información personal, sensible, confidencial de la víctima o directamente para realizar un chantaje telefónico.

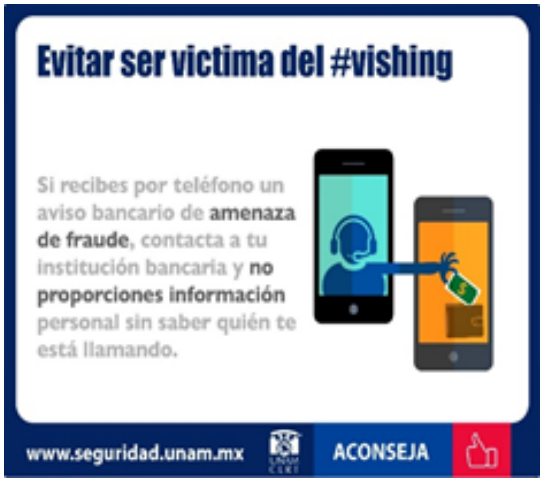
La práctica del vishing se usa para llevar a cabo la estafa del supuesto servicio técnico de una empresa, para hacer una estafa del CEO (Director ejecutivo) más sofisticada, para suplantar una entidad bancaria, extraer información y las credenciales de un usuario o para engañar por la supuesta participación en un sorteo o mil historias, la imaginación de los malos no tiene fin.

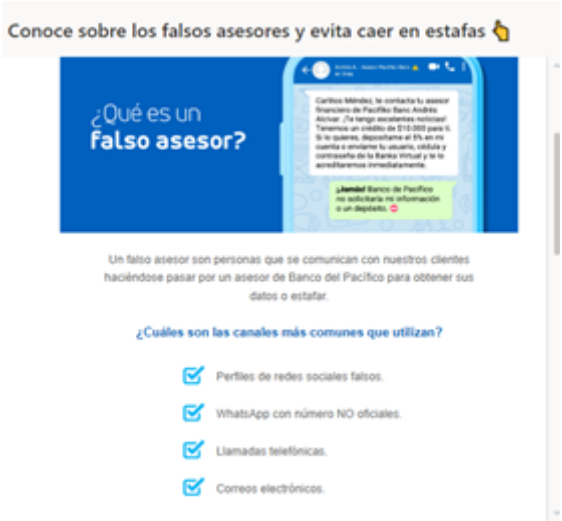
Nunca hay que facilitar datos personales ante la llamada de un desconocido e incluso cuando la persona que llama es conocida y pide datos personales cuando no suele ser lo usual, hay que desconfiar.

Tal y como se explica en la charla “Una mirada a Dark web y la suplantación de identidades” hay fórmulas sencillas de suplantar la identidad de una persona por teléfono incluso herramientas/servicios que permiten suplantar un número de teléfono real.

De esa forma se simplifica el proceso para que la potencial víctima baje la guardia pues al producirse la llamada desde el número de teléfono de una persona conocida o si se combina con DeepFake de audio y se suplanta la misma voz de un conocido, el engaño está hecho.

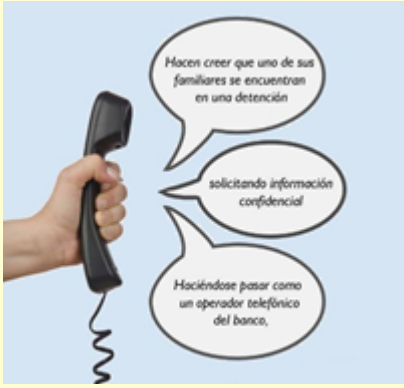
Ahí entran en juego estafas más perfeccionadas o incluso los llamados secuestros express. Ante este panorama conviene ser muy cautos y hay que aconsejar una vez más que hay que practicar la desconfianza, de manera más especial ante desconocidos.





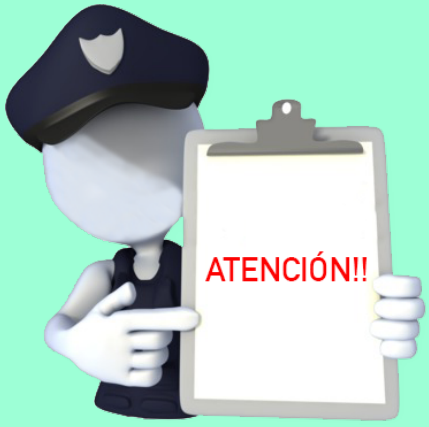
Ejemplo:

En este caso utiliza mensajes de texto para la estafa, pero a su vez el asesor falso puede realizar llamada telefónica al señor Carlitos Méndez de acuerdo a la ilustración de la gráfica anterior, solicitando sus datos personales y depositar en la cuenta bancaria del falso asesor.



Normalmente se hacen pasar por un teleoperador y le indican a la víctima que para participar en un concurso y recibir el premio debe facilitarles datos de su tarjeta de crédito o realizar una transferencia. También hay casos donde se ofrecen 'cheques regalo' o premios a cambio de datos personales y bancarios.
Otra modalidad es donde estos criminales se hacen pasar por servicio técnico de una compañía, advierten de un virus informático y piden la instalación de un programa para acabar con el problema. Este tiene un código malicioso que ataca al dispositivo y da acceso remoto al ciberdelincuente para acceder a toda la información. En ocasiones piden recompensa monetaria a cambio de la información desencriptada.

¿CÓMO PROTEGERNOS?



- No compartir datos personales y sobre todo confidenciales a terceros o a través de medios como correo electrónico, redes sociales, SMS o teléfono.
- Concientizar a todo el personal sobre la ingeniería social y sus modalidades, para evitar este tipo de fraude de los ciberdelincuentes.
- En los casos que se presente este tipo de ciberdelitos se recomienda seguir los procedimientos legales (denuncia).

REFERENCIAS:

https://gmsseguridad.com/vishing-la-estafa-comienza-con-una-llamada-telefonica/