VISHING

EL PHISHING A TRAVÉS DE UNA LLAMADA

¿QUÉ ES?

Es un ataque de Ingeniería Social que busca obtener información confidencial de sus víctimas a través de llamadas telefónicas.

También puede obtenerse información confidencial de las organizaciones a través de sus empleados.

¿CÓMO SE EJECUTA UN VISHING?

1 RECONOCIMIENTO

Los ciberatacantes utilizan diferentes técnicas de recopilación de información para crear un perfil de la víctima. Se conocen detalles específicos, como información personal, gustos, intereses y/o aficiones. Se diseña un ataque personalizado a la víctima en base a la información obtenida.

2 EJECUCIÓN

El ciberatacante ejecuta su ataque, generalmente guionizado. Se gana la confianza de la víctima, haciendo que ésta le desvele información confidencial, como claves de acceso, horarios, direcciones o proyectos confidenciales. Se suele combinar con técnicas de Phishing o Smishing para aumentar la confianza.

3 BARRIDO

Aprovechando la información desvelada, el ciberatacante accede a las cuentas de la víctima, llevando a cabo diferentes acciones que ponen en riesgo su integridad.
La entrada del ciberatacante a las cuentas de la víctima permite también comenzar el proceso con otra víctima de rango superior.

COFM
GOVERTIS
Part of Telefónica Tech

VISHING

EL PHISHING A TRAVÉS DE UNA LLAMADA

TIPOS ALTERNATIVOS DE VISHING

WARDIALING

Sistema automatizado de llamadas en serie a diferentes códigos de área específicos con un mensaje en el que se involucra a bancos, por ejemplo. Al responder se escucha una grabación que solicita al usuario información confidencial.

VOIP

Sistema telefónico basado en Internet. La conversación inicia y termina con una voz automatizada en un ordenador en cualquier lugar del mundo. El gancho es la voz, ya que es muy similar a la utilizada por las grandes empresas para contactar con sus clientes.

DEEPFAKE

El DeepFake es una técnica de Vishing que utiliza la Inteligencia Artificial para suplantar la voz de la persona suplantada. Además, oculta la identidad del emisor de la llamada al cambiar la forma en que se muestra su nombre y número en el servicio de identificación de llamadas.

¡PROTÉGETE!

Evita proporcionar datos confidenciales a través de una llamada telefónica; recuerda que la sensación de urgencia es sinónimo de fraude.

En vez de llamar a un número que te proporcionen en un SMS, contacta con la empresa o servicio a través de sus canales oficiales para que validen la veracidad del SMS.

Ante cualquier duda, consulta con el equipo de seguridad interna corporativo o el equipo de IT.

¡LA SEGURIDAD DIGITAL COMIENZA CONTIGO!

COFM
GOBERTIS
Part of Telefónica Tech