SMISHING

1. ¿Qué es el smishing?

El smishing (Combinación de las palabras SMS y Pishing), es el intento de fraude para obtener información personal, financiera o de seguridad a través de un mensaje de texto o SMS. Al igual que el phishing el smishing tiene como objetivo de robar información privada o realizar una estafa.

La mayoría de las personas están familiarizadas con el phishing y han aprendido a identificar un correo malicioso donde se pide compartir información, descargar archivos o dar click en enlaces que son enviados a través de correo electrónico; sin embargo, cuando se recibe un mensaje de texto se da por sentado que es auténtico y se comparte información personal, en especial bancaria, se accede a pagar por un servicio o se da click en un enlace.

2. Objetivos del smishing

Los objetivos del smishing son:

- Obtener información personal, como por ejemplo claves o datos bancarios. También se envían mensajes para vender productos que no existen o avisos de premios que se ha ganado en un sorteo.

- Infectar el teléfono móvil con alguna aplicación maliciosa, en este caso se enviará un enlace para descargar una aplicación de apariencia legítima e infectar el dispositivo móvil y de esta forma acceder al teléfono. La aplicación instalada suplanta a una oficial, en algunos casos, contiene un troyano bancario por lo que si el usuario accede a la banca online desde su dispositivo, los delincuentes podrán robar las credenciales de acceso e interceptar los mensajes SMS enviados como doble factor de autenticación permiten confirmar la realización de transferencias bancarias.

- Enviar por mensaje de texto un link a páginas web con la finalidad de sustraer información de tarjetas de crédito o datos personales para acceso a servicios financieros.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec

3. Ejemplos de smishing

A continuación se muestran algunos ejemplos que smishing:

a) Smishing para robo de datos bancarios

Estimado cliente, su tarjeta de crédito ha sido bloqueada por su seguridad. Para desbloquear su tarjeta tiene que visitar urgentemente el siguiente link: www.tarjeta.com y completar la información que le solicita. Tiene 24h.

b) Smishing para acceso a páginas fraudulentas

Esta es la web que te dije www.cbarato.com. Encontrarás marcas como Calvin Klein, Dolce Gabanna, Hugo Boss, Loewe, Chanel etc todo a mitad de precio. Dale un vistazo y me dices…

4. ¿Qué hacer para no ser víctima de smishing?

a) No se debe confiar en mensajes que provienen de números desconocidos.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec

b) Ignorar mensajes que tienen faltas ortográficas, está mal redactado o en otro idioma y que ofrecen premios, descuentos o regalos.
c) No se debe confiar en los SMS que hablan de trabajos (que no existen), premios (sin haber jugado) o paquetes recibidos (sin haberlos pedido)
d) No dar click en links que se envían por mensaje de texto y que el remitente es desconocido. Ante la duda no responder a los SMS.
e) No descargar aplicaciones de sitios no oficiales.
f) No proporcionar información personal o bancaria por mensajes de texto.
g) No almacenar información financiera como número de tarjetas de crédito y contraseñas en el dispositivo móvil.
h) No contestar mensajes de texto de números desconocidos.
i) Debemos estar pendientes de cualquier comportamiento extraño de nuestro dispositivo móvil ya que podría indicar que se ha instalado un malware, como por ejemplo: llamadas a números desconocidos, aplicaciones nuevas instaladas, alto consumo de batería o reinicio constante.
j) Vigilar regularmente el consumo que se realiza, en caso de notar incrementos notables en la factura, contactar a la operadora telefónica.

5. Referencias

- EHACKING. Ethical Hacking consultores. Recuperado el 01 de septiembre de 2021. Obtenido de https://blog.ehcgroup.io/2021/01/22/11/32/58/10533/smishing-por-que-siguen-siendo-tan-efectivas-los-mensajes-sms/noticias-de-seguridad/ehacking/.

- Kaspersky. Recuperado el 01 de septiembre de 2021. Obtenido de https://www.kaspersky.es/resource-center/threats/what-is-smishing-and-how-to-defend-against-it.

- ING. Recuperado el 01 de septiembre de 2021. Obtenido de https://www.ing.es/seguridad-internet/todo-sobre-fraude/que-es-smishing#.

- INCIBE. OSI. Recuperado el 01 de septiembre de 2021. Obtenido de https://www.osi.es/es/actualidad/blog/2013/09/09/fraudes-online-vii-smishing-estafa-que-llega-traves-de-un-sms.

- LISA Institute. Recuperado el 01 de septiembre de 2021. Obtenido de https://www.lisainstitute.com/blogs/blog/smishing-estafa-sms-riesgos-ejemplos.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec