AMCDC

Asociación Mexicana
Contra Delitos Cibernéticos

Reporte Técnico Sobre Correos Electrónicos Apócrifos

Santiago López Montaño - Egresado de la Universidad Autónoma del Estado de México Centro Universitario UAEM Valle de Chalco

fecha viernes 12 de abril del 2019 Chalco Estado de México

RESUMEN

Con el crecimiento de la popularidad de los servicios bancarios online, el robo de datos bancarios se ha convertido en uno de los tipos más habituales de actividades delictivas en internet. Además de robar los datos de acceso a las cuentas bancarias personales y de las empresas, los cibercriminales también roban los números de las tarjetas de crédito.

El uso de tecnologías por parte de los delincuentes hace posible que ellos utilicen elementos como logotipos, tipografía e incluso hasta pueden usar el mismo lenguaje oficial o tipo de discurso para cometer crímenes cibernéticos, desgraciadamente esta pericia ha logrado que algunas personas caigan en la trampa con correos falsos pueden ser víctimas de fraudes electrónicos.

Los cibercriminales mandan correos falsos a cualquier número de personas, con el engaño de que su tarjeta está bloqueada y que para desbloquearla el usuario tiene que entrar a un sitio web para poder desbloquearla. Una vez dando clic en la liga, esta te manda a una página web clonada del banco, empresas, y un sinfín de sitios web que son diseñadas por estos cibercriminales.

Al estar en la página web apócrifa te van guiando y pidiendo tus datos poco a poco, con el pretexto de desbloquear tu tarjeta.

El correo falso a analizar es un correo que fue mandado con el engaño de ser la empresa financiera Bancomer.

INTRODUCCION

El presente documento tiene como objetivo presentar la evolución de las técnicas para obtener información confidencial o privada en internet, ya sea a través de web o a través de programas dañinos además se presentan los consejos básicos para reconocer y evitar este tipo de ataques.

Desde el nacimiento del comercio electrónico, los servicios ofrecidos a través de internet cambiaron radicalmente la manera de hacer negocios ampliando significativamente su horizonte al establecer nuevos modelos de mercado.

Uno de los servicios más representativos surgidos de este nuevo modelo de negocio, es el que brindan las entidades financieras y bancarias al facilitar la realización de operaciones de cualquier tipo, requiriendo para ello tan solo una conexión a internet. Esto posibilita una manera cómoda y eficiente de interactuar con las organizaciones, desde la tranquilidad del hogar y sin necesidad de trasladarse hasta el lugar físico de la misma.

El robo de información confidencial a través de medios virtuales, aprovechando las ventajas y facilidades que ofrece internet, es un nuevo desafío para las jurisprudencias internacionales.

Dependiendo de la legislación de cada país, estos fraudes muchas veces no son ilegales debido a que las leyes no las consideran, destacándose una falta importante de acciones en este sentido

En los últimos años se ha registrado un mayor incremento de estas modalidades delictivas, convirtiéndose en la principal y más peligrosa amenaza para los usuarios que hacen uso de servicios online.

Análisis: Como es que funcionan los correos falsos

1- Una de las principales observaciones de las ligas de este tipo de correos falsos es que se utiliza el protocolo HTTP (**Hypertext Transfer Protocol**), las urls comienzan con http://, este protocolo es inseguro y está sujeto a ataques que pueden permitir al atacante obtener acceso a bancos y a cuentas de un sitio web e información confidencial, HTTPS está diseñado para resistir esos ataques y ser más seguros.

2- La hipótesis de cómo es que los cibercriminales pueden hacer este tipo de delitos es;

Ataque de phishing:

3- Utilizan un servidor que es controlado por el atacante.

Imagen 1 servidor

4 -Crean un dominio web parecido al de un banco.

www.bamcomer.com/ www.bamcomer.com.

Donde la primera es verdadera, con esto se puede lograr que el usuario ingrese al sitio falso cuando comete el error de acceder desde el enlace sin notar la diferencia en el nombre del dominio.

En esta metodología conocida como typosquatting, el atacante puede jugar con los caracteres y registrar una dirección web que a simple vista parece la original.

En algunos casos se hace la ofuscación de url. Evita la fácil lectura de la dirección o url a la que ingresa el usuario.

5- Crean o clonan un sitio web lo más parecida a la página web de un banco, que se alojada en el servidor del atacante.

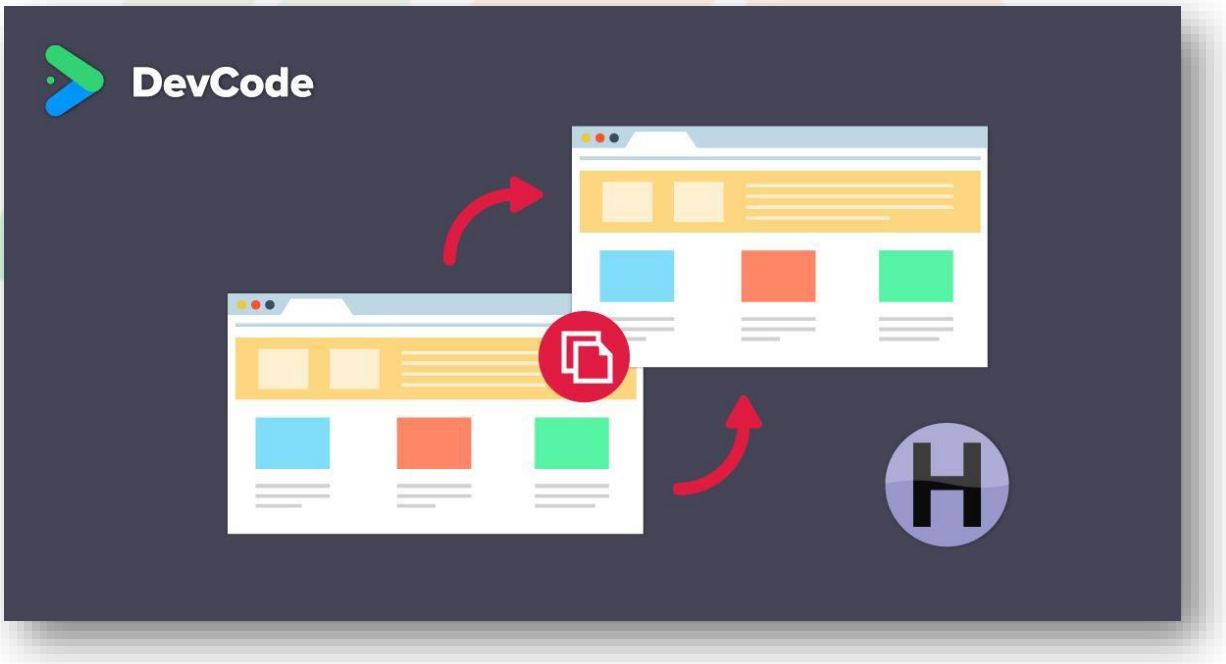

Imagen 2.Clonación de página web.

6- Se mandan correos al azar y en caso de que un usuario del banco se crea lo que este supuesto correo dice y accede a la liga, esta lo llevara a la sitio web falso que está en manos del atacante, le pedirán su información bancaria al proporcionarla esta información se guarda en el servidor del atacante y será utilizada para transferencias ilegales.

Imagen 3 correo falso

Otra de las observaciones de los correos falsos es que, al meternos a las ligas para entrar a la web falsa estas se encuentran caducadas, lo cual quiere decir que los cibercriminales no se arriesgan demasiado tiempo para evitar ser rastrados.

El correo especifico de Bancomer que se investigó cuenta con estos datos.

Teléfono 5556241199 este número no existe

La dirección Venustiano Carranza con el núm. 44 Cuauhtémoc distrito federal titular Bancomer s.a. Es más que evidente que no existen debido a que aún utilizan el nombre de distrito federal a lo que ahora se le llama Ciudad de México

.

Técnicas del robo de información

1. Spam

   Se puede considerar como spam a cualquier mensaje de correo electrónico enviado a varios destinatarios que no solicitaron tal mensaje, también llamado correo electrónico basura; un mensaje de spam debe cumplir con varios aspectos; ser enviado de forma masiva, ser un mensaje no solicitado por el usuario y tener contenido engañoso (habitualmente de tipo publicitario).

   Una vez que el usuario accede al contenido engañoso provisto por el spam, se pueden presentar dos escenarios, el primero, cuando el usuario es direccionado a una página web controlada por el atacante en donde mediante el llenado de formularios proveerá información personal que posteriormente se utilizara para cometer un fraude; el segundo escenario se presenta cuando el usuario descarga el contenido adjunto a spam, lo que se traduce en una invasión a su equipo de cómputo mediante un virus que roba la información del dispositivo.

2. SPim

   Es un caso específico de spam a través del cual se envían mensajes instantáneos cuyo contenido puede incluir spyware, registradores de pulsaciones, virus, vínculos a sitios de phishing o invitaciones para suscribirse a servicios o promociones falsas mediante el envío de mensajes instantáneos a un servidor controlado por el atacante, cuyo objetivo es tomar el control de la lista de contactos para suplantar la identidad del afectado

3. Registradores de pulsaciones

   Es una forma de software espía que guarda las letras que fueron pulsadas en un documento de texto, cuando un usuario que tiene este software instalado está navegando en la web, visitando sitios de comercio electrónico o banca electrónica, el registrador de pulsaciones puede registrar los caracteres digitados, este software es una combinación cuidadosamente elaborada en formato HTML, en la que entre las hojas de estilo capas, cuadros de texto y objetos de contenido, un usuario al estar escribiendo, lo hace en un marco invisible controlado por el atacante.

4. Phishing o suplantación de identidad

   En una estafa en línea, a través de la utilización de spam, sitios web falsos, mensajes de correo electrónico, mensajes instantáneos, cuya finalidad es obtener de los usuarios de internet información confidencial, tales como contraseñas o información detallada sobre tarjetas de crédito y otra información bancaria. El termino proviene de la palabra fishing (pesca) y hace alusión a pescar usuarios para obtener información financiera y sus contraseñas. Los autores del fraude, conocidos como phishers simulan ser empresas legítimas, y pueden utilizar el correo electrónico para solicitar información personal e inducir a los destinatarios a responder a través de sitios web maliciosos.

   Los phishers suelen utilizar tácticas alarmistas o solicitudes urgentes para tentar a los destinatarios a responder. Los sitios de robo de identidad parecen sitios legítimos, ya que tienden a utilizar las imágenes de copyright de los sitios legítimos; sin embargo, no incluyen el protocolo seguro de transferencia de hipertexto https://. Los mensajes fraudulentos generalmente no está personalizados y es posible que compartan propiedades similares, como detalles en el encabezado y en el pie de página.

5. Pharming

   Vulneración que tiene la finalidad de redirigir a un usuario de internet que navega en páginas web a una página falsa diseñada para robarle información persona. A diferencia del phishing, el pharming está programado para atacar al equipo de la probable victima; hace que la navegación web se redireccione a servidores plagados de sitios controlados que tienen un aspecto similar al que el usuario trata de ingresar, es decir cuando la víctima introduce una dirección electrónica correcta, esta es enrutada o redirreccionada hacia el servidor del atacante. El pharming es una granja de victimas

6. Pharming

   Vulneración que tiene la finalidad de redirigir a un usuario de internet que navega en páginas web a una página falsa diseñada para robarle información persona. A diferencia del phishing, el pharming está programado para atacar al equipo de la probable victima; hace que la navegación web se redireccione a servidores plagados de sitios controlados que tienen un aspecto similar al que el usuario trata de ingresar, es decir cuando la víctima introduce una dirección electrónica correcta, esta es enrutada o redireccionada hacia el servidor del atacante. El pharming es una granja de victimas

7. Troyanos bancarios

   A diferencia de los keyloggers convencionales, los troyanos bancarios están diseñados para detectar patrones de cadenas como por ejemplo “password” o “contraseña” cada vez que el usuario ingresa a la zona de registro de la entidad atacada. En ese momento, se activa la captura de información específica, obteniendo los datos de registro del usuario.

8. Re direccionamiento web

   Otra de las técnicas utilizadas por los troyanos bancarios e la denominada DNS Poisoning (envenenamiento de DNS), consiste en modificar los DNS para redireccionar el dominio real ha dirección IP falsa creada por el atacante.

Prevención contra este tipo de correos falsos

Además de enfatizar que las entidades financieras y bancarias jamás solicitan claves, cambios de ellas o información personal de los clientes a través del correo electrónico, es sumamente importante que los usuarios incorporen hábitos de navegación que permitan minimizar el impacto que provoca ser víctima de los ataques descritos anteriormente.

A continuación, se presentan una serie de consejos que ayudan a contrarrestar estas acciones maliciosas.

- Mantener el sistema operativo, el navegador y el antivirus con las ultimas actualizaciones de seguridad disponibles. Esto ayuda a mantener el sistema libre de todo tipo de códigos maliciosas, sobre todo, aquellos que aprovecha técnicas de inyección de código html
- Instalar un antivirus con capacidades de detección proactiva. Debido a la gran variedad de malware.
- Hacer caso omiso a correos electrónicos de origen desconocido o a nombre de entidades financieras o bancarias.

- Evitar introducir datos personales y financieros en sitios desconocidos

- No acceder a sitios web por medio de enlaces incrustados en correos electrónicos, es conveniente acceder a dichos sitios escribiendo directamente la dirección en la barra de navegador del explorador que utilice.
- No operar desde ambientes públicos
- Verificar las medidas de seguridad del sitio web, el sitio web a ingresar debe comenzar con “https” esto indica que se esta navegando con un protocolo seguro.

- Utilizar contraseñas fuertes

Conclusiones

Los correos electrónicos que hacen fraude por medio de phishing, son más comunes de lo que se piensa juegan con el miedo de las personas e intimidan con cuestiones económicas, de esta manera las personas se precipitan y actúan de manera impulsiva, caen en las redes de los cibercriminales.

Sin duda hay una gran vulnerabilidad de los ciudadanos, debido a que las leyes están un poco implícitas con respecto a estos delitos además de que es muy difícil dar con los delincuentes ya que son muy dinámicos.

Cabe mencionar que se multiplicaran estos delitos y sus formas de actuar evolucionaran. Por eso se debe de ser muy responsable y atender las recomendaciones antes mencionadas. La responsabilidad de la seguridad informática combinado con los software (antivirus) forman un buen escudo contra cualquier amenaza.

Bibliografía

[1] Misael Mora. (13/04/2016). fraudes con correo falso del SAT. 11/04/2019, de rankia Sitio web: https://www.rankia.mx/blog/sat-servicio-administracion-tributaria/2827342-fraudes-correo-falso-sat

[2] Jorge Mireles,. (26/06/2008). robo de información online. 11/04/2019, de technical & Educational Manager de ESET para Latinoamérica Sitio web: https://www.eset-la.com/pdf/prensa/informe/robo_informacion_online.pdf

[3] wikipedia. (22/03/2019). protocolo de transferencia de hipertexto. 11/04/2019, de wikipedia Sitio web: https://es.wikipedia.org/wiki/Protocolo_seguro_de_transferencia_de_hipertexto

[4] ruy Alonso Rebolledo. (31/05/2017). Robo de identidad. 11/04/2019, de el economista Sitio web: https://www.eleconomista.com.mx/politica/14-tecnicas-para-robar-tu-identidad-20170531-0038.html

Imágenes

[1] animal político 2019. Imagen, coreo falso 11/04/2019 sitio web: https://www.animalpolitico.com/2018/05/correo-bancomer-robar-datos/

[2] tecnozero 2019. Imagen, servidor torre 11/04/2019 sitio web: https://www.tecnozero.com/servidor/torre/

[3] juan jase pino reyes 2019. Imagen devcode 11/04/2019 sitio web:

https://devcode.la/tutoriales/como-clonar-un-sitio-web