



VE&S

Engineering & Services



www.eysglobal.com

TEMA:
DELITOS INFORMATICOS
“ la necesidad de un análisis forenses “
ACTIVIDAD PRACTICA 1



DELITO INFORMÁTICO

una definición de delito informático, como todo acto dirigido contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos.

En concordancia con lo anterior, dicho Convenio establece varias conductas que se consideran como un delito informático y que tiene una consecuencia desde el punto de vista penal para quien las cometa.

CONDUCTAS

- Acceso abusivo a un sistema informático.
- Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Interceptación de datos informáticos.
- Daño Informático.
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales.
- Hurto por medios informáticos y semejantes.
- Transferencia no consentida de activos.
- Entre otros,



CIBERDELICUENCIA



CIBERDELICUENCIA

Qué es la ciberdelincuencia?

Se podría decir que la ciberdelincuencia es aquella actividad que por medio de la red (sea pública o privada) o a través de un sistema informático “tenga como objetivo atentar a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y los datos, así como el uso fraudulento de tales sistemas, redes y datos”.

Dentro de los ciberdelitos también se encuentran delitos informáticos como pueden ser la suplantación de identidad, el acoso o la estafa.



AMENAZAS MÁS COMUNES ASOCIADAS A CIBERDELINCUENCIA



Ciberdelito: Las estafas informáticas: cuya conducta consiste en realizar una actividad engañosa produciendo un desplazamiento patrimonial en perjuicio de la víctima y obteniendo así un ánimo de lucro.

La estafa informática se diferencia de la estafa normal en que los actos de engaño se dirigen a sistemas informáticos que asimismo producen el consiguiente engaño en la víctima.

AMENAZAS MÁS COMUNES ASOCIADAS A CIBERDELINCUENCIA

Este delito informático podría considerarse como uno de los más cometidos, y se puede realizar por una multitud de conductas, entre las más habituales están la estafa Nigeriana, donde su autor remite a la víctima un correo electrónico prometiéndole una gran cantidad de dinero a cambio de un ingreso de una determinada cantidad por adelantado.

Dentro de este tipo de ciberdelito se encuentran:

EL PHISING: que consiste en la obtención fraudulenta de contraseñas bancarias con el fin de transferir dinero a otra cuenta bancaria. En estos casos la jurisprudencia ha admitido que la responsabilidad sería del proveedor de servicios de pago (el banco), salvo que se aprecie fraude o negligencia grave en la víctima.



LAS 4 AMENAZAS MÁS COMUNES ASOCIADAS A CIBERDELINCUENCIA



EL CARDING: que consiste en un copiado de las tarjetas de crédito de la víctima para realizar posteriormente una adquisición de bienes con estas.

SKIMMING. Robo de información de tarjetas de crédito utilizado en el momento de la transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para su posterior uso fraudulento. Consiste en el copiado de la banda magnética de una tarjeta (crédito, débito, etc).

AMENAZAS MÁS COMUNES ASOCIADAS A CIBERDELINCUENCIA

PISHING. Método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso



DELITOS ASOCIADOS A LA TARJETA DE CREDITO



Delitos a través de los medios electrónicos

El portafolio de los punibles a través de los medios electrónicos contiene una gran variedad de modalidades, entre ellos se cuentan:

- Fraudes con tarjeta de crédito o Skimming: Esta modalidad es muy común en cajeros automáticos y establecimientos comerciales, consiste en el robo de información mediante la copia de la banda magnética de la tarjeta de crédito, el objetivo de los delincuentes es permitirse hacer avances y apropiarse del dinero que están en las cuentas bancarias del usuario afectado.

DELITOS ASOCIADOS A LA TARJETA DE CREDITO



Clonación de tarjetas:

Mediante el uso de dispositivos especializados como falsos teclados, cámaras espías, entre otros, los delincuentes logran obtener información que les va permitir hacer una copia de la tarjeta original y a partir de la información obtenida previamente (claves personales), podrán hacer compras y utilizar el dinero del cuentahabiente para lo que ellos deseen. El portal web Finanzas Personales indica que “para este tipo de robo, el dispositivo más utilizado es un ‘Skimmer’, un aditamento que se inserta en la ranura para la tarjeta en el cajero, el cual tiene una cámara para captar en video que cuando se teclea la clave, la graba instantáneamente y que además, al deslizar la tarjeta al interior, se captura la información de la banda magnética

DELITOS ASOCIADOS A LA TARJETA DE CREDITO

Smishing: Esta modalidad de delito utiliza los teléfonos móviles de los usuarios financieros, los delincuentes pretenden suplantar la identidad, a menudo de personal bancario o establecimientos comerciales, gerentes o representantes de ventas, con el fin de que las personas accedan mediante mensaje de texto o llamada a un link que le proporcionara al atacante información necesaria para hackear el teléfono de la víctima.



DELITOS ASOCIADOS A LA TARJETA DE CREDITO



Extorsión: En esta ocasión el delincuente pretende el pago en dinero efectivo o moneda virtual (bitcoins) afectando el patrimonio de su víctima, quien se encuentra bajo la amenaza de hacer públicas información sensible (fotos, videos, información personal, datos empresariales) que los ciberdelincuentes aseguran tener, el modus operandi en esta modalidad es “el uso de un software malicioso conocido como ransomware, este término proviene de las palabras del idioma inglés “ransom”, cuyo significado es rescate y “software”, programa de cómputo...normalmente cifra los archivos de la víctima para pedir un rescate por ellos.

DELITOS ASOCIADOS A LA TARJETA DE CREDITO

Estafas: El analista Ignacio Acosta Sorge, define la estafa electrónica como “la comisión, con ánimos de lucro, de un acto que produzca daños y perjuicios patrimoniales cuantificables a terceros, cometido mediante el uso ilícito de tecnologías y procedimientos de la informática, es decir, cualquier transferencia no consentida de un activo patrimonial que produzca daños a terceras personas, mediante la manipulación indebida de la informática”



DELITOS ASOCIADOS A LA TARJETA DE CREDITO

Suplantación de identidad o Phishing: Esta forma de delito el objetivo del delincuente es conseguir contraseñas, claves de tarjetas de crédito, información financiera, entre otros, utilizando páginas webs falsas a las cuales dirigen a la víctima.

Carta Nigeriana: Esta modalidad ofrece a la victima ser la dueña de una cantidad considerable de dinero, el contacto se hace a través de correos electrónicos donde le indican a la victima que debe consignar por adelantado un pago, a fin de entregarle el “la herencia o fortuna”.



ACTIVIDAD PRACTICA



realice un cuadro comparativo teniendo en cuenta los delitos mencionados en este análisis, de la siguiente manera , delito, tipo de delito y pena o multa, con un mínimo de 10 ejemplos

EJEMPLO :

DELITO	TIPO DE DELITO	PENA O MULTA
Engañar a una persona por cualquier medio electrónico para que le entregue los datos de la tarjeta de crédito y después robarla.	Fraude en tarjeta de crédito.	La cárcel.