Delitos, Fraudes & Tics

Laura Laexandra Ureta Arreaga

Especialista Informática Acreditada (Perito Informática del Concejo de la Judicatura) y Magister en Sistemas de Información Gerencial – Universidad Politécnica del Litoral (ESPOL), Ecuador.

Consultor Independiente en Detección de Fraudes Informáticos y Evaluación de Riesgos de Activos de Información. Docente: Universidad Metropolitana de Quito (Unidad Académica Boyacá) y Docente Invitada Universidad Técnica Estatal de Quevedo, ECOTEC, UEES

RESUMEN

Este artículo introduce al lector al mundo de los delitos y fraudes informáticos, y su alarmante incremento en el país. Se muestra estadísticas de los entes públicos que controlan y dan el oportuno seguimiento a las denuncias entorno a estos tipos de delitos. Además, se actualiza en temas relacionados a la tipificación de este tipo de actividades dolosas y de sus penas para quienes los cometen.

PALABRAS CLAVE

TICs, hackers, cyberdelito, computación forense.

ABSTRACT

This article introduces the reader to the world of computer crime and fraud, and the alarming increase in the country. It displays statistics of public bodies that monitor and provide timely follow-up to allegations surrounding these types of crimes. In addition, updates on issues related to the characterization of such malicious activities and their penalties for the perpetrators.

KEYWORKS

ICT, hackers, cybercrime, computer forensics,

1. INTRODUCCIÓN

El avance tecnológico y vertiginoso, de la informática o de las ciencias computacionales, permite que los procesos de las organizaciones mejoren y sean eficientes en gran medida, la habilitación de iniciativas que permiten disminuir la brecha en el acceso a las información a través de internet, brindan la posibilidad de que se incorporen más usuarios a consumir los servicios disponibles en la Web, sin embargo, este mismo desarrollo tecnológico viene acompañado de nuevas amenazas y riesgos inherentes, que conllevan a la necesidad de que estas tecnologías, cuenten con una base fundamental en materia de seguridad.

Cada vez más recobra, especial importancia el mantener esquemas básicos de seguridad informática y de la información, mediante la habilitación de recursos de difusión y concientización, de dar uso a las herramientas tecnológicas por parte de los internautas de una manera responsable.

Ecuador no ha quedado rezagado en términos del desarrollo tecnológico y las organizaciones han hecho uso del mismo, aún cuando el acceso a internet como uno de los rubros de mayor crecimiento tecnológico, mantiene niveles de penetración muy bajo con relación a países vecinos, no obstante, esta condición, no exime de que el mal uso de las tecnologías impacten en gran medida a distintos sectores como financiero, comercial, educativo, entre otros.

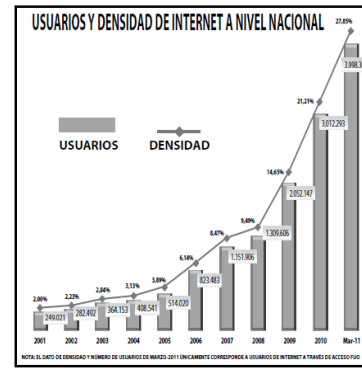

Figura 1: *Densidad de Internet en el Ecuador.*

Fuente: www.conatel.gob.ec

Las facilidades de acceso a la información, así como también el fácil acceso, a través del cual se encuentran disponibles muchas herramientas inclusive gratuitas y de fácil adquisición a través de internet, permiten vulnerar, infraestructuras y sistemas informáticos, sin discriminación a los tipos de empresas u organizaciones, puede ejecutarse acciones ilegales por parte de los conocidos cyberdelincuentes.

2. CYBERDELINCUENCIA

El Convenio de Ciberdelincuencia del Consejo de Europa[1], define los delitos informáticos como: "los actos dirigidos 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".

Desde esta definición se observa la importancia de los tres pilares fundamentales de la seguridad de la información.

En este convenio desde el año 2001, se observa que se incorporan figuras como: Acceso ilícito, intercepción ilícita, interferencia en los datos, interferencia en el sistema, abuso de los dispositivos, falsificación informática, fraude informáticos, delitos relacionados con la pornografía infantil, delitos relacionados con las infracciones de propiedad intelectual y de los derechos afines, en relación con algunas de las figuras delictivas que atentan a los sistemas.

Los Cyberdelincuentes o también conocidos como delincuentes informáticos dan un mal uso a las TICS, a través de la utilización de herramientas tecnológicas o métodos técnicos, que permiten vulnerar los sistemas de todo tipo de organizaciones, cuyas afectaciones van desde el uso indebido de los sistemas hasta la inhabilitación o destrucción de los mismos, con el objetivo de conseguir el reconocimiento o incluso una recompensa económica.

3. FIGURAS DELICTIVAS MEDIANTE LA UTILIzACIÓN DE LAS TICS

Nuevos conceptos como Phising, Skimming, SMishing, pornografía infantil a través de internet, usurpación de identidad en las redes sociales, y muchos otros van incorporándose e identificándose como los nuevos actos delictivos en las que se mal utilizan las tecnologías de la información y afectan de diversas maneras al internauta ecuatoriano.

El Phising y el Skimming, son modalidades delictivas que afectan principalmente al sector financiero, y que además ha tenido un nivel alto de perjuicio económico, impactando la economía de la sociedad ecuatoriana, estas modalidades dejan entrever que incluso entidades de estos sectores que cuentan con mayor desarrollo en sus infraestructura tecnológica son vulnerables ante los ataques delictivos de este tipo.

Phising[2] Skimming[3]

Figura 2: *Modalidades delictivas de fraudes electrónicos. Fuente: Ver nota al pie.*

La pornografía infantil en internet, que utiliza los medios electrónicos desde su proceso de producción y culmina la cadena hasta su proceso de distribución relacionado con este tipo de material, en donde el agresor puede hacer uso de las tecnología para fácilmente revestirse del anonimato y por ende hacer más difícil su localización e identificación.

Figura 3: *Pornografía infantil.*

La usurpación de identidad en las redes sociales, utilizan la información de la que disponen y cargan los mismos usuarios de dichas redes sociales, y de esta forma permiten el fácil acceso a información personal que les corresponde, cuando no se habilitan restricciones de acceso básicos de la información.

Estos son algunos de los tipos de ataque a los que los usuarios de internet se encuentran expuestos, pero existen muchos más que generan repudio por el impacto que puede causar a grupos vulnerables como: niños y adolescentes, llegando incluso a tener consecuencias tan nefasta como el suicidio, este tipo de ataque es conocido como cyberbulling o ciber-acoso, fenómeno que se ha venido incrementado de forma alarmante según los datos obtenidos en la encuesta realizada por BitDefenser( ) en varios países, es necesario entonces comprobar que están subiendo a la red los niños, darles a conocer la importancia de la privacidad, así como también instruirles que no es favorable compartir información personal en internet, incluso con los amigos.

Todas estas modalidades o nuevas formas de delinquir, precisan del apoyo y conocimiento de

profesionales especializados que puedan rastrear e identificar aquellos elementos que con sus conocimientos en tecnología cometan acciones antijurídicas y a quienes se les denomina los hackers

4. HACKER

La contraparte de los crackers, es reconocida como hackers éticos, los mismos que propone y diseñan estrategias de seguridad, en la implantación proactiva de herramientas que cierran las vulnerabilidades que permiten el acceso a los delincuentes informáticos. Estos especialistas también brindan apoyo con sus conocimientos para identificar los procesos utilizados por aquellos personajes que se aprovechan de las vulnerabilidades de los sistemas para cometer actos de índole delictiva.

Cabe recalcar que el conocimiento, en las técnicas e incluso las herramientas que utilice el especialista, ante la investigación de fraudes o infracciones de naturaleza informática, son de vital importancia ante un proceso legal, en el que se debe mantener especial cuidado en la manipulación o manejo de las evidencias digitales, así como la estricta conservación del mantenimiento de la respectiva cadena de custodia.

Por ello, se ha venido desarrollando una nueva ciencia que permite a los especialistas enfrentar los desafíos que conlleva el análisis de la evidencia digital, esta ciencia es reconocida como la Informática Forense

Posterior al análisis técnico que ejecuta el especialista informático, luego de la revisión de las evidencias digitales, debe considerar mantener un lenguaje claro, comprensible y fluido sin tecnicismo, mediante el cual pueda transmitir el mensaje de su revisión a la autoridad competente. También se precisa reconocer que así como existe la Informática Forense también se encuentra disponible el kit de herramientas para la aplicación de técnicas Anti-Forense que complican la tarea encomendada al técnico Forense

5. LEGISLACIÓN ECUATORIANA

Ecuador mantiene en su legislación desde el año 2002 la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en donde se definen y reglamenta los mensajes de datos, firmas electrónicas y los servicios de certificación de información, contempla también las penalizaciones atribuibles a las infracciones informáticas, imponiendo sanciones para quienes vulneran los sistemas informáticos.

La Ley de Propiedad Intelectual también contempla especificaciones que salvaguardan los derechos de autor y derechos conexos de los programas de ordenador, a través de una adecuada protección a los derechos intelectuales de su creador. En varios países de Latinoamérica como Chile desde 1993, Argentina desde el 2008 y Colombia desde 2009, ya se configuran y se mantienen Leyes que regulan y sancionan los delitos informáticos y en donde se considera como un "bien jurídico protegido" a la información, salvaguardando los pilares fundamentales de la seguridad de la información como son la confidencialidad, integridad, y disponibilidad de los recursos tecnológicos.

6. IMPLICACIONES INTERNACIONALES

Los delitos informáticos a diferencia de los delitos comunes (robo, asesinato) mantienen una muy particular consideración, puesto que mientras el ofendido o víctima radica en un lugar específico de un país particular, su atacante puede llegar a traspasar fácilmente las líneas fronterizas, y es ahí donde hay la necesidad de colaboración por parte de los estados o naciones aunar esfuerzo que permitan radicar esta nueva forma de delinquir utilizando los medios tecnológicos.

Así también, se identifican iniciativas en los centros universitarios que mediante la implantación de programas especiales a nivel de las carreras de pregrado y postgrado, introducen en el estudiante conceptos básicos fundamentales y que le permita reconocer los riesgos y vulnerabilidades que tienen las TICs, en programas relacionados con el estudio de la seguridad informática o seguridad de la información

Ciudadanos ecuatorianos en los últimos años han sido víctima de este tipo de infracciones informáticas, su crecimiento exponencial ha estimulado que diferentes sectores incorporen iniciativas que permitan alertar a la ciudadanía, de cómo protegerse ante la sospecha de que se pueda materializar un delito de este tipo y engrose las estadísticas relacionadas a estas infracciones.

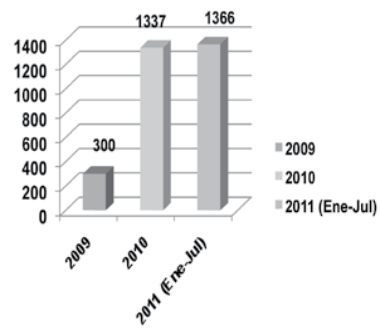

Figura 4: *Estadísticas Delitos Informáticos Ecuador.*
Fuente: *Datos de la Fiscalía del Estado www.fiscalìa.gob.ec*

7. CONCLUSIONES

El crecimiento de internautas y/o usuarios de internet que consumen cada vez más estos servicios, ponen en relieve la necesidad de seguir incorporando iniciativas que permitan difundir y socializar el alcance de los delitos informáticos y el impacto que tienen estos en la sociedad.

Impartir programas que involucren el estudio en materia de delitos informáticos o informática jurídica a nivel de formación de pregrado en los centros universitarios en las carreras de Derecho e Ingenierías de Sistemas, permitirá acortar la brecha en las comunicaciones o lenguaje utilizado entre los profesionales del derecho y los técnicos informáticos.

Establecer y utilizar estándares básicos de seguridad informática o de la información, al hacer uso de los servicios de tecnología de una manera responsable, aportará a que los incidentes relacionadoscon los delitos informáticos disminuyan y sobretodo implantado estos esquemas permitirá proteger a usuarios más vulnerables, que pueden ser afectados como los niños y los adolescentes.

8. GLOSARIO DE TÉRMINOS

TIC's: Tecnologías de la Información y Comunicaciones
Phising: Es una forma de engaño mediante la cual los atacantes envían un mensaje (anzuelo) a una o varias personas, intentando convencerlas para que revelen sus datos personales.

Usualmente, esta información es luego utilizada para realizar acciones fraudulentas, como transferencias de fondos de su cuenta bancaria, compras con sus tarjetas de crédito u otras acciones delictivas que pueden efectuarse mediante la utilización de esos datos.

Skimming: Es el robo de información de tarjetas de crédito, 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).

SMishing: Es un término informático para denominar un nuevo tipo de delito o actividad criminal usando técnicas de ingeniería social empleado mensajes de texto dirigidos a los usuarios de Telefonía móvil. El SMiShing es una variante del phishing.

Cyber-bulling: Es el uso de información electrónica y medios de comunicación tales como correo electrónico, redes sociales, blogs, mensajería instantánea, mensajes de texto, y websites difamatorios para amenazar, intimidar, perseguir o acosar a un individuo o grupo, mediante ataques personales u otros medios.

Hacker: Se refiere a la acción de explotar y buscar las limitantes de un código o máquina, interrumpe e ingresa de manera forzosa a un sistema de cómputo o a una red.

Informática Forense: Ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un medio computacional

Técnica Anti-Forense: Técnicas de manipulación, eliminación y/o ocultamiento de pruebas para complicar o imposibilitar la efectividad del análisis forense

REFERENCIAS

- COE. (21 de Mayo de 2011). www.coe.int. Recuperado el 10 de Octubre de 2011, de www.coe.int: http://www.coe.int/t/dghl/cooperation/economiccrime/ cybercrime/default_EN.asp?
- CONATEL. (01 de Abril de 2010). www.conatel.gob.ec. Recuperado el 10 de Octubre de 2011, de www.conatel.gob.ec: www.conatel.gob.ec

---

[1]El Concejo de Europa - http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_EN.asp?

[2] http://www.muypymes.com/2009/09/03/hacienda-como-gancho-para-hacer-phishing

[3]Inagen tomada del sitio web: http://www.badgeholder.com/tag/card-skimming-tactics/