KEYLOGGER

Es un dispositivo (hardware) o un programa informático (software) que almacena todas y cada una de las pulsaciones que se hagan en el teclado de una computadora.

Los de hardware pueden ser:

- ***Adaptadores:*** Se conectan entre el teclado y la computadora de la víctima.
- ***Dispositivos:*** Se conectan dentro del teclado de la víctima.
- ***Teclados reales:*** Son instalados en la computadora de la víctima.

Los keylogger de software son:

- Un programa muy pequeño que se instala en la computadora del objetivo.

  - Se ejecuta sin que el usuario se de cuenta.
  - No presenta signos visibles.

- Guarda cada tecla presionada en el teclado.
- Toma una impresión de pantalla cada determinado tiempo.
- La información puede ser enviada a través de una red local o a través de Internet a otra computadora o cuenta de correo electrónico, sin que el usuario lo note.

- Estos programas pueden ser encubiertos en archivos de texto, imágenes, presentaciones, archivos de música o video, entre otros.

RECOMEDACIONES

1. Actualizar constantemente el sistema operativo de su computadora.
2. Tener un antivirus actualizado.
3. Instalar un programa muro de fuego o firewall personal.
4. Limitar el acceso de personas ajenas a usted, a la computadora de su empresa o casa de habitación.
5. Haga caso omiso de cualquier correo electrónico o página de Internet (que no sea de su entera confianza), que le indique que debe descargar una herramienta de seguridad, juego, documento u otro archivo.
6. No abra mensajes de correo electrónico donde no conozca al remitente.
7. No reciba archivos por mensajería instantánea que no conozca quién se lo está enviando.
8. Nunca utilice computadoras de acceso público como Café Internet para ingresar al servicio de Internet de su banco.
9. Cuando ingrese su clave de acceso, asegúrese que nadie lo está viendo.
10. No comparta sus contraseñas. A nadie!.
11. Utilice claves con mas de 12 dígitos, combinando letras y números, mayúsculas y minúsculas.
12. No escriba sus pines o claves en ningún lugar, ni lo porte en su billetera. Memorícelo!

SECCIÓN DELITOS INFORMÁTICOS

Teléfonos:
2295-3127 - 2295-3069
Línea gratuita: 800-8000-OIJ (645)

Correo electrónico:
invest_informaticas@poder-judicial.go.cr

Departamento de Artes Gráficas - B. 34510

ORGANISMO
DE INVESTIGACIÓN JUDICIAL
DEPARTAMENTO
DE INVESTIGACIONES CRIMINALES

SECCIÓN DELITOS INFORMÁTICOS

RESEÑA HISTÓRICA

En 1996 se presentan una serie de casos donde existía medios informáticos donde se almacenaba información importante para la investigación, tal es el caso del Banco Anglo Costarricense y otros. Para la extracción de la información se coordina con los Profesionales de la Sección de Soporte Técnico del Departamento de Informática del Poder Judicial.

Sin embargo, en aras de estandarizar y profesionalizar los procedimientos, se crea en 1997 la Unidad de Investigación Informática, la cual es la encargada de investigar los delitos informáticos y otros actos delictivos en dónde la informática fue utilizada para la comisión de estos o pueda ser útil para esclarecer la verdad de los hechos. Debido a su importancia y crecimiento, a partir del año 2002 pasa a ser la Sección de Delitos Informáticos.

OBJETIVO GENERAL

Realizar las investigaciones de los delitos en los cuales los medios informáticos son los principales o únicos indicios existentes; así como apoyo en el ámbito informático en investigaciones relacionadas con otros delitos.

OBJETIVOS ESPECÍFICOS

Realizar investigaciones en el ámbito informático para determinar el modus operandi y los presuntos responsables de los ilícitos.

Identificar, preservar y analizar la información contenida en diferentes medios de almacenamiento informático.

Apoyar a las instancias correspondientes en el desarrollo de actividades referentes a los allanamientos, apertura y respaldo de evidencias, entre otras.

DELITOS INFORMÁTICOS

Los delitos informáticos son actividades ilícitas que se cometen utilizando medios tecnológicos, tales como computadoras, sistemas de información, sistemas de comunicaciones, páginas de Internet, entre otros. Donde estos medios informáticos son el fin del perpetrador o en otros casos es el medio por el cual se comete el delito.

¿QUÉ ES PHISHING?

Es una estafa o fraude que utilizando medios informáticos o electrónicos e ingeniería social, tiene como fin extraer información confidencial de sus victimas y utilizarla para extraer dinero u otros fines. Para esto se hace pasar por una persona o empresa que requiere su información confidencial, tal como:

- Número de Tarjetas de debito o crédito
- Contraseñas o claves de paso
- Información de cuentas
- Información personal

La víctima puede ser abordada mediante:

- SMS (mensaje de texto)
- Llamada telefónica
- Página de Internet o ventana emergente http://www.nombredelbanco paginasgratis.com
- Correo electrónico

CARACTERÍSTICAS

- Los correos electrónicos parecen ser enviados por una cuenta de correo electrónico real del banco, empresa o inclusive persona real. agenciavirtual@banco.fi.cr
- Factor miedo, con el fin de conseguir una respuesta inmediata de la víctima. Amenaza a la víctima con perder dinero o cerrar la cuenta sino sigue las instrucciones del correo electrónico.
- El correo electrónico incluye un acceso directo o vínculo o link, supuestamente a la página de Internet del banco. http://www.nombredelbanco.paginasgratis.com/.
- Creación de una página de Internet casi igual a la de la entidad bancaria o empresa.
- En ella se pide la información confidencial de la víctima.

RECOMENDACIONES

1. Ningún banco o empresa le solicitará información confidencial por correo electrónico, mensaje de texto a su celular o por vía telefónica.
2. No conteste ningún correo electrónico donde su banco le pida información.
3. Haga caso omiso a cualquier correo electrónico o página de Internet que le indique que ingrese a una página de Internet de su banco para actualizar sus datos u otro motivo o que le indique que debe descargar una Herramienta de Seguridad para hacer transferencias seguras.
4. Visualice errores gramaticales en los correos electrónicos.
5. Siempre digite la dirección electrónica correspondiente a su banco, nunca lo haga mediante alguna sugerencia en un correo electrónico o página de Internet, si tiene duda, llame al banco.
6. La dirección electrónica de su banco siempre debe iniciar con “https” y busque en el programa navegador un candado, que le indicará que es una conexión segura.