SISTEMAS DE ALERTAS

La CFN a través del Programa de Educación Financiera busca orientar hacia un correcto manejo de información que minimice el riesgo y errores en la toma de decisiones financieras, a través del mejoramiento de sus conocimientos financieros básicos.

A medida que los delincuentes cibernéticos dirigen su atención a las redes sociales, una variedad de ataques pueden esperarse.
El delito informático es el término genérico para aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Por tanto es importante mantenerse protegido de las principales amenazas informáticas que generalmente se realizan por medio de:

Malware es un término general que se utiliza para referirse a distintas formas de software hostil, intrusivo o molesto.
El software malintencionado o malware es un software creado por hackers para perturbar las operaciones de una computadora, obtener información confidencial o acceder a sistemas informáticos privados.

El malware incluye virus informáticos, gusanos, troyanos, spyware, adware, la mayoría de rootkits y otros programas malintencionados.

Las siguientes son algunas formas de software malintencionado:

SPYWARE: es un tipo de malware (software malintencionado) que se instala en las computadoras para obtener información sobre los usuarios sin que éstos lo sepan. El spyware suele estar oculto al usuario y puede ser difícil de detectar. Algunos spywares, como los keyloggers —registradores de teclas—, pueden ser instalados de forma intencionada por el propietario de una computadora de uso común, corporativo o público para controlar a los usuarios.

SPAM: consiste en el uso de sistemas de mensajes electrónicos para enviar de forma indiscriminada un gran número de mensajes no solicitados. Aunque la forma más conocida de spam es el de correo electrónico, el término se aplica también a abusos similares en otros medios: spam de mensajes instantáneos, spam de grupos de noticias de Usenet, spam de motores de búsqueda en la web, spam en blogs, spam en wikis, spam en anuncios clasificados de Internet, spam de mensajes de teléfonos móviles, spam en foros de Internet, transmisiones fraudulentas por fax, spam en redes sociales, publicidad en televisión y spam en redes de uso compartido de archivos.

PHISHING: consiste en el intento de adquirir información (y, en ocasiones, también de dinero, aunque sea de forma indirecta), como nombres de usuarios, contraseñas y datos de tarjetas de crédito haciéndose pasar por una entidad de confianza en una comunicación electrónica. Los correos electrónicos de phishing pueden contener enlaces a páginas web infectadas con

malware.

La forma más habitual de phishing utiliza mensajes instantáneos o correos electrónicos fraudulentos en los que se pide a los usuarios que introduzcan sus datos en una página web falsa que es casi idéntica a la página auténtica. El phishing es un ejemplo de las técnicas de ingeniería social empleadas para engañar a los usuarios, el cual aprovecha las limitaciones de uso de las actuales tecnologías de seguridad en la web. Entre los intentos de lucha contra el creciente número de incidentes de phishing figuran medidas legislativas, de formación de usuarios, de divulgación y de seguridad técnica.

PHARMING: es una forma de ataque cuyo objetivo es redireccionar el tráfico de un sitio web hacia una página fraudulenta.

El término “pharming” es un neologismo formado por la unión de las palabras inglesas “phishing” y “farming”. El phishing es una técnica de ingeniería social que pretende obtener datos de acceso, como nombres de usuarios y contraseñas. Tanto el pharming como el phishing se han utilizado en los últimos años con el fin de adquirir información que permita el robo de identidades online. El pharming es ya un problema grave para las empresas de comercio electrónico y banca electrónica.

Para prevenir esta seria amenaza se requieren sofisticadas medidas conocidas como anti-pharming, ya que los programas antivirus y el software de eliminación de spyware no ofrecen suficiente protección contra el pharming.