PELIGROS CONCRETOS DEL INTERNET

EDUFUTURO

Índice

Peligros concretos del Internet

En la actualidad debido a que la mayor parte de las personas utilizan Internet, los peligros se han incrementado considerablemente, por lo que todas las personas deben adoptar medidas preventivas y aconsejar a los menores. Internet ofrece grandes ventajas y herramientas, para disfrutar de estos beneficios, deberás evitar los aspectos negativos.

1. Malware

Es el acrónimo en inglés de software malicioso (malicious software).

El objetivo de este tipo de aplicaciones es dañar la computadora. En la mayoría de los casos, la infección ocurre por "errores" realizados por los usuarios, al ser engañados por el atacante.

Existen muchas herramientas (antivirus, antispyware) y buenas prácticas, que reducen el riesgo de infección, ante todas las variantes de códigos maliciosos: virus, gusanos, troyanos, spyware, etc.

La diferencia entre estas variantes radica en la forma en que se distribuyen: algunas veces se aprovechan de sistemas vulnerables y otras de usuarios no precavidos.

2. Spam

El spam es el famoso "correo basura". Son aquellos mensajes que no fueron solicitados por el usuario y que llegan a la bandeja de entrada. Normalmente, este tipo de correos contienen propagandas – muchas veces engañosas – que incitan al usuario a ingresar a páginas, con ofertas "milagrosas", cuyo contenido es potencialmente dañino para el usuario.

3.-Scam

Los scam son engaños o estafas, que se llevan a cabo a través de Internet.

Se realizan de diversas formas como, por ejemplo, a través de correos no solicitados (spam), así como también a través de técnicas de Ingeniería Social.

Estas últimas, intentan convencer al usuario de la prestación de un servicio cuando en realidad sólo quieren acceder a información confidencial. Un ejemplo son los mensajes falsos solicitando nuestra contraseña y clave de redes sociales a través de Internet.

4.-Ciberacoso

Es una conducta hostil que puede ser practicada hacia los niños. La víctima de este tipo de acosos, es sometida a amenazas y humillaciones de parte de sus pares en la web, cuyas intenciones son atormentar a la persona y llevarla a un quiebre emocional. Estas prácticas pueden ser realizadas a través de Internet, así como también, teléfonos celulares y videoconsolas.

También denominado en inglés, cyberbullying, no siempre son realizadas por adultos, sino también son frecuentes entre adolescentes.

5.-Grooming

Se trata de la persuasión de un adulto hacia un niño, con la finalidad de obtener una conexión emocional y generar un ambiente de confianza para que el niño realice actividades sexuales. Muchas veces los adultos se hacen pasar por niños de su edad e intentan entablar una relación para, luego, buscar realizar encuentros personales.

6.-Sexting

Proviene del acrónimo formado entre Sex y Texting. Inicialmente, y como lo indica su nombre**,** se trataba del envío de mensajes con contenidos eróticos. Posteriormente, dado el avance tecnológico, esta modalidad evolucionó hacia el intercambio de imágenes y videos.

7.-Robo de información

Toda la información que viaja por la web, sin las medidas de precaución necesarias, corre el riesgo de ser interceptada por un tercero.

De igual modo, existen también ataques con esta finalidad. La información buscada, normalmente apunta a los datos personales. Un paso en falso ante este tipo de incidentes, puede exponer al menor de edad a la pérdida de dinero familiar o al robo de identidad.

Algunos delitos convencionales potenciados por internet

Denominamos delitos convencionales a aquellos que se dan dado y se dan sin la utilización de internet, pero que han encontrado en este medio una potenciación en el sentido de su multiplicación y dificultad de persecución.

1. Espionaje:

Se han dado casos de acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera.

2. Espionaje industrial:

También se han dado casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y know how estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada.

3. Terrorismo:

La existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.

4. Narcotráfico:

Tanto el FBI como el Fiscal General de los EEUU han alertado sobre la necesidad de medidas que permitan interceptar y descifrar los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles.

También se ha detectado el uso de la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

5. Otros delitos

Las mismas ventajas que encuentran en Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

6. Usos comerciales no éticos:

Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos llevando a cabo "mailings electrónicos" al colectivo de usuarios de un gateway, un nodo o un territorio determinado. Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet, poco acostumbrados, hasta fechas recientes, a un uso comercial de la red.

7. Actos parasitarios:

Algunos usuarios incapaces de integrarse en grupos de discusión o foros de debate on- line, se dedican a obstaculizar las comunicaciones ajenas, interrumpiendo conversaciones de forma repetida, enviando mensajes con insultos personales, etc. Aunque la mayoría de estas conductas están previstas por los suministradores de servicios on-line, resolviendo el contrato con los reincidentes, existen algunos partidarios de que se establezcan normas para sancionar estos actos.

Glosario

- **Delitos**
  Es definido como una conducta típica, antijurídica y culpable, sometida a una sanción penal y a veces a condiciones objetivas de punibilidad. Supone una conducta infraccional del Derecho penal.

- **Gateway**

  Puerta de enlace, es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación.

- **Mensajes encriptados**
  Es el proceso para volver ilegible información considera importante. La información una vez encriptado sólo puede leerse aplicándole una clave.

- **Scam**
  Es una palabra inglesa que se usa comúnmente para designar algún tipo de estafa y cada vez más, dicho término ha quedado relegado a los engaños en la red.

- **Variantes**
  Cada una de las diversas formas con que se presenta algo, variedad o diferencia entre diversas clases o formas de una misma cosa.

Referencias:

- http://www.protecciononline.com/¿cuales-son-los-principales-peligros-en-internet.
- Ética en Internet – La Santa Sedewww.vatican.va/…/rc_pc_pccs_doc_20020228_ethics-internet_sp.html22 feb. 2002 – PONTIFICIO CONSEJO PARA LAS COMUNICACIONES SOCIALES
- https://pixabay.com/es/

Palabras: 1,172
Por Mildred Montúfar
Edufuturo