

Protección anti virus y fraudes

Virus



Programa capaz de colarse en un ordenador, smartphone o tableta para llevar a cabo acciones maliciosas: robar datos privados, hacer que el dispositivo deje de funcionar correctamente, tomar su control, etc.



Tipos de virus

Troyano: Software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.^{1 2} El término troyano proviene de la historia del caballo de Troya mencionado en la *Odisea* de Homero.



Keylogger: Es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.



Spyware: Es un malware que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.



Rogueware: Es un tipo de programa informático malicioso cuya principal finalidad es la de hacer creer que una computadora está infectada por algún tipo de virus, induciendo a pagar una determinada suma de dinero para eliminarlo



Ransomware: Es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.



Gusano informático: Es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.



Fraudes

Definición: Actividad delictiva que se lleva a cabo a través de medios como Internet, ordenadores y dispositivos móviles.



Medidas de seguridad para evitar virus

- **Evitar descargar archivos de lugares no conocidos.**
- **No aceptar software no original o pre-instalado sin el soporte original.**
- **Actualizar los patrones de los programas de antivirus cada uno o dos meses, algunos paquetes lo hacen automáticamente.**



- Tener especial cuidado con los archivos que pueden estar incluidos en nuestro correo electrónico, no abrir archivos de usuarios desconocidos.



- Las computadoras conectadas a una Red, preferentemente, no deberan tener unidades de diskettes, a fin de prevenir la infecci3n de virus inform3ticos. El uso de los diskettes debera ser efectuado por el administrador de red



- Otra opción muy recomendable para aumentar la seguridad. Puede bajarse alguno gratuito o configurar el del sistema operativo (especialmente si se cuenta con Windows XP)
- En las salas de chat es muy común enviar archivos de todo tipo a través del sistema DDC. Si se recibe uno que no se solicitó o de origen desconocido jamás aceptarlo por más interesante que parezca.



· Prestar mucha atención si los archivos aumentan de tamaño inesperadamente o aparecen avisos extraños de Windows. También evitar descargar programas desde sitios de Internet que despierten sospechas o desconocidos.



- No abrir archivos cuya extensión sea VBS (Visual Basic Script es un lenguaje que permite ejecutar rutinas dentro de la PC) a menos que se esté absolutamente seguro que el mail viene de una persona confiable y que haya indicado previamente sobre el envío.



Casos famosos de fraude.

- **A mediados de 1994 Kevin Poulsen fue condenado a 51 meses al ser encontrado culpable de lavado de dinero y obstrucción de la justicia valiéndose de medios tecnológicos.**
- **En 1995 Chris Pile fue condenado en el Reino Unido a 18 meses de cárcel al ser encontrado culpable de crear y distribuir códigos maliciosos. Dentro de los códigos maliciosos se encuentran los virus Pathogen y Queeg que se cargaban en memoria para afectar los programas que estuvieran en ejecución.**



- **Su caso fue retomado en el cine por el mismísimo Steven Spielberg en la película “Atrápame si puedes”. Frank Abagnale suplantó ocho veces su identidad y cambió cheques falsos por 2.5 millones de dólares. Hoy en día (irónicamente) dirige una compañía financiera de consultas por fraudes.**
- **Carlo Ponzi fue un timador que inventó el método de la “estafa piramidal”, la que consiste en buscar inversores que convencen a más inversores. Él creó la empresa Securities Exchange Company, con la que prometía intereses del 50% en 90 días: una oferta a la que pequeños y grandes inversionistas no pudieron resistir.**



- Quizá una de las condenas más famosas es la que en 1999 se le impusiera a Kevin Mitnick. Debió permanecer 68 meses meses en la cárcel después de ser encontrado culpable de interceptar comunicaciones y estar relacionado con otros delitos de fraude.

