3.1 Definición y conceptos

DEFINICIÓN Y CONCEPTOS

El término “virus” se utiliza comúnmente para referirse a las aplicaciones informáticas que buscan alterar el funcionamiento de los dispositivos (PC, tabletas, smartphones, etc.) y en muchos casos, robar información del usuario. Existen numerosos tipos de programas maliciosos que se han vuelto más sofisticados y más peligrosos, y más difíciles de detectar.

Al principio los virus solían centrar su actividad en causar molestias al usuario, borrando información, impidiendo el uso de determinados programas o ralentizar el arranque del ordenador.

Por desgracia, **la mayoría de los virus actuales tienen como objetivo el obtener información de los usuarios infectados**, tales como datos bancarios fotos, contraseñas o uso de la webcam.

Hoy en día existen muchos **programas maliciosos** que permiten tomar el control absoluto del ordenador y realizar cualquier tipo de acción sin nuestro conocimiento, como por ejemplo:

- Suplantar nuestra identidad y enviar correos electrónicos en nuestro nombre.
- Utilizar nuestro ordenador para realizar ataques a otros ordenadores.
- Realizar estafas en las que figurará nuestro ordenador (y nuestra IP) como origen del delito.
- Enviar publicidad.
- Secuestrar y cifrar nuestros archivos, y exigir un pago para recuperarlos.

Los ciberdelincuentes utilizan diversas **técnicas para infectar los sistemas con virus**, como por ejemplo:

- La infección puede llevarse a cabo al instalar un archivo o un programa supuestamente legítimo pero que contiene código malicioso porque haya sido pirateado.
- La infección puede producirse simplemente conectándote a una web infectada, aprovechando una vulnerabilidad (fallo de seguridad) en el sistema operativo, en el navegador, en plugins y aplicaciones que los usuarios utilizan habitualmente
- Otra forma de infección se produce cuando se pulsa sobre un enlace malicioso recibido a través de alguna aplicación de mensajería (por ejemplo, WhatsApp, Twitter, o Facebook).

Copyright 2026

En el momento de pulsar el enlace se redirige al usuario a una web en la que se produce la infección. El gancho para pulsar sobre el enlace suele consistir en una invitación para ver una noticia llamativa.
- Los dispositivos externos como pen drives también pueden incluir virus que infecten los ordenadores.
- Algunas estrategias de engaño pueden infectar tu equipo, por ejemplo cuando recibes un mensaje indicándote que proporciones tus datos de clave de usuario y contraseña para activar tu cuenta, alegando un falso mantenimiento del servicio.

En la actualidad **existen virus para todas las plataformas y dispositivos**, por lo que cualquier ordenador conectado a Internet es susceptible de ser infectado por un virus, independientemente de la plataforma (Windows, Apple, Linux) o el dispositivo (ordenador, tabletas, teléfono móvil).

A estos riesgos, hay que añadir que los menores poseen ciertas características tales como inocencia, curiosidad, inexperiencia o impaciencia, que los pueden hacer especialmente débiles al potenciar los riesgos de infección y fraude.

Tipos de fraude online

Los fraudes electrónicos pueden ser muy variados. En algunos casos, se estudian los hábitos de la víctima (especialmente a través de la redes sociales), y se busca ganar su confianza para eliminar protecciones (por ejemplo, se suele aconsejar desactivar el antivirus para que el ordenador vaya más rápido).

En otros casos, se recurre a incluir condiciones en unos términos ambiguos antes de instalar un juego o programa, confiando en que el usuario aceptará las condiciones de instalación sin leerlas, especialmente, si se trata de un menor.

Algunos **tipos de fraude online** que te puedes encontrar en tu actividad diaria en la red son:

- **Rogue software o fakeav**: Se le denomina Rogue Software (o también Rogue Rogueware, FakeAVs, Badware, Scareware) a los “Falsos programas de seguridad” que no son realmente lo que dicen ser, sino que todo lo contrario. Bajo la promesa de solucionar falsas infecciones, cuando el usuario instala estos programas, su sistema es infectado. Estos falsos Antivirus y Antispyware están diseñados para mostrar un resultado predeterminado (siempre de infección) y no hacen ningún tipo de escaneo real en el sistema al igual que no eliminaran ninguna infección que podamos tener. La estafa consiste en invitarnos a descargar la versión completa del programa de protección solicitando para ello el pago, por medios “poco seguros”, de cierta cantidad de dinero
- **Phishing**: Es una actividad delictiva encaminada al robo de contraseñas personales y credenciales bancarias, es decir a la “pesca de contraseñas” que ya explicamos en el tema anterior.

Copyright 2026

- **Suscripción a servicios Premium o de pago**: Existen aplicaciones fraudulentas para dispositivos móviles que envían mensajes SMS Premium desde nuestro teléfono sin que seamos conscientes de ello hasta que recibimos la factura. A veces la información suele hallarse camuflada en el listado de condiciones que debemos aceptar antes de instalar una aplicación. Cuando pulsamos el botón y aceptamos la instalación, estamos dando nuestro consentimiento para que la aplicación envíe mensajes SMS Premium en nuestro nombre, cuyo coste será cargado en nuestra factura. Este tipo de fraudes se produce muy a menudo en la descarga de juegos, aprovechando la ingenuidad de nuestros menores.
- **Fraudes vinculados al mundo del videojuego.** Otro de los aspectos que aprovechan los ciberdelincuentes es el hecho de que muchos menores utilizan la misma clave de acceso y contraseña para distintos servicios lo que aumenta aún más el riesgo de robo de información personal cuando se es víctima de una estafa. Entre los más importantes tenemos la suscripción oculta y con coste y el robo de tatos. En el primer caso se produce al hacer clic en la publicidad de aplicaciones para móviles. En el segundo caso se produce en algunos juegos muy populares que te ofrecen algunos trucos o vidas infinitas ofreciendo a cambio sus datos de acceso a sus redes sociales.

Revision #1
Created 2022-02-01 12:07:29 CET by Equipo CATEDU
Updated 2022-02-01 12:07:29 CET by Equipo CATEDU

Copyright 2026