



**Mondragon
Unibertsitatea**

Biblioteka

Competencias Digitales

Materiales de formación para
estudiantes de grado

4. Seguridad

4.1. Protección de dispositivos:

4.1.1. Amenazas en el entorno digital

Material elaborado por CRUE-REBIUN y adaptado por la Biblioteca de Mondragon Unibertsitatea



Excepto si se señala otra cosa, la licencia del documento se describe como Atribución-NoComercial 3.0 España, 2020

Seguridad.
Protección de
dispositivos.

AMENAZAS EN EL ENTORNO DIGITAL



CRUE

REBIUN

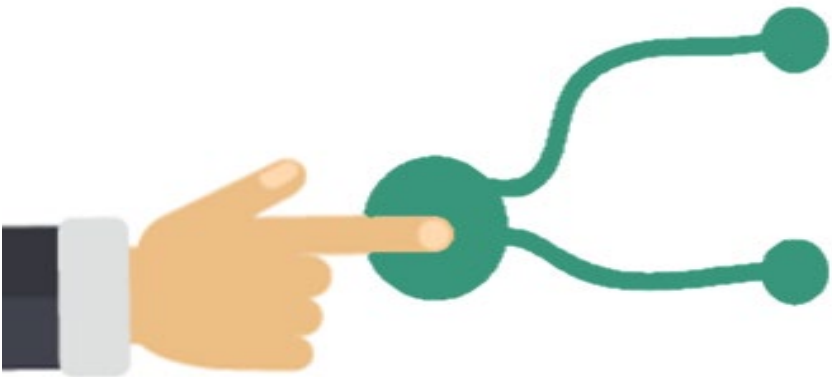
Red de Bibliotecas Universitarias

SUMARIO

- Amenazas de seguridad en línea
- Malware
 - Virus
 - Gusano
 - Spyware
 - Adware
 - Ransomware
 - Troyano
- Phishing
- Botnet
- Spam

OBJETIVO

Al finalizar esta actividad tienes que ser capaz de:



Conocer las características y peligros del software malicioso y otras amenazas

Aprender cómo actúan y cómo se detectan las amenazas en línea

AMENAZAS DE SEGURIDAD EN LÍNEA

Desde el momento en que conectamos nuestros dispositivos a la red estamos expuestos a múltiples amenazas y riesgos, también conocidas como **ciberamenazas**, que aprovechan vulnerabilidades de seguridad para atacar los equipos.

Los **ciberdelincuentes** perfeccionan continuamente sus métodos de ataque para burlar las herramientas de seguridad, por lo que es conveniente ser conscientes y tomar las precauciones necesarias para proteger los dispositivos.

Las principales amenazas que acechan a los dispositivos personales son:

 Malware

 Phishing

 Botnets

 Spam

Los riesgos de seguridad afectan a cualquier tipo de dispositivo conectado: ordenadores, dispositivos móviles u objetos conectados como electrodomésticos, bombillas, altavoces, etc.

AMENAZAS MALWARE

TIPOS DE MALWARE

El malware más conocido es aquel que está destinado a infectar nuestros dispositivos y usarlos como medio de propagación:

☼ Virus

☼ Gusano

Otros tipos de malware pretenden robar nuestros datos personales u obtener beneficios a través de publicidad no deseada:

☼ Spyware

☼ Adware

Un tipo de malware más sofisticado puede llegar a inutilizar los dispositivos mediante el bloqueo de equipos o el cifrado de su contenido:

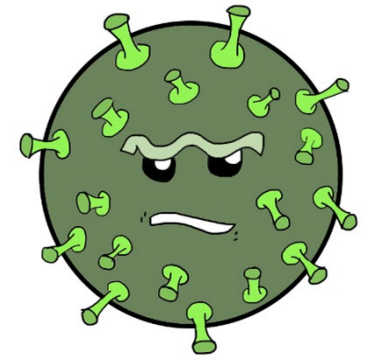
☼ Ransomware

Además, existe un malware oculto que puede contener diferentes tipos:

☼ Troyano



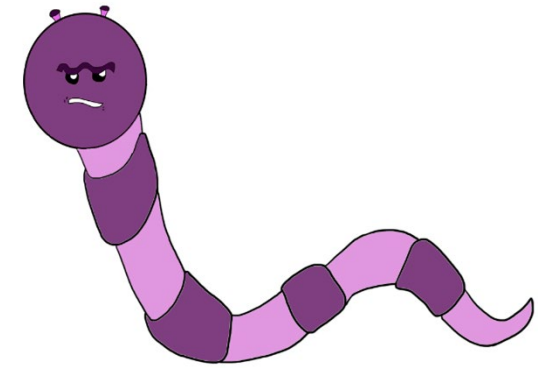
AMENAZAS MALWARE VIRUS



VIRUS

¿Qué es?	Programa o fragmento de código malicioso que se ejecuta en un dispositivo sin nuestro permiso o conocimiento.
¿Cómo llega a los dispositivos?	Se instala al ejecutar un software, al abrir un archivo corrupto a través de una página web o como adjunto al correo electrónico.
¿Cómo actúa?	Infecta archivos y carpetas replicándose a sí mismo sin conocimiento del usuario/a, llegando a modificar o borrar datos y aplicaciones. Su intención es infectar por completo el dispositivo y propagar su código a través de Internet o por medio de otros dispositivos como memorias USB.
¿Cómo se previene?	Se debe evitar: instalar programas o aplicaciones desde fuentes desconocidas, descargar archivos no confiables, o abrir adjuntos de remitentes de correo sospechosos o desconocidos.
¿Cómo se detecta?	El dispositivo puede volverse lento. El comportamiento de las aplicaciones es irregular. La conexión a Internet puede ser inestable. Los programas de detección pueden desactivarse.
¿Cómo se elimina?	Con herramientas antivirus o antimalware.

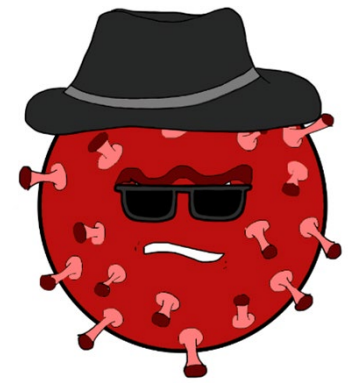
AMENAZAS MALWARE GUSANO



GUSANO

¿Qué es?	Programa malicioso que se ejecuta en un dispositivo sin nuestro permiso o conocimiento.
¿Cómo llega a los dispositivos?	Se instala al abrir un archivo corrupto a través de una página web o como adjunto al correo electrónico.
¿Cómo actúa?	Su principal objetivo es autoreplicarse dentro de un dispositivo de origen y propagarse a través de la red. Al contrario que los virus, no necesita ser ejecutado por el usuario. Comúnmente, consume una gran cantidad de memoria interna y datos de red. No suele causar daños severos en los archivos o dispositivos, pero su actividad puede llegar a bloquearlos.
¿Cómo se previene?	Se debe evitar: descargar archivos no confiables o abrir adjuntos de remitentes de correo sospechosos o desconocidos.
¿Cómo se detecta?	El dispositivo puede volverse lento hasta llegar a bloquearse. La conexión a Internet puede ser inestable. El consumo de datos de red se puede disparar.
¿Cómo se elimina?	Con herramientas antivirus o antimalware.

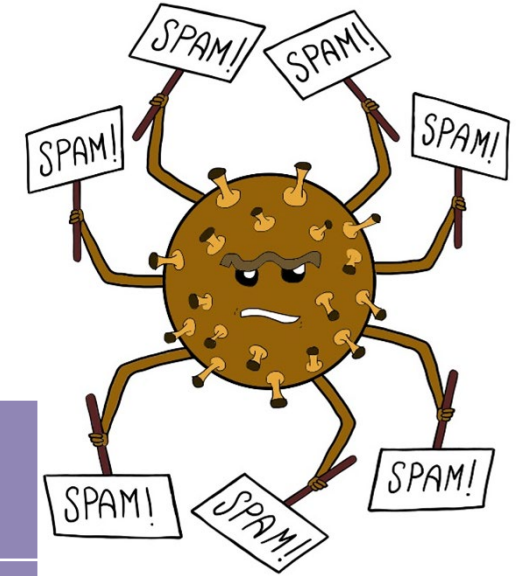
AMENAZAS MALWARESPYWARE



SPYWARE (PROGRAMA ESPÍA)

¿Qué es?	Programa o fragmento de código malicioso diseñado para tomar control de un dispositivo sin consentimiento o conocimiento del usuario.
¿Cómo llega a los dispositivos?	Se instala al ejecutar un software o abrir un archivo corrupto adjunto al correo electrónico. También al acceder a un anuncio publicitario no deseado lanzado desde una aplicación o página web.
¿Cómo actúa?	Se autoinstala y actúa mientras el dispositivo permanece encendido. Captura datos personales, historial de navegación, ubicación, contraseñas o datos bancarios. En ocasiones puede mostrar publicidad no deseada.
¿Cómo se previene?	Se debe evitar: instalar programas o aplicaciones desde fuentes desconocidas, aceptar avisos de ventanas emergentes en el dispositivo o navegador, abrir anuncios no deseados o abrir adjuntos de remitentes de correo sospechosos o desconocidos.
¿Cómo se detecta?	El dispositivo puede volverse lento hasta llegar a bloquearse. Aparición de iconos de nuevas aplicaciones no instaladas por el/la usuario/a. Página de inicio del navegador diferente a la habitual. Mensajes de error no habituales. Aparición de avisos publicitarios no deseados.
¿Cómo se elimina?	Con herramientas antivirus o antispyware . Activando el firewall en equipos con Windows. Instalando un bloqueador de ventanas emergentes en el navegador. Además se recomienda desinstalar aplicaciones sospechosas.

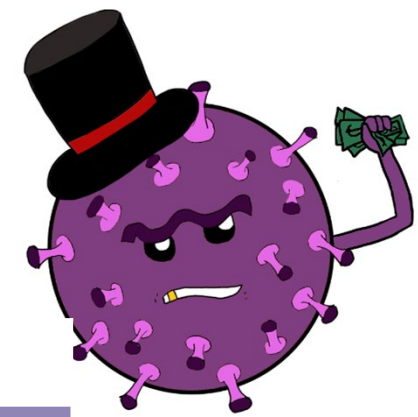
AMENAZAS MALWARE ADWARE



ADWARE (PROGRAMA CON PUBLICIDAD)

¿Qué es?	Programa diseñado para mostrar publicidad no deseada. En general, simplemente es molesto, pero alguna de sus versiones puede actuar como spyware.
¿Cómo llega a los dispositivos?	Se instala al ejecutar un software en el que viene incluido. También al acceder a un anuncio publicitario no deseado lanzado desde una aplicación o página web.
¿Cómo actúa?	Lanza ventanas emergentes desde aplicaciones o páginas web con publicidad no deseada . En ocasiones puede recopilar datos personales, historial de navegación o ubicación.
¿Cómo se previene?	Se debe evitar: instalar programas o aplicaciones desde fuentes desconocidas, aceptar avisos de ventanas emergentes en el dispositivo o navegador, abrir anuncios no deseados.
¿Cómo se detecta?	Aparición de ventanas emergentes con publicidad no deseada. Página de inicio del navegador diferente a la habitual.
¿Cómo se elimina?	Con herramientas antivirus o de eliminación de adware. Actualizando el sistema operativo del dispositivo. Activando el firewall en equipos con Windows. Instalando un bloqueador de ventanas emergentes en el navegador.

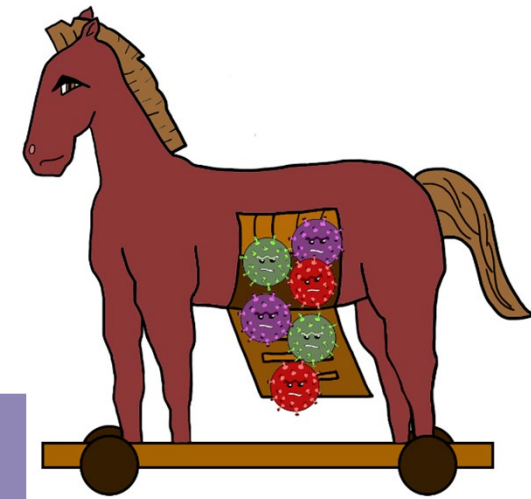
AMENAZAS MALWARE RANSOMWARE



RANSOMWARE (PROGRAMA DE RESCATE)

¿Qué es?	Programa o fragmento de código malicioso que se ejecuta en un dispositivo sin nuestro permiso o conocimiento.
¿Cómo llega a los dispositivos?	Se instala al ejecutar un software, al abrir un archivo corrupto a través de una página web o como adjunto al correo electrónico.
¿Cómo actúa?	Bloquea el dispositivo mostrando un mensaje de advertencia generalmente suplantando la identidad de la Policía o el FBI. En su versión más temible, cifra todo el contenido del dispositivo, impidiendo el acceso a archivos y carpetas, y exige un rescate económico para recuperar el acceso.
¿Cómo se previene?	Se debe evitar: aceptar avisos de ventanas emergentes en el dispositivo o navegador, abrir anuncios no deseados o abrir adjuntos de remitentes de correo sospechosos o desconocidos. Se recomienda hacer copias de seguridad del contenido del dispositivo.
¿Cómo se detecta?	Aparición de ventanas emergentes con avisos suplantando a las autoridades policiales. Imposibilidad de acceder a los archivos o aplicaciones del dispositivo. Aparición de mensajes solicitando un rescate por los archivos.
¿Cómo se elimina?	Actualmente no existe una herramienta que permita eliminarlo de forma eficaz. Se recomienda devolver el dispositivo al estado de fábrica y restaurar una copia de seguridad.

AMENAZAS MALWARE TROYANO



TROYANO

¿Qué es?

Programa en apariencia útil y legítima que aprovecha los privilegios concedidos para saltarse los métodos de seguridad y ejecutar de forma oculta acciones maliciosas.

¿Cómo llega a los dispositivos?

Entra en los dispositivos al instalar un software aparentemente legítimo, que lo contiene de forma oculta.

¿Cómo actúa?

Simula ser de utilidad, pero ejecuta malware como virus o spyware. No se autoreplica, pero una vez activado permite el acceso remoto al dispositivo creando una brecha en la seguridad que se puede traducir en robo de datos personales, borrado de archivos o bloqueo del dispositivo.

¿Cómo se previene?

Se debe evitar: instalar programas o aplicaciones desde fuentes desconocidas, descargar archivos **ejecutables** (extensiones .exe, .vbs, .bat) no confiables, o abrir adjuntos de remitentes de correo sospechosos o desconocidos que contengan ejecutables.

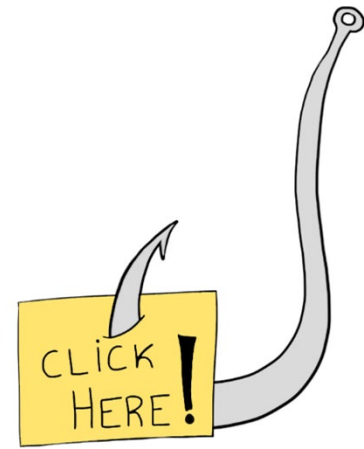
¿Cómo se detecta?

El dispositivo puede volverse lento hasta llegar a bloquearse.

¿Cómo se elimina?

Con herramientas **antivirus** o antimalware. Además se recomienda desinstalar aplicaciones sospechosas.

AMENAZAS PHISHING



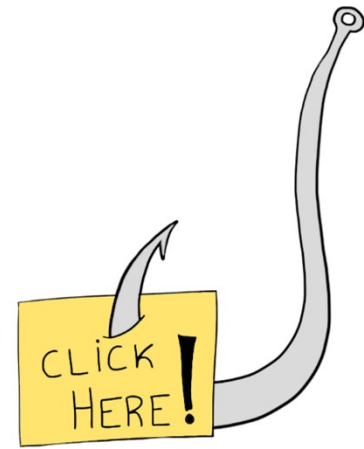
El phishing o **suplantación de identidad** es un método de engaño utilizado por ciberdelincuentes para obtener datos personales como contraseñas de acceso o datos de tarjetas de crédito.

Mediante un correo electrónico, sms o una ventana emergente en el navegador se suplanta la identidad de organismos gubernamentales, servicios de paquetería, entidades bancarias o redes sociales. Estos mensajes nos urgen a facilitar datos personales y enlazan a sitios web que imitan al detalle al original.

Habitualmente este tipo de mensajes es detectado automáticamente por los proveedores de correo o mensajería, pero conviene estar alerta.

AMENAZAS PHISHING

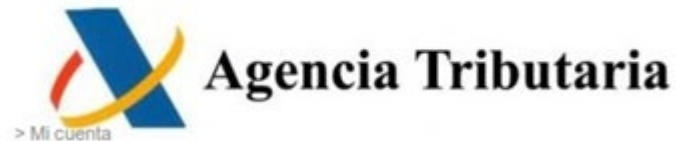
Cuando se reciban mensajes de estas características es importante utilizar el **sentido común** y **sospechar** de un posible intento de phishing.



Para detectar si estamos ante una suplantación de identidad es importante:

- ↳ Eliminar mensajes inesperados donde nos urjan a facilitar datos personales, bancarios o contraseñas.
- ↳ Sospechar de correos con errores gramaticales o faltas ortográficas.
- ↳ Desconfiar de correos impersonales: 'Hola', 'Estimado cliente', 'Estimado amigo'.
- ↳ En caso de acceder al enlace contenido en el mensaje, comprobar la URL de la página a la que nos remite ya que suele estar mal escrita, terminar en otro dominio diferente (por ejemplo: .ly en vez de .es) o ser totalmente ininteligible.

  | a0269908.xsph.ru/agencia/login/index.html?websrc=b120



Ante la sospecha de estar ante un caso de phishing es importante comunicarlo a la entidad suplantada y a las autoridades competentes

AMENAZAS BOTNET



Una red de bots o botnet, es una red de dispositivos que han sido infectados con un malware que se encarga de reclutarlos para efectuar acciones maliciosas sin consentimiento o conocimiento del usuario.

Estas redes, conocidas popularmente como **redes zombi**, controlan cientos de dispositivos para utilizarlos en *ataques de denegación de servicio distribuido* (DDoS), propagación de virus o envío de spam.

Podemos sospechar que nuestro equipo está siendo utilizado en una botnet por motivos similares a los que encontramos en la detección de malware:

- El dispositivo puede volverse lento hasta llegar a bloquearse.
- El consumo de datos puede dispararse.
- Los dispositivos salen continuamente del modo de suspensión o espera.

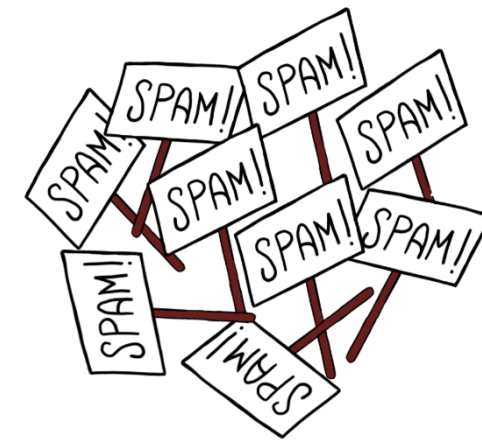
Para prevenir el uso remoto de nuestros equipos es recomendable:

- Evitar instalar programas o aplicaciones desde fuentes desconocidas.
- No descargar archivos no confiables.
- No abrir adjuntos de remitentes de correo sospechosos o desconocidos.

Para eliminar a nuestro equipo de la red de bots es necesario utilizar una herramienta antivirus o antimalware.

La Oficina de Seguridad del Internauta (OSI) ofrece una [herramienta](#) para comprobar si nuestro dispositivo ha sido captado por una botnet.

AMENAZAS SPAM



El correo no deseado, conocido comúnmente como **spam**, son mensajes no solicitados que muestran publicidad sin consentimiento del/a usuario/a procedentes de envíos automatizados que se realizan de forma masiva y aleatoria.

Generalmente lo encontramos asociado al servicio de correo electrónico, pero con la llegada de la web social, es común que este tipo de mensajes no deseados lleguen también por SMS, mensajería instantánea o a través de redes sociales.

El objetivo principal de esta amenaza es vender un producto o servicio, pero en ocasiones se trata de correos de organizaciones o particulares inexistentes que contienen malware adjunto o pretenden engañar al destinatario mediante phishing.

Los servicios de correo electrónico o de mensajería instantánea cuentan con sistemas capaces de filtrar automáticamente este tipo de mensajes desviándolos a carpetas específicas.

Como complemento a estas medidas se recomienda:

- No utilizar la cuenta de correo o número de teléfono principal para servicios de suscripción o newsletters
- No abrir ni contestar mensajes cuyo remitente nos resulte sospechoso o desconocido
- No abrir ni contestar mensajes previamente categorizados como spam
- Categorizar como spam todo aquel correo no deseado que haya logrado burlar los filtros automáticos
- Crear filtros de correo personalizados

PARA SABER MÁS...

Echa un vistazo a estos artículos:

[Ponte al día con los virus informáticos](#)

[Qué es una botnet o una red zombi de ordenadores](#)



**Mondragon
Unibertsitatea**

Biblioteka

Si tienes alguna duda, pregunta en tu [biblioteca](#):



**Basque Culinary Center
Biblioteka**

Juan Abelino Barriola pasealekua, 101
20009, Donostia, Gipuzkoa.
T. 943574514
biblioteca@bculinary.com

**Enpresa Zientzien Fakultatea
Biblioteka**

Ibarra Zelaia, 2
20560, Oñati, Gipuzkoa.
T. 943718009
biblioteka.enpresagintza@mondragon.edu

**Humanitate eta Hezkuntza Zientzien Fakultatea
Biblioteka**

Dorleta, z/g.
20540, Eskoriatza, Gipuzkoa.
T. 943714157
biblioteka.huhezi@mondragon.edu

**Goi Eskola Politeknikoa
Biblioteka**

Campus Iturripe. Loramendi, 4. 20500 Arrasate – Mondragon, Gipuzkoa.
Campus Orona Ideo. Fundazioa eraikuntza, Jauregi Bailara, z/g. 20120 Hernani, Gipuzkoa.
T. 943794700
biblioteka.mgep@mondragon.edu