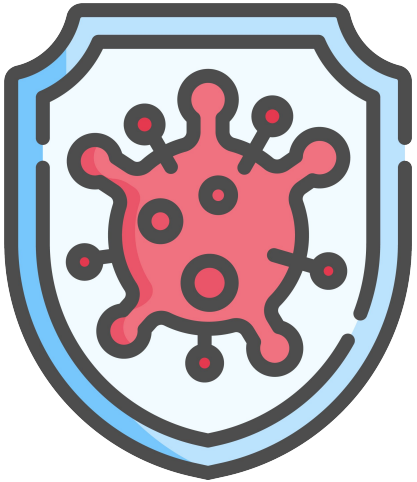
UNIVERSIDAD DE COSTA RICA

CI Centro de Informática



# Ciberataques

## Seguridad de la información

# Temas: III Parte

I Parte

- Ataques a contraseñas
- Ataques por Ingeniería Social
- Medias de protección

II Parte:

- Ataques a las conexiones
- Medidas de protección

**III Parte**

- **Ataques por malware**
- **Medidas de protección**

Centro de Informática

**Expositor:**

**Máster Juan José León.**

Área de Investigación y Desarrollo

Centro de Informática

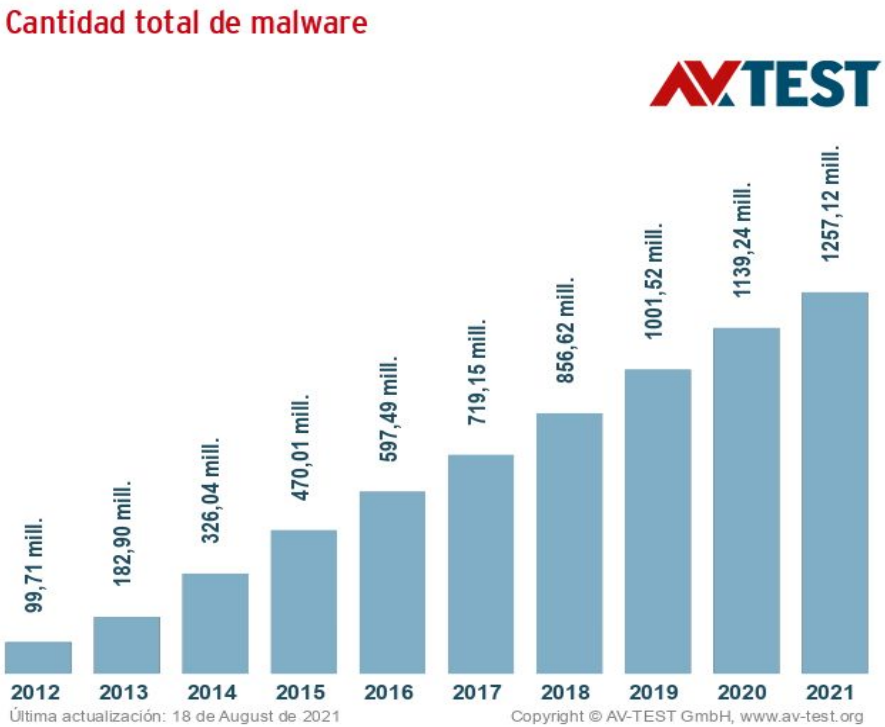
# Malware

Centro de Informática

# Ataques por malware

- Se sirven de programas maliciosos cuya funcionalidad consiste en llevar a cabo acciones dañinas en un sistema informático y contra de nuestra privacidad.
- Buscan robar información, causar daños en el equipo, obtener un beneficio económico a nuestra costa o tomar el control de su equipo.

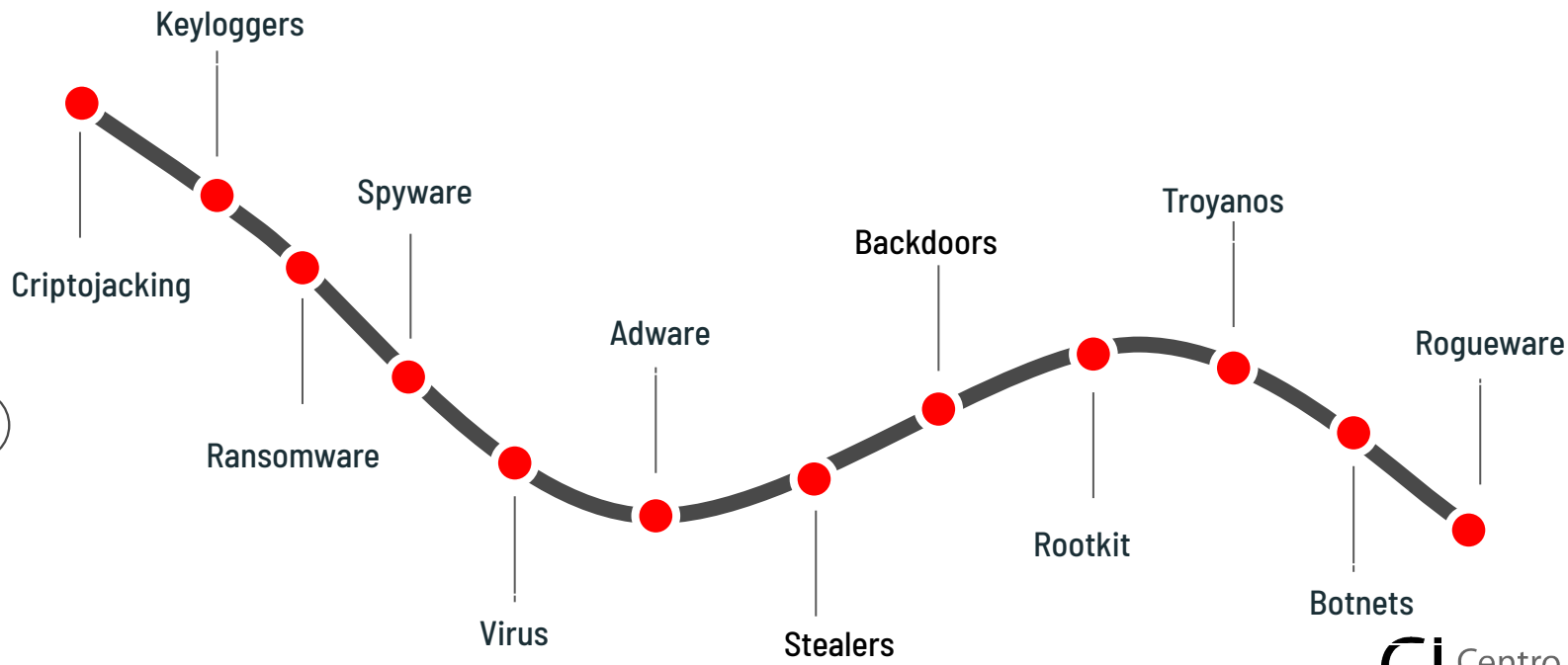
# Ataques por malware




Fuente:
https://www.av-test.org/es/estadisticas/software-malicioso/

Centro de Informática

# Ataques por malware




Centro de Informática

# Formas en las que los dispositivos se pueden infectar con malware

- Aplicaciones y configuraciones vulnerables con conexión a la red
- Correo
- Sitios web
- Dispositivos de almacenamiento externo
- Torrents e intercambio de archivos P2P
- Aplicaciones de mensajería
- Software comprometido

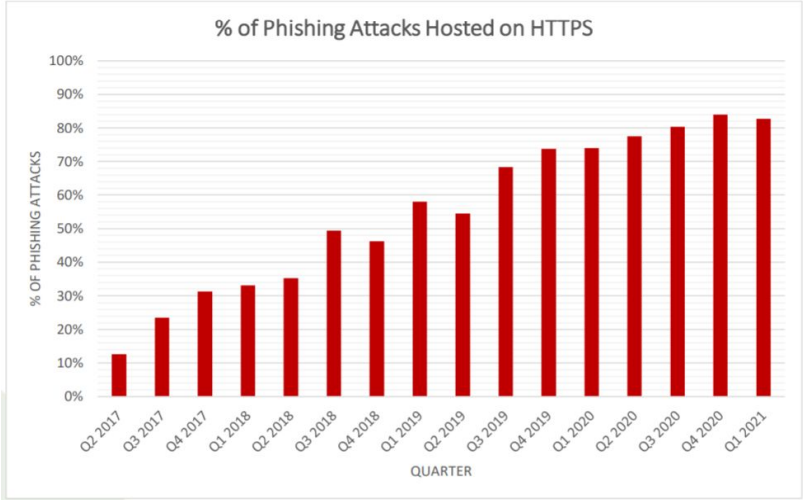
# ¿Mi dispositivo está infectado?

1. El dispositivo empieza a funcionar más lento de lo normal.
2. Disminuye o falta espacio de almacenamiento.
3. Se despliegan ventanas emergentes y programas no deseados.
4. Las aplicaciones se bloquean frecuentemente.
5. Aumenta sin explicación el uso de datos.
6. Despliegue indeseado y constante de anuncios.
7. La batería del dispositivo rinde menos de lo normal.
8. Se dispara la factura telefónica.
9. No es posible instalar o desinstalar aplicaciones.
10. Imposibilidad para ejecutar algunas aplicaciones.
11. Ocurre sobrecalentamiento del dispositivo.
12. Mensajes de error en el sistema.
13. Alertas de que la solución de seguridad entre ellas el firewall no están activas.
14. Aplicaciones con permisos abusivos sobre el sistema o los datos

CI Centro de **Informática**

# Medidas de protección

- **No compartas tu información personal** con cualquier desconocido ni la publiques o guardes en páginas o servicios webs no fiables.
- **Haz copias de seguridad** para minimizar el impacto de un posible ciberataque.
- Utiliza solo **webs seguras con https y certificado digital** y utiliza el modo incógnito cuando no quieras dejar rastro.




Fuente:
Phishing Activity Trends Report APWG
https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf

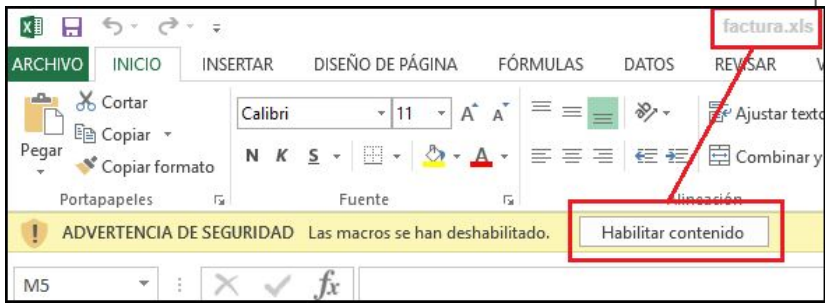
Centro de Informática

# Medidas de protección

- **Utiliza un antivirus** para analizar todas las descargas y archivos sospechosos. Debes mantenerlo siempre actualizado y activo.
- Mantén el **sistema operativo, navegador y aplicaciones siempre actualizadas** a su última versión para evitar vulnerabilidades.
- Utiliza **contraseñas robustas** y diferentes para proteger todas tus cuentas. Si es posible, utiliza la verificación en dos pasos u otro factor de autenticación.
- **Evita conectarte a redes wifi públicas o a conexiones inalámbricas desconocidas.** Especialmente cuando vayas a intercambiar información sensible, como los datos bancarios.

# Medidas de protección

- **Desconfíe de los adjuntos sospechosos, enlaces o promociones** demasiado atractivas. La mayoría de los fraudes se basan en ataques de ingeniería social que pueden ser detectados aplicando el sentido
- En caso de que tengas que conectarte por una emergencia, **trata de utilizar una VPN.**
- **Descarga solo de sitios oficiales aplicaciones o software legítimo** para evitar acabar infectado por malware. En el caso de las aplicaciones, recuerda dar solo los permisos imprescindibles para su funcionamiento.




Fuente:
https://www.incibe.es/protege-tu-empresa/blog/evitar-incidentes-relacionados-los-archivos-adjuntos-al-correo

Centro de Informática

# Tips de reconocimiento de malware o programas potencialmente peligrosos

Demo 1

Examinar correo de phishing

Obtener el enlace malicioso y buscarlo en https://www.virustotal.com/

Abrir el enlace en Firefox, Chrome y Edge.

Ir al sitio https://whois.domaintools.com/ y consultar por los dominios https://www.caixabank.es/, https://ucr.ac.cr y https://ucr.cr

Centro de Informática

# Cómo identificar un correo electrónico malicioso

**Cientos de emails fraudulentos llegan a nuestras bandejas de correo y, aunque muchos son eliminados, otros consiguen su objetivo, ser leídos. Depende de nosotros saber cómo identificar un correo electrónico malicioso:**

### 1 REMITENTE
**¿Esperabas un email de esta persona/entidad?**

Comprueba que el email coincida con la persona o entidad remitente que dice ser o si está suplantando a alguien.

### 2 ASUNTO
**¿Capta tu atención el asunto del correo?**

La mayoría de correos fraudulentos utilizan asuntos llamativos e impactantes para captar tu atención. Ten en cuenta esta consideración.


### 3 OBJETIVO DEL MENSAJE
**¿Cuál es el objetivo del correo?**

Una entidad de servicios como el banco, suministros del hogar (agua, gas) u otros nunca te pedirá tus datos personales por correo. Además, si es de carácter urgente, amenazante o con ofertas y promociones muy atractivas, es muy posible que sea un fraude.

### 4 REDACCIÓN
**¿Tiene errores ortográficos o parece una mala traducción de otro idioma?**

Revisa la redacción en busca de errores de ortografía o gramaticales. Además, si no está personalizado o parece una traducción automática, sospecha.

### 5 ENLACES
**¿Los enlaces llevan a una página legítima?**

Sitúa el cursor encima del enlace, o mantén presionado el enlace en dispositivos móviles, podrás ver la URL real a la que redirige. Si no coincide o es una web sin certificado de seguridad (https://), no hagas clic.

### 6 ADJUNTOS
**¿Contiene un archivo adjunto que no estabas esperando o es sospechoso?**

Analiza los adjuntos antes de abrirlos, puede tratarse de un *malware*.
Los antivirus y analizadores de ficheros te ayudarán a identificar si están infectados.

Finalmente, **no olvides utilizar el sentido común y aplicar todos los contenidos que se encuentran en la OSI** para convertirte en un usuario ciberseguro.

**¡Sigue estas pautas y disfruta de un correo electrónico libre de riesgos!**


GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
@INCIBE INCIBE @INCIBE
017

Mantente al día con nuestras campañas de concienciación para estar informado.
**¡Es nuestra mejor defensa!**
www.incibe.es | www.osi.es

OSI Oficina de Seguridad del Internauta
@osiseguridad osiseguridad

# Tips de reconocimiento de malware o programas potencialmente peligrosos

Demo 2 Android

Búsqueda en google Play de “VirusTotal”

Identificación del desarrollador, revisión de comentarios, # de descargas, permisos para “VirusTotal Móvil”

Revisión de permisos en Android

Apertura de enlaces, ejemplo de identificación con https://unshorten.me/

# Tips de reconocimiento de malware o programas potencialmente peligrosos

Demo 3 Windows

Visita los sitios https://www.amtso.org/security-features-check/

Ejecución de test desde distintos navegadores

https://www.eicar.org

Intento de apertura de archivos descargados desde el explorador de archivos.

# Enlaces de interés

https://apwg.org/trendsreports/

Herramientas

https://www.amtso.org/check-desktop-phishing-page/

https://www.eicar.org

https://www.virustotal.com/

https://phishtank.org/

https://www.amtso.org/security-features-check/

https://opentip.kaspersky.com/

https://www.fortiguard.com/faq/onlinescanner

https://unshorten.me/

# Enlaces de interés

Pruebas de conocimiento

https://www.ftc.gov/es/tips-advice/business-center/small-businesses/cybersecurity/quiz-es

https://phishingquiz.withgoogle.com/?hl=es

# ¡Muchas gracias!

**Contacto:**

Máster Juan José León, juan.leon@ucr.ac.cr

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

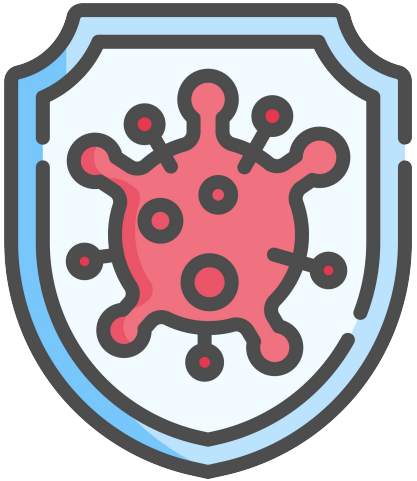
Referencia: Guía de Ciberataques

INCIBE (Instituto Nacional de Ciberseguridad España 2020)

Centro de Informática

UNIVERSIDAD DE COSTA RICA

CI Centro de Informática



# Unidad de Riesgo y Seguridad
# Centro de Informática
# Universidad de Costa Rica

## Seguridad de la información