CIBERSEGURIDAD
o el reto de asumir la responsabilidad de nuestras acciones

ezberdin
ACOMPAÑAMIENTO EN ENTORNOS DIGITALES

GAZTEEN EUSKAL BEHATOKIA OBSERVATORIO VASCO DE LA JUVENTUD

CIBERSEGURIDAD
o el reto de asumir la responsabilidad de nuestras acciones

Ane Martínez Recio
ane@ezberdin.net
@kizkur
637 000 987

ezberdin
ACOMPAÑAMIENTO EN ENTORNOS DIGITALES

GAZTEEN EUSKAL BEHATOKIA OBSERVATORIO VASCO DE LA JUVENTUD

Indice

COMIENZA UN NUEVO DÍA…

- Te conectas a una red wifi.
- Envías o recibes un e-mail o un mensaje instantáneo.
- Haces click sobre un enlace.
- Le das a me gusta a una publicación en redes sociales.
- Publicas contenido en una red social, blog, aplicación o web
- Haces una búsqueda en Google o cualquier otro buscador.
- Te registras en una web o aplicación. Descargas e instalas una aplicación en tu dispositivo.
- Compras algo en una tienda online.

1 / INTRODUCCIÓN

Tenemos la falsa sensación de que lo que ocurre en Internet no pertenece a nuestra vida real, pero es un gran error. Nuestras vidas digitales son una extensión de nuestra vida analógica. Y, **si bien el riesgo 0 no existe, debemos poner las barreras necesarias**.

En muchas ocasiones consideramos que la seguridad informática va ligada a instalar una o varias herramientas en nuestros dispositivos, pero, con frecuencia, se nos olvida que **en nosotros y nosotras está hacer un uso más seguro de Internet.**

Pero…¿para qué quieren mis datos?

TODO DATO ES VALIOSO

(y …¡todo dato tiene un precio!)

Beneficio económico

- Robo de dinero mediante fraudes o software malicioso
- Extorsión online
- Venta de datos e información personal robada

Suplantar identidad

Nuestro nombre, apellidos, nuestras fotos, direcciones, teléfono, etc…pueden usarse para suplantarnos en redes sociales o para contratar servicios online

https://haveibeenpwned.com

¿QUÉ DAÑO NOS PUEDE HACER UN CIBERATAQUE?

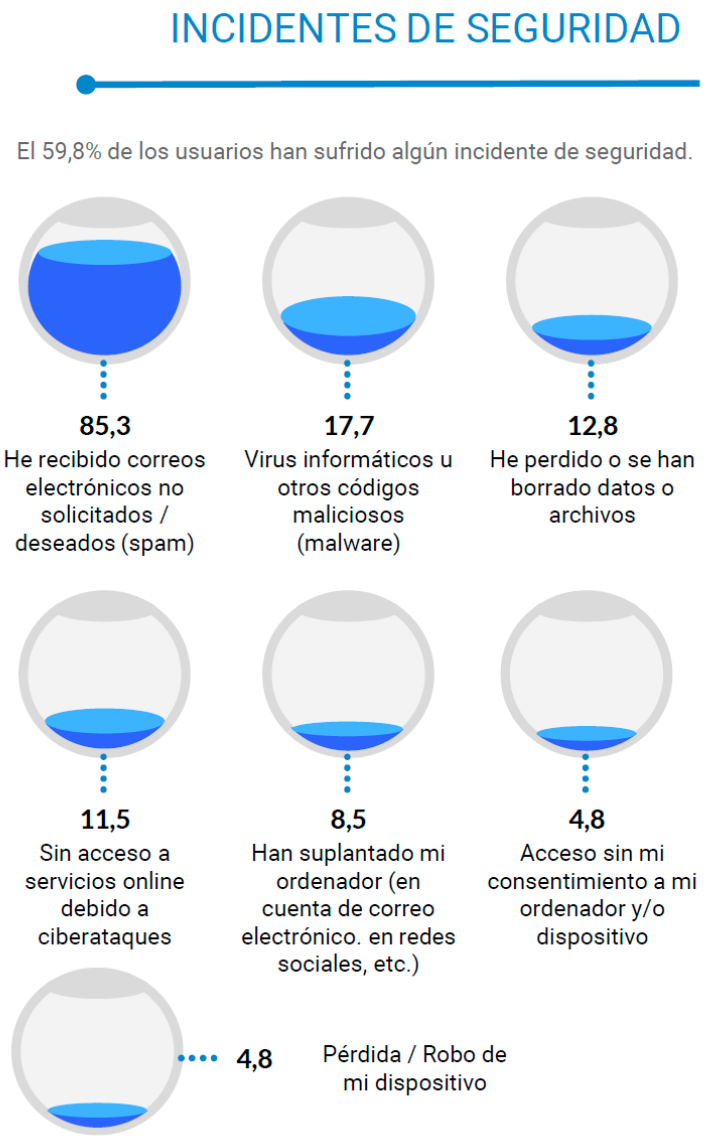
Indudablemente, el principal objetivo de los cibercriminales es **ganar dinero**. Por eso, cuando nos roban información a través de un ataque informático, su siguiente paso es venderla en el mercado negro o aprovecharla para sacar algún tipo de beneficio con ella.

Cualquier dato sensible puede ser moneda de cambio, desde el contenido que guardamos en nuestro correo electrónico, hasta en nuestro ordenador o teléfono móvil. También son de gran valor las direcciones de e-mail, los datos bancarios y de tarjetas de crédito (aunque nos pueden colar aplicaciones que directamente cogen el dinero de cuentas bancarias. *Ej: Android.Fakebank)*

El riesgo que corremos es que, desde el momento en el que tenemos en nuestras manos un dispositivo con conexión a Internet y lo consideramos algo ajeno a nuestra vida, no lo protegemos ni lo cuidamos y podemos no ser conscientes de cuándo nos han atacado y **puede que pase mucho tiempo hasta que nos enteremos**.

Ahora bien, cada problema tiene una solución…

“Tener información y conocer las diferentes técnicas de ataque a las que podemos estar expuestos es vital para poder detectarlas a tiempo y evitar futuros problemas”



Fuente: Estudio sobre la ciberseguridad y confianza del icudadano en la Red (ONTSI). Julio-Diciembre 2019

2 / TIPOS DE ATAQUES MÁS COMUNES y cómo detectarlos

CIBERSEGURIDAD
o el reto de asumir la responsabilidad de nuestras acciones

SPAM

https://www.osi.es/es/servicio-antibotnet

Correos enviados de manera masiva a muchos destinatarios. Contenido publicitario o comercial.

CONSEJOS BÁSICOS Y PREVENCIÓN

- NUNCA responder al spam, sólo les confirmas tu dirección
- NO abrir ningún enlace, pueden llevar a webs falsas que recopilan información sobre nosotros
- Valorar bien dar nuestra dirección a un concurso o sorteo
- OJO al cancelar la suscripción

BUENA PRÁCTICA

- No utilizar la misma dirección de correo para todo
- En caso de tener que hacer pública nuestra dirección de correo evitar ser indexados por los buscadores ane**[arroba]**ezberdin**[punto]**net

SPIM

Mensajes enviados de manera masiva a muchos destinatarios, pero a través de nuestros teléfonos. Habitualmente sms y servicios de mensajería. Contenido publicitario o comercial. Nos llegan a través de uno de nuestros contactos, suelen finalizar con un mensaje que nos dirige a la página fraudulenta e infectar nuestro Smartphone.

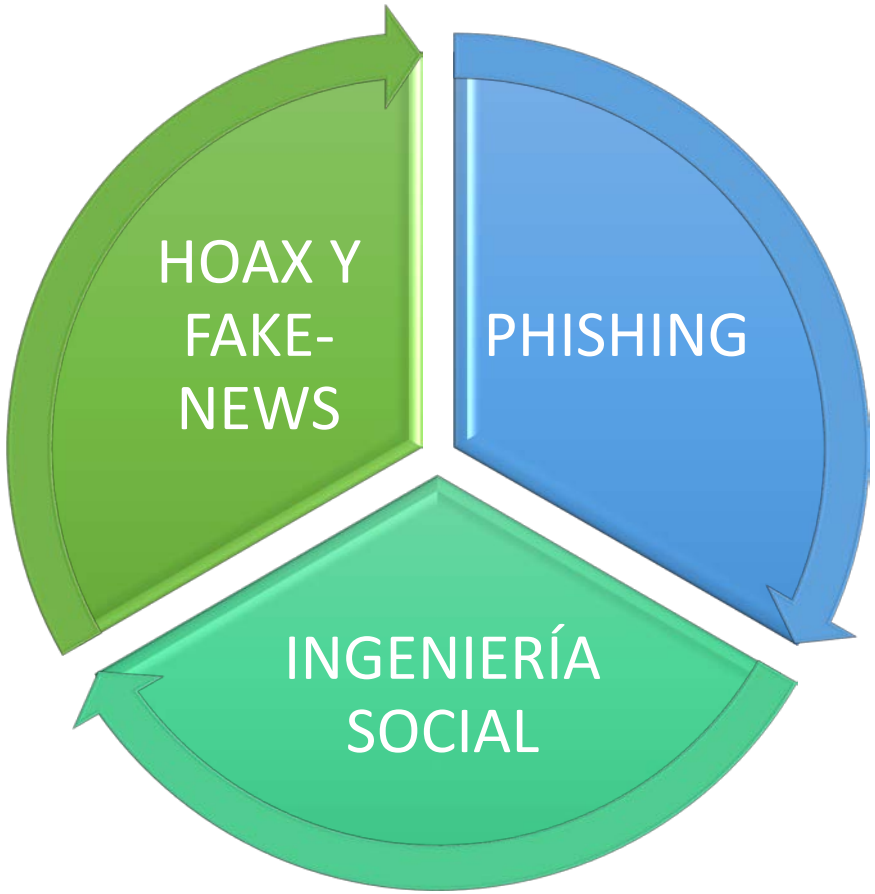
CONSEJOS BÁSICOS Y PREVENCIÓN

- ☞ Evita hacer público tu número de teléfono en redes sociales, foros o páginas web
- ☞ No acceder a los enlaces que puedan aparecer en el mensaje

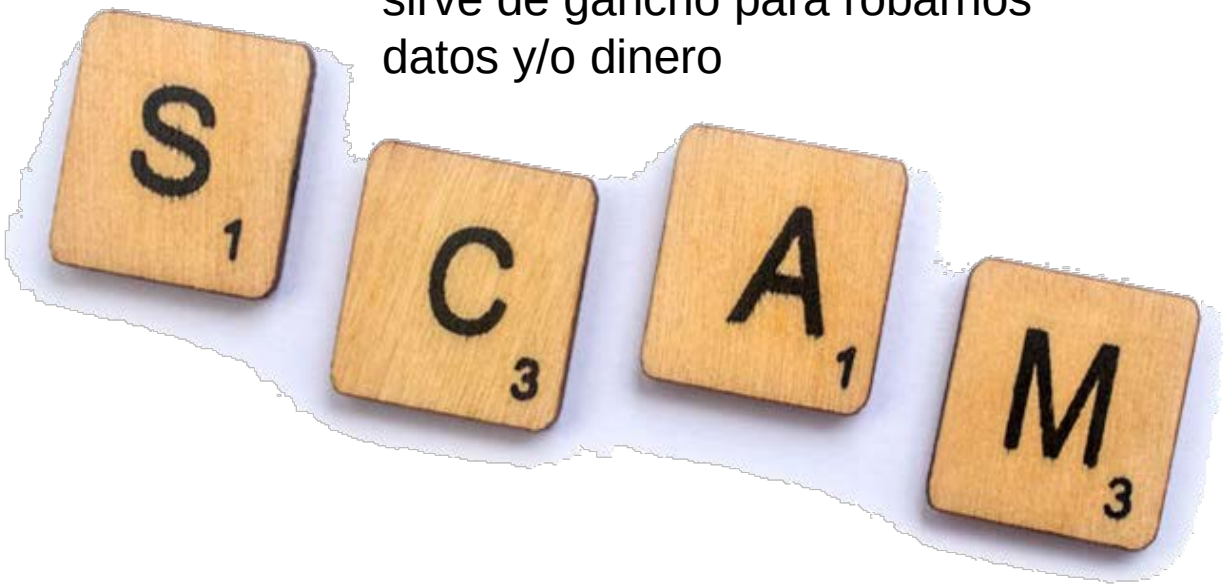
BUENAS PRÁCTICAS

- ☞ Mantener actualizada la app de mensajería
- ☞ Advertir a quien te lo ha mandado ya que su dispositivo puede estar infectado.

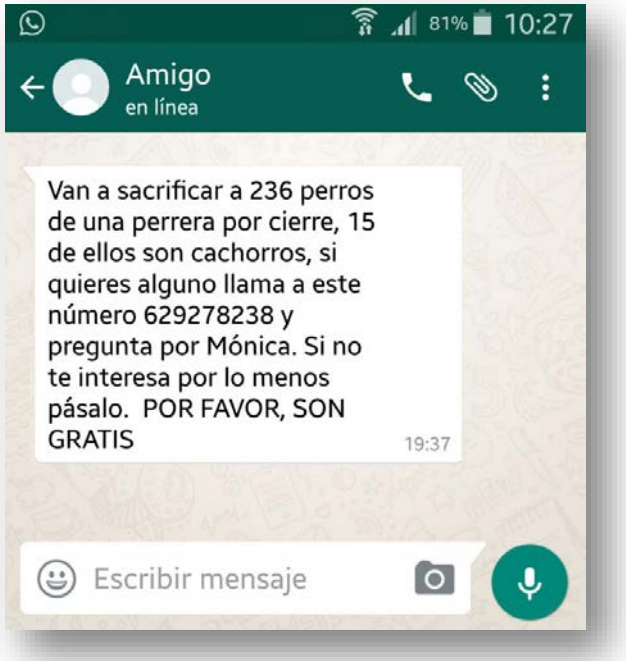
FRAUDES Y EXTORSIONES



Técnicas de engaño con contenido falso y ventajoso que sirve de gancho para robarnos datos y/o dinero



HOAX



Señales de alarma

1. Se solicita reenviar el mensaje a tantas personas como sea posible
2. Se amenaza con consecuencias si se ignora esta solicitud
3. No se nombra la fuente que añadiría credibilidad a la noticia o se da una fuente falsa
4. No se citan detalles acerca del autor y el origen de la información
5. Información sobre el tiempo, como "la semana pasada" o "el día de ayer“, nunca se menciona un claro momento en el tiempo

En muchos casos de correo electrónico, la estructura del mensaje indica que se ha copiado y reenviado en numerosas ocasiones. Esto se puede reconocer porque el texto ya no tiene ningún formato o en el correo electrónico aparecen numerosos destinatarios.

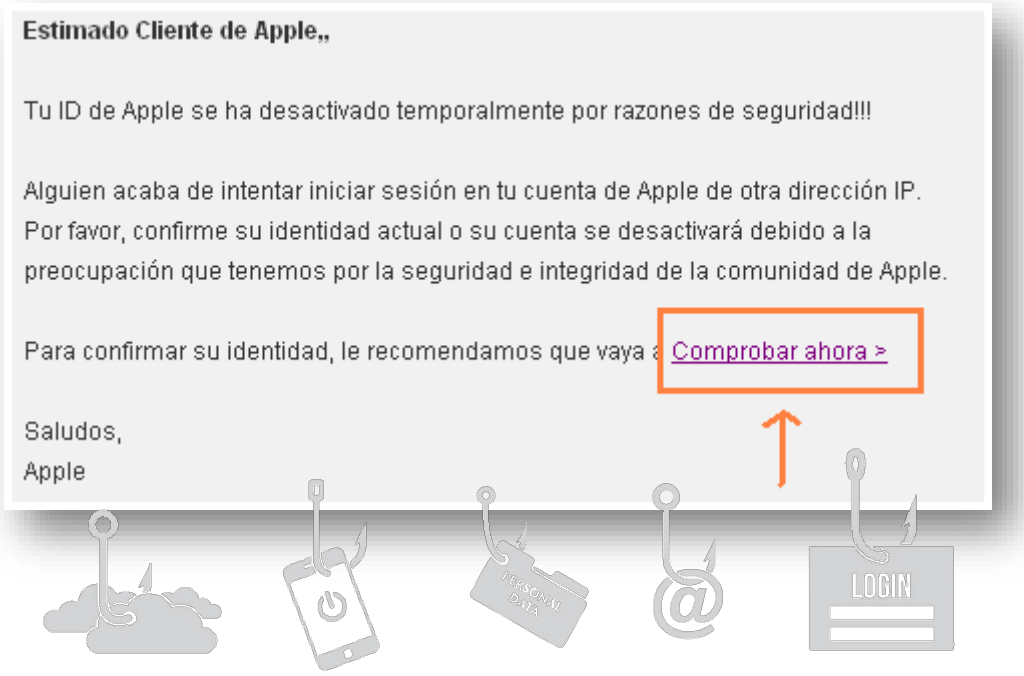
Un hoax es fácil de reenviar, pero no siempre es sensato hacerlo a ciegas. Piénsatelo primero antes de reenviarlo, los engaños aprovechan la tendencia de los usuarios a preocuparse o a empatizar…

PHISING

El phishing es una amenaza en la que los atacantes utilizan mecanismos de ingeniería social con intención de engañarnos para que les revele mis datos confidenciales y puedan suplantar mi identidad en sitios web o transaciones financieras.

El objetivo del phishing es obtener datos (credenciales) o engañar al usuario para infectarlo.
Lo hacen pidiéndonos:

1. Que respondamos a los e-mail facilitando nuestra información.
2. Que descarguemos un archivo que se adjunta en el correo y contiene un virus.
3. Que nos pidan pinchar sobre un enlace que conduce a una página web fraudulenta en la que el atacante puede pedir otras acciones como meter datos personales que les llega a los atacantes.



La mejor prevención para el phishing se basa en desconfiar del contenido que recibimos a través del e-mail, mensajería instantánea, redes sociales e incluso desconfiar cuando alguien nos llama para pedirnos información privada por teléfono.

TIPOS DE ATAQUES MÁS COMUNES
Mensajes maliciosos

Sidertia

España es el sexto país que más ataques de phishing sufre

Endpoint 18 SEP 2019

NOTICIAS

El 90% de las empresas del globo sufrió 'phishing' en 2019

Tags: Ciberseguridad phishing

También te puede interesar:

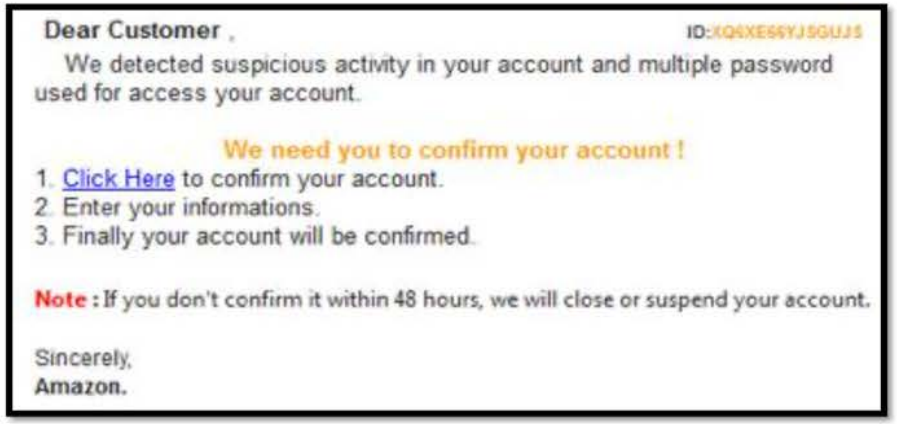
- Los ciberdelincuentes se valen de herramientas gratuitas en su última campaña de 'phishing' mundial
- Una campaña de 'phishing' trata de robar los datos de los usuarios de Bankia
- 225.000 intentos diarios de 'phishing' en 2018

CIBERSEGURIDAD
o el reto de asumir la responsabilidad de nuestras acciones

CCN-CERT
centro criptológico nacional

Sidertia

MEJORAS EN LOS NUEVOS PHISHING



Dear Customer ,

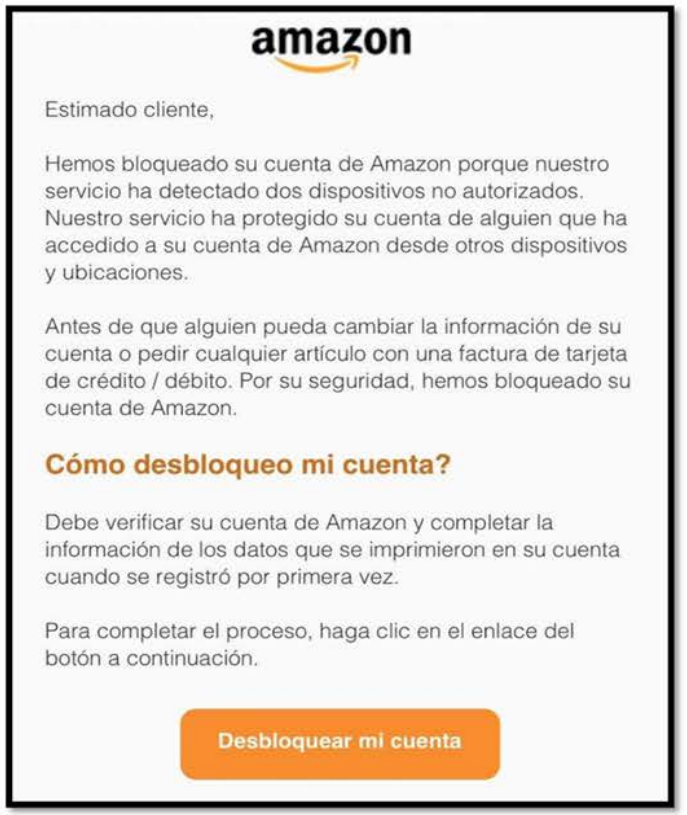
We detected suspicious activity in your account and multiple password used for access your account.

We need you to confirm your account !

1. Click Here to confirm your account.
2. Enter your informations.
3. Finally your account will be confirmed.

Note : If you don't confirm it within 48 hours, we will close or suspend your account.

Sincerely,
Amazon.



amazon

Estimado cliente,

Hemos bloqueado su cuenta de Amazon porque nuestro servicio ha detectado dos dispositivos no autorizados. Nuestro servicio ha protegido su cuenta de alguien que ha accedido a su cuenta de Amazon desde otros dispositivos y ubicaciones.

Antes de que alguien pueda cambiar la información de su cuenta o pedir cualquier artículo con una factura de tarjeta de crédito / débito. Por su seguridad, hemos bloqueado su cuenta de Amazon.

Cómo desbloqueo mi cuenta?

Debe verificar su cuenta de Amazon y completar la información de los datos que se imprimieron en su cuenta cuando se registró por primera vez.

Para completar el proceso, haga clic en el enlace del botón a continuación.

Desbloquear mi cuenta

INGENIERÍA SOCIAL

Se basa en interactuar con la víctima para ganarse su confianza. El fraude y el phishing utilizan técnicas de ingeniería social.

Los **objetivos** de la ingeniería social son:

- ☞ Claves de acceso a cuentas y servicios (usuari@ y contraseña)
- ☞ Datos personales o sensibles
- ☞ Información bancaria: acceso a cuentas online, datos de tarjetas de crédito
- ☞ Infectar un ordenador o dispositivo, para acceder a su información de forma remota.

Ejemplos:

- *email para reactivar un servicio, una llamada mediante un sistema automático (una máquina que nos dice que nuestra tarjeta ha sido bloqueada y nos dan los pasos para desbloquearla)*
- *larga encuesta en la que se nos van preguntando datos personales*
- *memoria USB abandonada a posta en un lugar estratégico para infectar un ordenador y controlarlo de forma remota (BAITING)*
- *ventana que alerta sobre un fallo de seguridad en nuestro pc y ofreciendo la descarga de un software o un número al que llamar, además de pagar una cantidad de dinero para solucionarlo (timo del servicio técnico)*

SPAM - PHISHING

Es habitual confundirlos

	Objetivo	Formato	Remitente	Enlaces	Variantes
SPAM	Anunciar un producto o servicio	Suele tener mala redacción o errores gramaticales. Ningún tipo de diseño, sólo texto.	Puede provenir de una empresa real.	Suelen redirigir a las webs donde adquirir los productos	No sólo se aplica al correo electrónico.
PHISHING	Obtener información personal o financiera	Incluye logotipo y colores de la entidad por la que se hace pasar. Contenido más elaborado	Suplanta la identidad de una compañía u organismo, intentando engañar al destinatario.	Dirigen a webs fraudulentas donde recopilan la información de la víctima.	Se distribuyen campañas de phishing a través de email, sms o apps de mensajerías.

Fuente: Ciberseguridad: consejos para tener vidas digitales más seguras.

Tipos de código dañino

Cuando se habla de código dañino o malware se está haciendo referencia a programas que se instalan en un sistema informático, normalmente de forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los sistemas operativos, aplicaciones y datos de dicho sistema, o bien simplemente para molestar o perjudicar al usuario.

Fuente: CCN, centro criptológico nacional

Cada día surgen nuevas muestras de malware susceptibles de mutar o transformarse adquiriendo nuevas funcionalidades y capacidades de ocultación. Aun así, se establece a continuación una clasificación básica sobre los tipos de malware más comunes que se pueden encontrar en el panorama actual.

VIRUS

- ✓ Código malicioso que tiene la capacidad de propagarse haciendo copias de si mismo.
- ✓ Efectos diversos según el tipo de virus que sea (ralentización del dispositivo, acciones inesperadas y autónomas en ellos o aplicaciones que se bloquean…)
- ✓ La fuente de infección puede ser a través de Internet o mediante un dispositivo externo.

GUSANOS

- ✓ Programa malicioso que también es capaz de replicarse a sí mismo y difundirse a través de la Red rápidamente.
- ✓ A diferencia de los virus no necesitan ser ejecutados por una persona.
- ✓ Su objetivo es infectar el mayor número de dispositivos posibles.
- ✓ Se utilizan para crear botnets (redes zombies de dispositivos que se activan de manera simultanea para cometer ciberataques).

https://www.osi.es/es/servicio-antibotnet

TROYANO

Caballo de Troya, o **troyano**, es un **malware que se presenta como un programa legítimo**, pero que, al ejecutarlo, abre un acceso remoto a nuestro dispositivo. Es decir, no es algo que se acopla a algo nuestro sino que, directamente lo descargamos como un programa legítimo (parches, juegos, películas, etc…son su camuflaje perfecto).

Los datos que recoge se envían al atacante mediante el correo electrónico o se almacenan en un servidor en espera de ser utilizados para tomar el control de nuestro dispositivo (archivos, micrófono, teclado, webcam…)

Los troyanos se clasifican según el tipo de acciones que pueden realizar en nuestros dispositivos:

- Backdoors
- Keyloggers
- Banker
- Downloader
- Botnets
- Proxy
- Password Stealer
- Dialer
- Cementery

ADWARE

Software malicioso que **muestra publicidad no deseada**. Además de molesto el peligro real del adware está en que puede cambiar los resultados de nuestras búsquedas con el propósito de llevarnos a sitios no legítimos o incluso infectadas con otros tipos de malware.

Puede instalar barras de herramientas y manipular la configuración de nuestro navegador cambiando incluso la página de inicio.

Prevenirlo y eliminarlo:

- ☞ Revisar periódicamente las extensiones instaladas en nuestros navegadores y tenerlo actualizado a las últimas versiones disponibles.
- ☞ Revisar los últimos programas instalados y desinstalarlos
- ☞ Si se cambia la lista de buscadores predeterminados eliminarlos y restaurar el nuestro.

SPYWARE

Software malicioso creado para recopilar información de nuestros dispositivos y enviársela a una tercera persona sin nuestro consentimiento (hábitos de navegación, historial y otros datos sensibles…) bien para suplantar nuestras identidades o para utilizarlos con fines comerciales.
Actúa de forma silenciosa porque su finalidad es recoger cuanta más información mejor.
Llegan a través de mensajes de correo, de descargas de la Web, ocultos en otros programas o tras hacer click en ventanas de publicidad.

Prevenirlo y eliminarlo:

- ☞ Revisar periódicamente los iconos de nuestra bandeja del sistema.
- ☞ Revisar los últimos programas instalados y desinstalarlos.
- ☞ Si se cambia la lista de buscadores predeterminados eliminarlos y restaurar el nuestro.
- ☞ Utilizar programas de confianza y actualizarlos periódicamente.

2 / TIPOS DE ATAQUES MÁS COMUNES
Software malicioso – Spyware

	Qué es	Daños provocados	Prevención
VIRUS	Infecta a otros archivos o programas.	Daños en el equipo, borrado o manipulación de archivos.	Cuidado a la hora de usar USB externas o descargar archivos.
GUSANOS	Se replican a sí mismos y se propagan solos.	Usados para crear botnets, redes de dispositivos zombies.	Evitar descargar adjuntos no solicitados.
TROYANOS	Crean puertas traseras por donde entrar y controlar el equipo en remoto.	Robo de información y control de webcam, teclado, micrófono…	Instalar antimalware que pueda deterctarlos y realizar análisis periódicos.
ADWARE	Muestra publicidad no deseada y altera búsquedas.	Manipula resultados de búsquedas y lleva a págs. alteradas o a la descarga de malware.	Evitar instalar programas de páginas o tiendas no oficiales.
SPYWARE	Recopila información de las personas usuarias.	Recopila información sobre hábitos de navegación, programas instalados o datos sensibles.	No aceptar cuadros de diálogo que aparezcan al navegar.

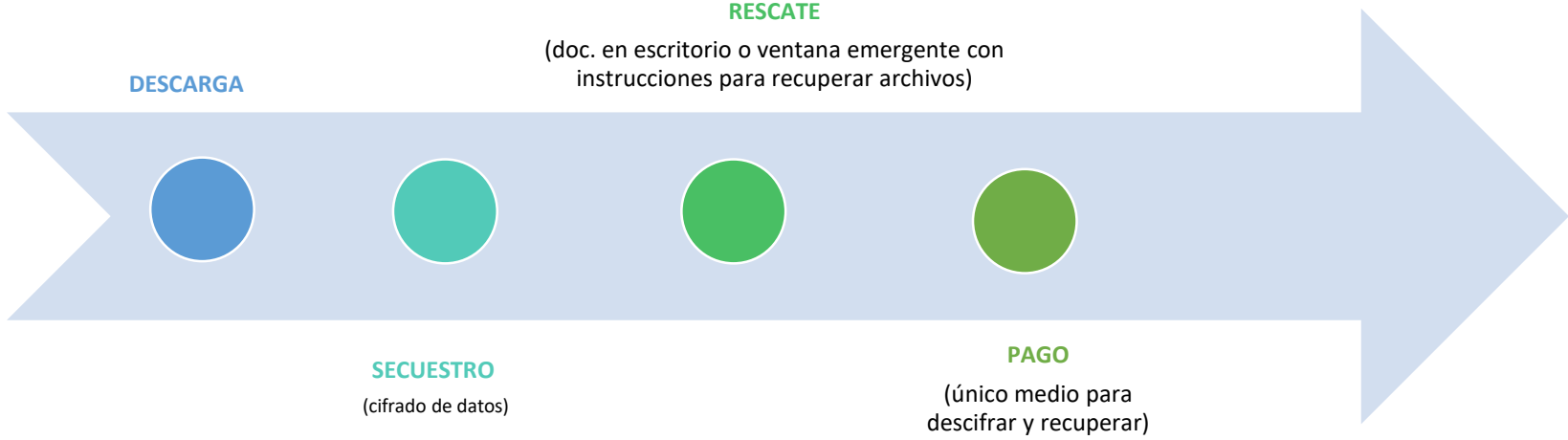

UPPS..!!
YOUR PERSONAL FILES ARE ENCRYPTED
Make payment or private key will be destroyed in
01:34

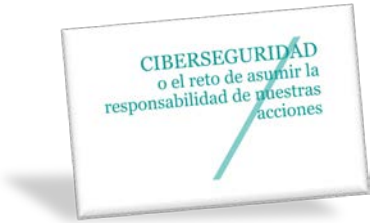
RANSOMWARE

Software malicioso capaz de “secuestrar” nuestros dispositivos y/o archivos mediante del **cifrado de datos**, y solicita un rescate para descifrarlos.
Es un tipo de **extorsión económica** que afecta a todo tipo de dispositivos; ordenadores, smartphones, tablets e incluso a los que incorporan el llamado “Internet de las cosas” (wearables, electrodomésticos, coches…)

Los ganchos son entidades o empresas destacadas (Correos, Amazon, entidades bancarias…) que nos ofrecen campañas y acciones que bien pudieran ser lícitas. Es decir, se basa en una combinación de correo electrónico malicioso, phishing y mucha ingeniería social.

Fases:





MIS DATOS…
¡MI TESORO!

CIBERSEGURIDAD
o el reto de asumir la responsabilidad de nuestras acciones

CÓMO PROTEGER MIS DATOS

Gran parte de las amenazas que pueden afectar a la seguridad de nuestros datos y dispositivos depende de la precaución (actitud + aptitud) que tengamos mientras realizamos las tareas más comunes; correo electrónico, navegar por internet, banca electrónica, redes sociales, etc…

Acciones que podemos realizar las personas para reforzar esa actitud de cautela y precaución:

- Autenticación Segura
- Copias de seguridad y Cifrado de Datos
- Herramientas específicas

AUTENTICACIÓN SEGURA

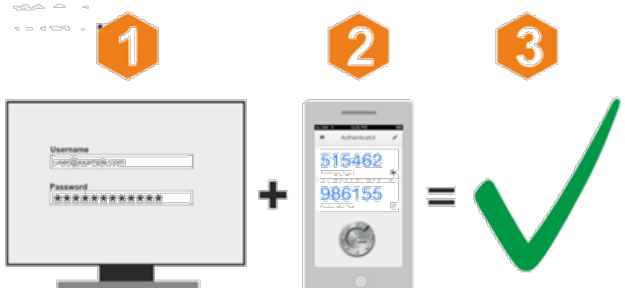
- Algo que tú sabes (nombre de usuari@ y la contraseña).
- Doble autenticación:
  - Me envíe un SMS al móvil
  - Me envíe una clave por email
- Aplicaciones de terceros:
  - Google Autenticator / Microsoft Autenticator, …
- Algo que tú tienes; llaves criptográficas (Titan Keys)
- Algo que tú eres
  - Huella dactilar
  - Reconocimiento facial
  - Iris, ...

CONTRASEÑAS

Las contraseñas son las **llaves** que dan acceso a nuestros servicios, y por ende a nuestra **información personal,** por lo que si alguien las consigue puede comprometer nuestra **privacidad**, pudiendo, entre otras cosas; publicar en nuestro nombre en redes sociales, leer y contestar a correos electrónicos haciéndose pasar por nosotros, acceder a nuestra banca online, etc.

SEGURAS Y ROBUSTAS

DOBLE AUTENTICACIÓN



GESTORES DE CONTRASEÑAS

KeePass
LastPass
1Password
bitwarden

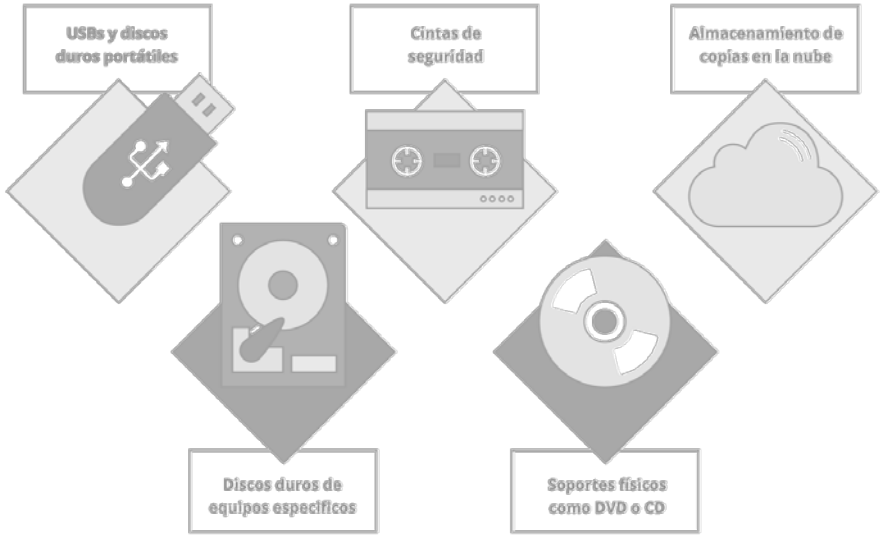
📽 Cómo generar contraseñas seguras

📽 Repaso prácticas seguridad

COPIAS DE SEGURIDAD

Si, como hemos indicado, los datos son nuestro gran tesoro y el objetivo último de todos los ataques en Internet, es lógico que tengamos especial cuidado en “tenerlos a buen recaudo”.

Existen soluciones mediante programas específicos para automatizar las copias de seguridad de nuestros dispositivos. También podemos hacerlas a mano, pero siempre debieran de ser en dispositivos o soportes externos ya que si, sufrimos un ataque o el dispositivo electrónico se pierde o inutiliza, nuestros preciados datos seguirán bajo nuestra custodia.



📣 Guía copias de seguridad

📣 #CómoHacerCopiasDeSeguridad

💣 *Atención a cómo finalizamos la vida útil de nuestros dispositivos, según la importancia de los datos que contengan no valdrá con formatear los discos duros*

BORRADO SEGURO DE DATOS

Se puede pensar que un simple formateo del disco duro impedirá que los datos almacenados en el mismo puedan ser recuperados. Sin embargo, hay aplicaciones que permiten **deshacer el formateo** de una unidad existiendo incluso métodos para **recuperar los datos** de los discos, aunque estos hayan sido sobrescritos.

Si se quiere garantizar que no se está distribuyendo información sensible, se deben sobrescribir los datos siguiendo un método (patrón de borrado) que no permita su recuperación de modo alguno.

Para tal fin, es necesario realizar **diversas pasadas de escritura** sobre cada uno de los sectores donde se almacena la información. Para simplificar la tarea, lo más sencillo es utilizar alguna aplicación especializada que permita eliminar la información de forma sencilla.

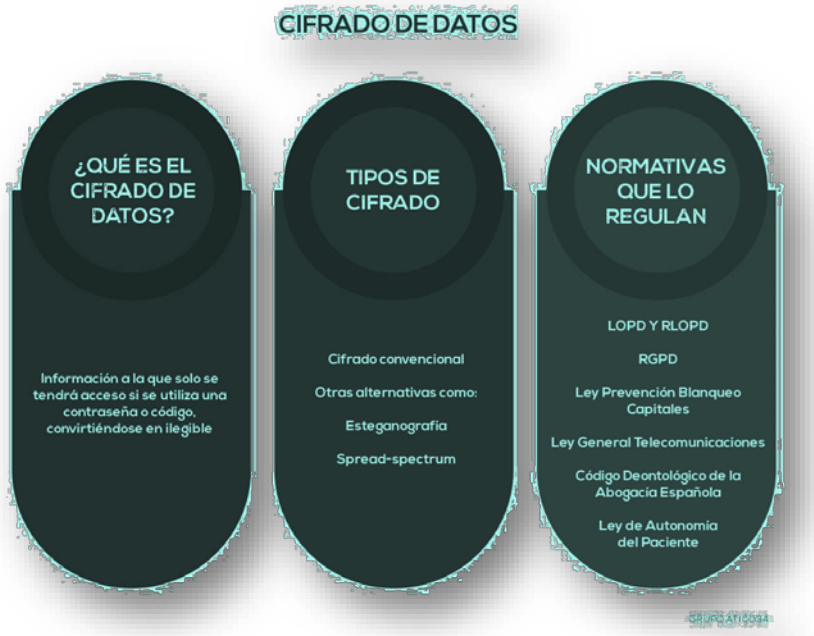
En el caso de fotografías digitales, archivos de audio o vídeo y documentos ofimáticos existen **metadatos** que pueden almacenar información oculta y no visible usando la configuración estándar de las aplicaciones, necesitando de una configuración específica o incluso un software concreto para revelar esos datos.

Fuente: Centro Criptográfico Nacional CCN

CIFRADO DE DATOS

Cifrar o encriptar información supone ocultar el contenido a simple vista, de modo que para acceder a esos archivos, carpetas, unidades, mensajes, etc…sea necesario realizar una interacción concreta. Se hace mediante la aplicación de un algoritmo matemático. Esto no es nuevo y ya existía desde hace 2.500 años

El cifrado, por tanto, **es el elemento más importante de la seguridad de datos y la manera mas simple de impedir que alguien robe o lea la información de un sistema digital con fines malintencionados.**



📣 Incibe | Protección de la Información

Además de proteger la información privada contra robos o amenazas, el cifrado también nos permite desmostrar la integridad y el origen de la información (base de los certificados digitales y firmas electrónicas). Existen varios métodos (clave simétrica y asimétrica) y muchas herramientas diversas para realizarlos (BilLocker en Win10-noHome-, FileVault en Apple, Veracrypt, AxCrypt, Kleopatra, etc..)

HERRAMIENTAS

Existen también herramientas que nos ayudan a **proteger nuestros dispositivos** (ordenador, smartphone, tablet) para que nuestras vidas digitales sean lo más seguras posibles.
La instalación de programas puede afectar al rendimiento y la seguridad de los dispositivos/equipos ya que, de hecho, son la vía de entrada de malware. Por ello, se recomienda:

Fuente: Oficina de Seguridad del Internauta (OSI)

- utilizar software legal y actualizado,
- no ejecutar a la ligera programas de origen desconocido, y
- trabajar habitualmente en el sistema como usuari@ sin privilegios, no como “Administrador”

HERRAMIENTAS

Malwarebytes · AdwCleaner · Spybot Search & Destroy · kaspersky · ESET

📣 Herramientas gratuitas | Oficina de Seguridad del Internatuta (OSI)

¿ALGO MÁS?

CIBERSEGURIDAD
o el reto de asumir la responsabilidad de nuestras acciones

NAVEGACIÓN SEGURA

La comunicación en Internet se sustentan en una idea básica: clientes (ordenador, teléfono, tableta, etc…) - servidores (webs, bases de datos…) que proporcionan información. Esta comunicación se lleva a cabo a través de un protocolo (http, https, ftp, etc..).

A su vez, el cliente está identificado en la red mediante una **dirección IP (TCP/IP)** y cada vez que se conecta a un sitio web éste (el servidor) conoce automáticamente la dirección IP, **nombre del dispositivo**, la página de procedencia, etc. Se produce un intercambio de información que habitualmente no es visible y donde el **navegador web** es el que facilita la mayoría de esos datos.

1. Un alto porcentaje de los usuarios no es consciente de la cantidad de información que, de forma inadvertida e involuntaria, está revelando a terceros al hacer uso de Internet.
2. Cada vez que se visita un sitio web, se suministra de forma rutinaria una información que puede ser archivada por el administrador del sitio.
3. Al sitio web le resulta trivial averiguar la dirección de Internet de la máquina desde la que se está accediendo, sistema operativo, etc.
4. Con ayuda de las "*cookies*" se puede personalizar aún más la información recabada acerca de los visitantes, registrando las páginas más visitadas, preferencias, tiempo de la visita, software instalado, etc.

Fuente: Centro Criptográfico Nacional (CCN)

NAVEGACIÓN SEGURA

Un **navegador web**, en favor de la máxima usabilidad, permite que se acceda a información aparentemente inofensiva.

La dirección IP pública con que se conecta el usuario.

- Tu dirección IP es xx.xxx.xxx.xxx
- Tu navegador está utilizando 128 bits de clave secreta SSL
- El servidor está utilizando 1024 bits de clave pública SSL.

La resolución de la pantalla.

El valor del campo "*User-Agent*".

- Mozilla/5.0(Windows NT 6.1 ; rv:16.0) Gecko/20100101 Firefox/16.0

Qué páginas se leen y cuáles no, qué figuras se miran, cuántas páginas se han visitado, cuál fue el sitio recientemente visitado "*Referer*".

El idioma y zona GMT del sistema operativo.

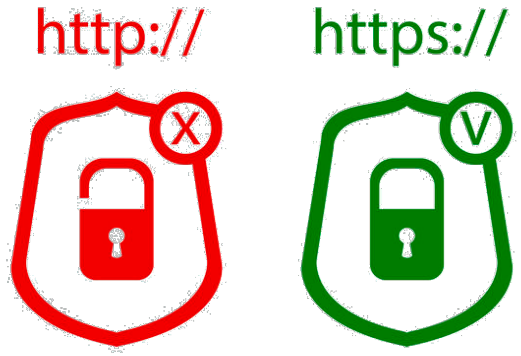
Si se aceptan o no "*cookies*".

Las fuentes cargadas en el sistema o *plugins* instalados y activados.

Fuente: Centro Criptográfico Nacional (CCN)

NAVEGACIÓN SEGURA

Las personas usuarias identificamos la “Navegación segura” con acceder a una página cuyo protocolo es http**S** y lleva el candado por delante.

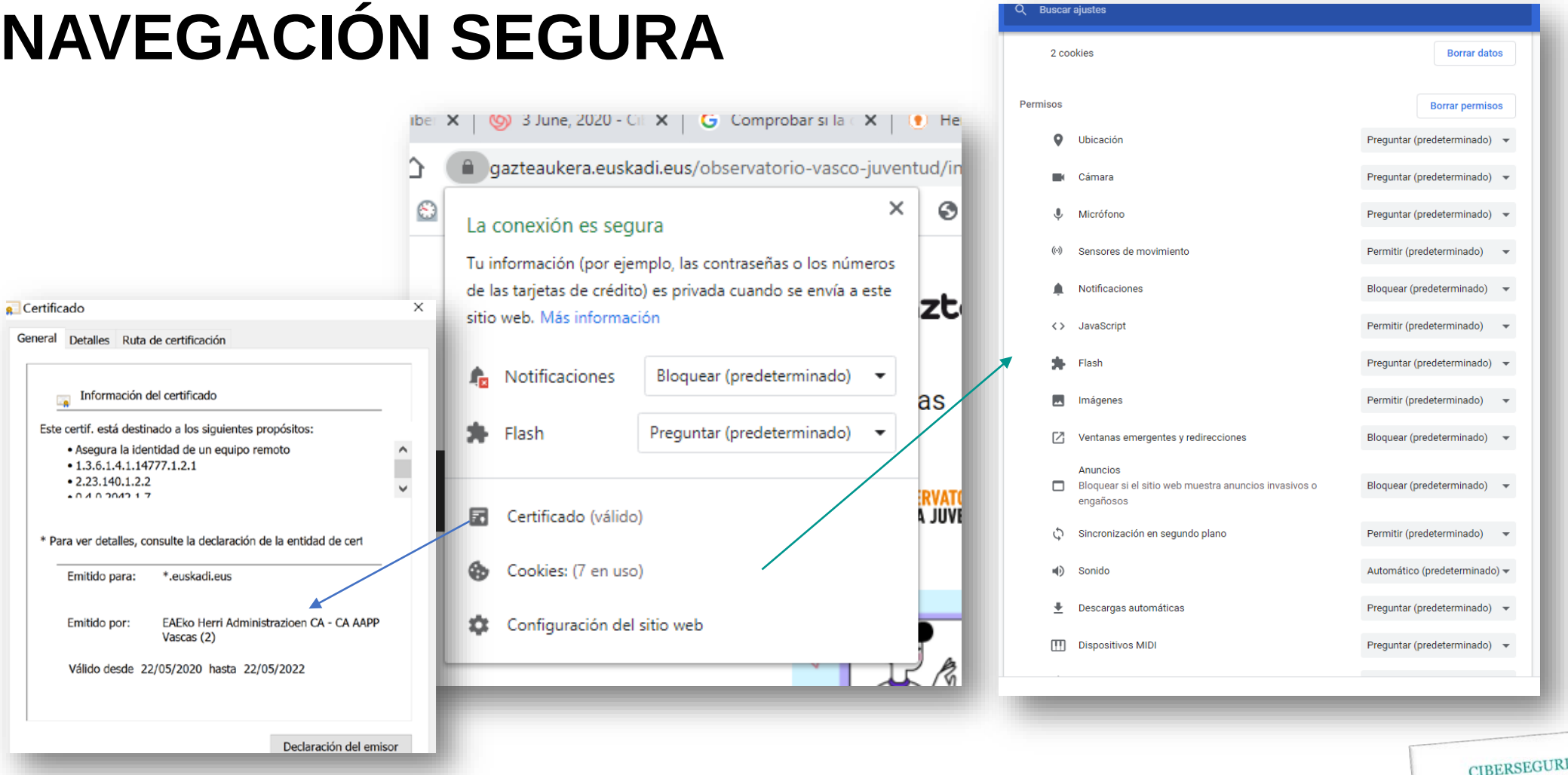


Este candado nos indica que la información viaja encriptada. El “protocolo http” es anterior y permitiría un ataque del tipo “Man-in-The-middle”, desde el que se pueden visualizar los datos que se están movilizando.

Para poder disponer de ese candado es necesario que la página web haya instalado un “Certificado SSL” que nos indica que el sitio es real, auténtico y confiable.

Ahora bien, hay que fijarse bien el certificado ya que ha podido ser emitido por una entidad no reconocida o emitido a un nombre que no coincida con el dominio de la página.

NAVEGACIÓN SEGURA

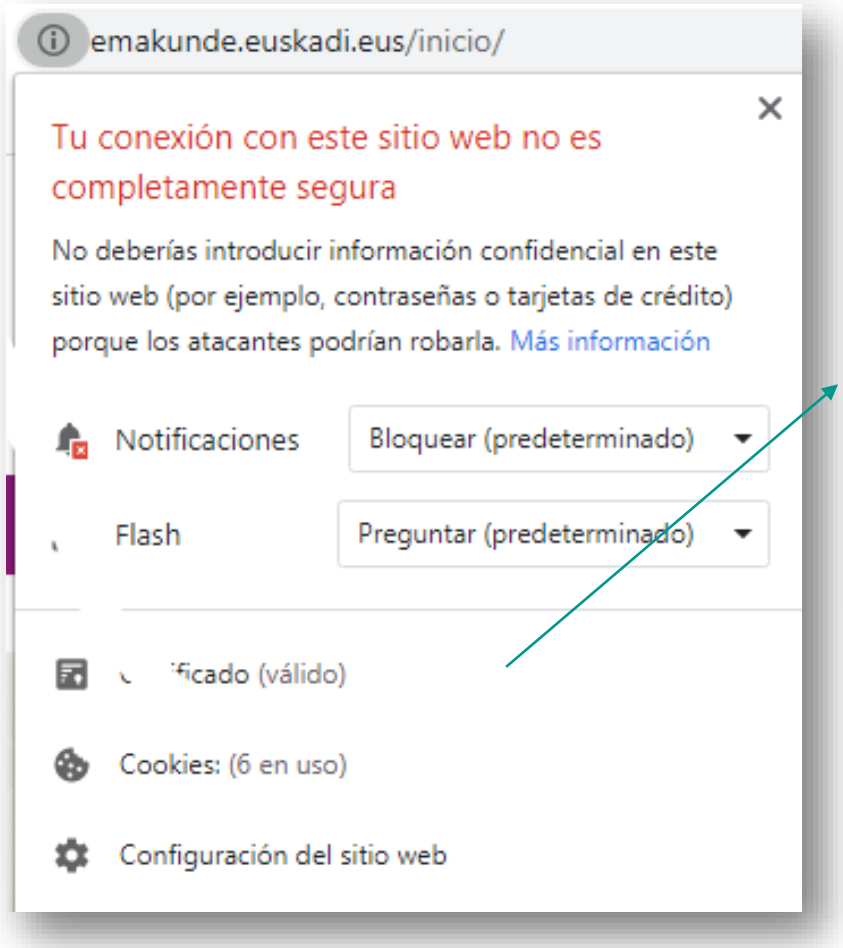


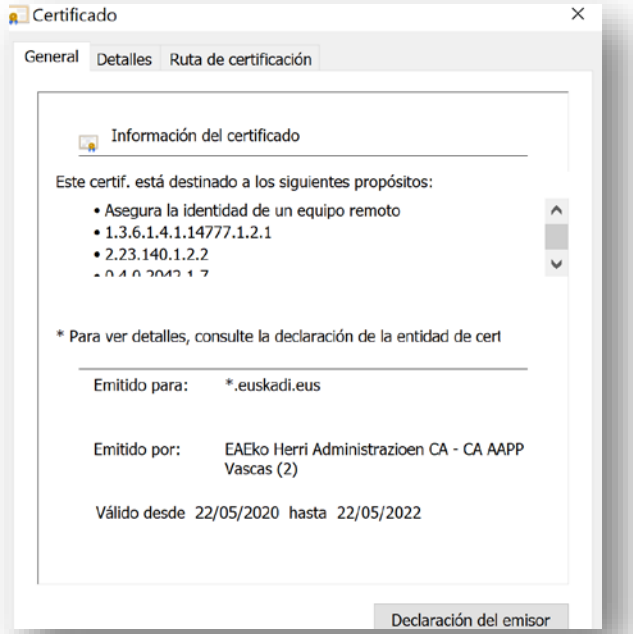
- Puede darse el caso de que nos marque una conexión como segura pero el emisor del certificado no sea de una entidad de confianza (phishing).

NAVEGACIÓN SEGURA

- Es posible que nos marquen una conexión como no segura, a pesar de tener un certificado válido.

- A pesar de que el certificado es válido, el contenido puede provenir de fuentes no originales.





RECOMENDACIONES NAVEGACIÓN SEGURA

1. Acceder únicamente a sitios de confianza.
2. Descargar los navegadores y programas desde los sitios oficiales. Mantenerlo actualizado.
3. Personalizar la configuración por defecto del navegador; nivel de seguridad, permisos para notificaciones, ventanas emergentes, autocompletados,
4. Borrar las ‘cookies’, historial de navegación y archivos temporales SIEMPRE en equipos ajenos y periódicamente en los nuestros.
5. Utilizar un usuario sin permisos de administrador para navegar e impedir la instalación de programas y cambios en los valores del sistema.
6. Utilizar, siempre que podamos sistemas de navegación anónima (desvinculándonos de la IP de origen). Recordando los sitios web que visitemos puedan seguir rastreando nuestra actividad, o nuestro proveedor de servicios.

RECOMENDACIONES NAVEGACIÓN SEGURA

7 Utilizar un **navegador** como **Tor** (The Onion router) para extremar el anonimato.

8 Utilizar un buscador como **DuckDuckGo** en alternativa a Google para garantizar la privacidad de nuestros datos)

9 Para quien quiera extremar la seguridad utilizar un sistema operativo live como **Tails** (basado en una distribución de Debian) que arranca de cero cada vez que se utiliza.

10 Personalizar el acceso y configuración de nuestro router. Podemos utilizar un programa como **FING** que nos puede ayudar a detectar intrusos en nuestra red.

11 Siempre que nuestro router disponga de él implementar la seguridad **WPA2-PSK (AES)**

12 Evitar, en la medida de lo posible, las redes wifi públicas y abiertas son puntos peligrosos y con potenciales amenazas para la seguridad de nuestros datos. Borra los datos de la red tras utilizarla para evitar una conexión automática.

13 Y, en caso de necesidad, utilizar una red virtual privada (VPN), donde los paquetes de información van cifrados. (**ProtonVPN**)

REDES SOCIALES

- Consideraciones a tener en cuenta en Redes Sociales

REDES SOCIALES

Privacidad en Facebook

Ver videotutorial

Privacidad en Twitter

Ver videotutorial

Privacidad en Instagram

Ver videotutorial

Privacidad en Youtube

Ver videotutorial

Privacidad en Whatsapp

Ver videotutorial

Privacidad en Snapchat

Ver videotutorial

- Guía de Privacidad y Seguridad En Internet (OSI)

REDES SOCIALES

1. Personalizar siempre nuestro perfil y la configuración de privacidad de todas la redes sociales.
2. No aceptar todo tipo de solicitudes de amistad. Ni permitir a las redes sociales que accedan a nuestra libreta de direcciones. Hemos de proteger también las direcciones de nuestros contactos.
3. Reflexionar sobre todo lo que publicamos; ahí queda.
4. No utilizar ni permitir apps de terceros dentro de ellas.
5. Ojo a los servicios basados en la localización y la información de nuestros Smartphone.
6. Precaución con los enlaces. Analízalos en caso de duda.
7. Escribir directamente la url en el navegador para evitar que un sitio falso pueda robar nuestra información personal..
8. Utilizar contraseñas robustas y añadir un segundo factor de autenticación (2FA).

SE TRATA DE…

PREVENIR → ANALIZAR → DESINFECTAR

PREVENCIÓN

1. Mantener actualizados firmware, sistema operativo y aplicaciones (sobre todo navegadores y software de seguridad) de nuestros dispositivos.
2. Copias de seguridad periódicas en diferentes almacenamientos no internos. Particionar el disco duro para mantener separado sistema operativo y datos almacenados.
3. Cifrado de carpetas y archivos en nuestros discos duros. Esta acción y la copia de seguridad cobra especial importancia en el Ransomware.
4. Atención especial para identificar posibles mensajes maliciosos, sobre todo phishing, en nuestro correo o apps de mensajería instantánea. No descargar cualquier adjunto no esperado ni abrir sin analizar.
5. Borrar periódicamente el historial y datos de navegación así como los archivos temporales y, si detectas algo extraño…¡desconecta de internet y ANALIZA!

ANÁLISIS

1. En todo dispositivo debemos tener unos programas básicos de seguridad; firewall o cortafuegos que impida conexiones no permitidas, antivirus actualizado para realizar diferentes tipos de análisis y un antimalware.
2. Si tenemos sospecha de algún tipo de ataque, realizar análisis online con alguna herramienta diferente a la que tenemos instalada (una segunda opinión…)
3. En caso de tener duda con algún enlace, analizar la URL para ver su legitimidad (VIRUSTOTAL, METADEFENDER)

DESINFECCIÓN

Si los análisis nos reportan infección por algún tipo de código malicioso proceder a su desinfección o puesta en cuarentena de los datos afectados.

Si, por el contrario, hemos sufrido algún tipo de ciberataque en el que nuestros datos personales, nuestra identidad digital o nuestros dispositivos se han visto afectados ponernos en contacto con:

En Euskadi

Resto de España

CIBERSEGURIDAD
o el reto de asumir la responsabilidad de nuestras acciones

Ane Martínez Recio

ezberdin
ACOMPAÑAMIENTO EN ENTORNOS DIGITALES