



Financiado por
la Unión Europea
NextGenerationEU



Plan de
Recuperación,
Transformación
y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD



ACTIVIDADES DEL MÓDULO ATAQUE



F-74 "Asturias" v1.2 (2025). Campus Tecnológico - Deportivo

© José Manuel Redondo López. Universidad de Oviedo



Contenido

	Ejercicios de Ataque	5
	Aspectos Relativos a las Personas	5
	Autenticación	5
	Ejercicio HAVEIBEEN. Consultar si te han robado la clave de algún servicio con Have I Been Pwnd?	5
	Computación "sensata"	7
	Ejercicio BULOS: Buscar una noticia patrocinada y compararla con una "normal"	7
	Ejercicio COACHES: Escucha opiniones de cierto tipo de "coaches de desarrollo personal"	7
	Uso de Internet	9
	Usando el navegador de forma segura	9
	Ejercicio NOTIFICACIONES. Buscar una web con notificaciones engañosas	9
	Ejercicio ANUNCIOSGOOGLE: Hacer una búsqueda en Google de un programa que muestre un anuncio potencialmente peligroso	11
	Uso de Redes Sociales	15
	Ejercicio ROBOCUENTAS: Leer acerca de los tipos de bots en redes sociales	15
	Ejercicio COLABORACIONES: Leer acerca de estafas de falsas colaboraciones en redes sociales	16
	Uso de Sistemas de Mensajería	17
	Email	17
	Ejercicio MAILSFALSOS: Analizar mails fraudulentos de ejemplo	17
	Ejercicio MAILFALSOSSPEAR: Analizar mails fraudulentos dirigidos de ejemplo	20
	Aplicaciones de Mensajería	23
	Ejercicio MENSAJESFALSOS: Analizar unos mensajes fraudulentos de ejemplo	23
	Ejercicio ROBOSCUENTAS: Investigar métodos de robo de cuentas documentados	26
	Dispositivos de Computación	28
	Telefonía Móvil	28
	Ejercicio PLAYSTORE: Mirar alguna aplicación con mala pinta en la Play Store	28
	Ejercicio APPSMALICIOSAS: Mira noticias de streamers / periódicos etc. que han recomendado aplicaciones maliciosas	30
	Ordenadores	32
	Ejercicio DESCARGAAPP: Consultar un procedimiento para descargar aplicaciones de forma más segura...	32
	Ejercicio PUP: Consultar casos donde ha habido descarga de PUPs con otro producto	34
	Hardware y Redes	36



■ Redes de Comunicaciones	36
✖ Ejercicio ROBLOX: Leer sobre los problemas que hay en juegos sociales cuando se mete “gentuza”	36
✖ Ejercicio ASISTENCIA: Investigar lo que hace un programa de asistencia remota.....	37
■ Dispositivos “Smart”	38
✖ Ejercicio CVEs: Mirar vulnerabilidades de programas conocidos	38
✖ Ejercicio SHODAN: Buscar una IP en Shodan y ver qué pasa	40
🏃 Seguridad “En el Mundo Real”.....	42
⌚ Seguridad “Física”.....	42
✖ Ejercicio QR: Escanear un QR con tu teléfono	42
✖ Ejercicio HACKUSB: Leer sobre USBs para “hacking”	43
💰 Seguridad Financiera.....	45
✖ Ejercicio ESTAFAS: Leer sobre estafas de segunda mano	45

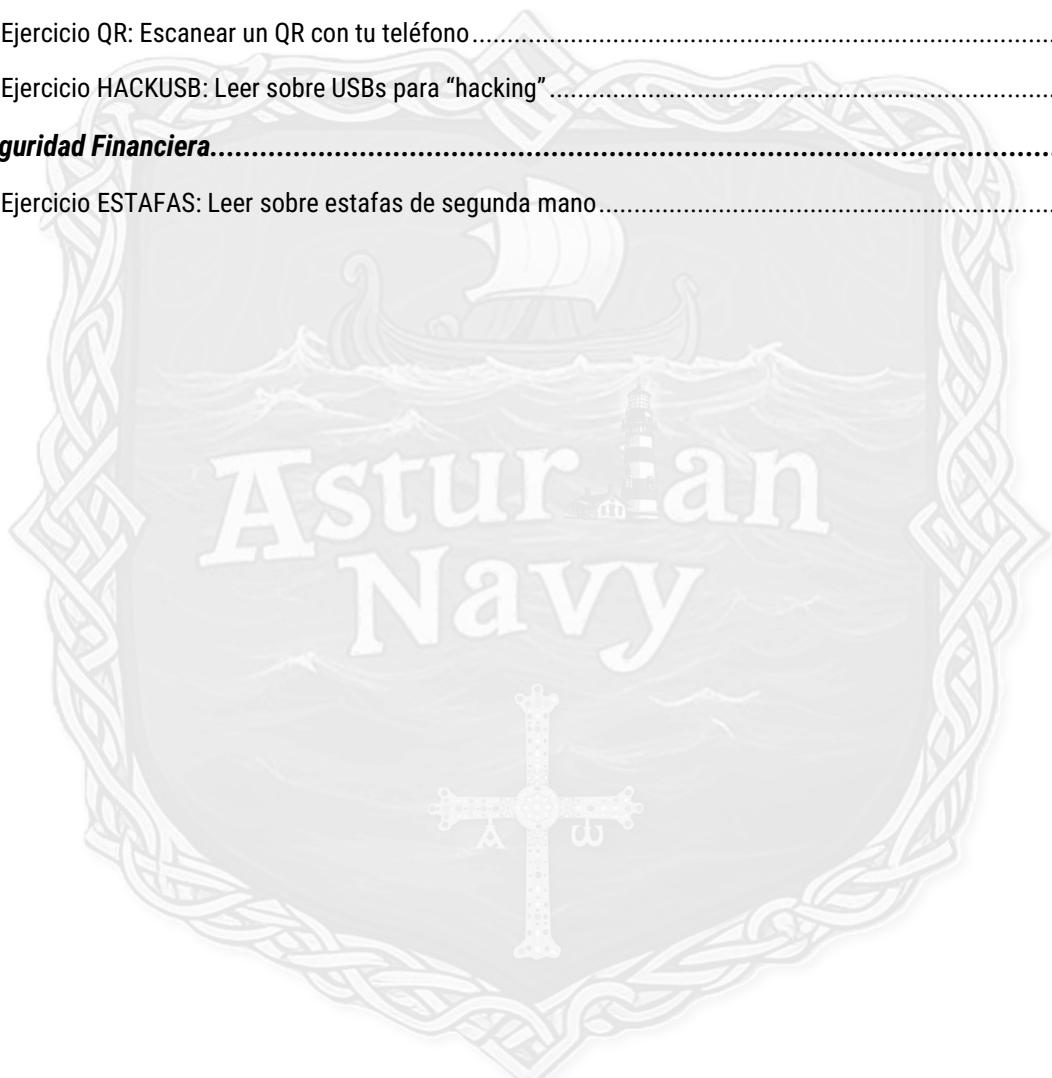




Tabla de Ilustraciones

Figura 1. Vaya movida...¡cambia la clave ya!	6
Figura 2. ¿Mostrar notificaciones? No, gracias. Bloquear y a pastar	9
Figura 3. Falsísimo. En serio. Y como estas (ventajas que te alarman con alguna movida chunga para que cliques) muchas más. Todas falsas también	10
Figura 4. Enlace patrocinado de Google, mal rollo asegurado. ¡No los cliques!	12
Figura 5. Toshiba, WD, son discos reales. Pero ¿UnionShine? ¿Sin marca? Malamente (tra, tra)	12
Figura 6. Un disco SSD (los más rápidos que hay) con ese tamaño (que difícilmente se fabrican en masa hoy día) y a ese precio. ¡Grita timo!.....	13
Figura 7. ¿Sin marca o marca rara impronunciable? Mira las valoraciones, y verás una lista de timados casi con un 100% de seguridad.....	13
Figura 8. ¿Te ha pasado algo de esto? Actúa. YA. Fuente: https://www.incibe.es/sites/default/files/images/concienciacion/imagen-indicadores-robo-cuenta.jpg .	15
Figura 9. Este esquema es más concreto que el que te di en teoría y por tanto lo puedes aplicar más rápido. Acierta en un enorme nº de casos	18
Figura 10. Esa copia exacta de un mail de Vinterd con un botón peligroso.....	19
Figura 11. ¡Oh no, me caduca la clave y no quiero recordar otra! Voy a darle a este botón de un email que no tiene nada que ver con Office para que...me la roben :)	19
Figura 12. Vaya, ¡soy rico! Voy a tener que irme a Andorra para no pagar impuestos	20
Figura 13. Te investiga, te contacta, te engaña y...la has liado. Fuente: https://us.norton.com/blog/online-scams/spear-phishing	21
Figura 14. Un resumen de lo que es un fraude del CEO, un timo de spear phishing peligrosísimos	22
Figura 15. Como le hagas caso te quedas sin cuenta. El delincuente finge ser tú, pero no sabe tu clave así que usa "Recordar contraseña". Eso genera un enlace que te llega a ti, y si le pasas lo que sale al pulsar el enlace, entonces podrá completar la jugada, suplantarte completamente y hasta luego cuenta.....	24
Figura 16. Mismo truco, diferente programa (se repite en todos prácticamente)	24
Figura 17. Pide dinero suplantando un familiar. Lo mejor es que si te pasa esto llames tu a ese familiar para confirmar. ¡Te sorprenderías la de gente que descubre que no era él realmente!	25
Figura 18. El mismo truco, pero ya con los datos de la transferencia. Es un timo muy común	25
Figura 19. Aunque sea tu jefe, padre, profesor... el procedimiento es sencillo: Te pide algo raro, llámale tú al nº de siempre y confirma que es cierto	26
Figura 20. Esto es una trampa clásica. ¡No caigas!	27
Figura 21. Menudo panorama tenemos en las tiendas de aplicaciones con los dichosos iconos parecidos para jugar al despiste e instalarte lo que no quieres :(.....	29
Figura 22. ¿Todo eso para cambiar el ícono de una aplicación? Venga ya, por favor.....	30



Figura 23. Todo esto suena muy bonito para tu bolsillo en primera instancia, hasta que de repente te descargas algo y lleva sorpresa no muy agradable :(.....	33
Figura 24. Hasta no hace tanto tiempo, estas casillas venían marcadas por defecto. Alguien debió darles el toque (probablemente la ley europea anti-prácticas de monopolio)	35
Figura 25. ¿Ahora sí que te sientes hacker eh? :).....	39
Figura 26. Curiosamente, dar esta información es completamente innecesario: La página funciona igual aunque no la des. Créeme. Pero aquí está, "cantándolo todo"	39
Figura 27. Si, esta máquina "cantaba" todas sus vulnerabilidades con Shodan. No te preocunes, ya no está en servicio :P	40
Figura 28. Si te pones creativo/a y le dedicas tiempo, este motor puede ser una auténtica mina	41
Figura 29. Si el INCIBE se ha molestado en crear una infografía tan detallada es por algo, créeme.....	43





Ejercicios de Ataque

NOTA: Si no lo has hecho ya, te recomiendo que leas la sección "Unas palabras antes de empezar" del bloque de "Defensa" para entender mejor el material que te entrego

Aspectos Relativos a las Personas

Autenticación

Ejercicio HAVEIBEEN. Consultar si te han robado la clave de algún servicio con Have I Been Pwnd?

Descripción de la actividad

Necesitas saber si la clave de cualquiera de tus cuentas **ha sido potencialmente filtrada** en alguno de las muchas filtraciones de datos que ocurren hoy día.

Resultados Esperados

Esta actividad se completará cuando inspecciones cualquier cuenta de correo electrónico que quieras saber si es parte de una fuga de datos conocida. Puedes además pensar en posibles usos de esta herramienta que atenten contra la privacidad. Por ejemplo, *¿Qué crees que podría pasar si pones el email de alguien que conoces y sale que se ha filtrado en sitios como Tinder?*

Otra información necesaria para su realización

Have I been pwnd? (<https://haveibeenpwned.com/>) es un sitio web que **almacena y permite consultar fugas de datos de usuarios**. Acepta correos electrónicos, e indica si ese correo se ha filtrado en alguna de las bases de datos de usuarios robadas conocidas. Por tanto, si la cuenta de correo electrónico consultada está dentro de una de ellas, te indicará el sitio cuyos usuarios han sido robados, cuándo y otros detalles sobre la fuga de datos asociada.

Debido a la probabilidad de usar la misma contraseña y correo electrónico en varios sitios, es muy importante verificar esto para evitar que un robo en un sitio facilite también intrusiones en otros sitios.

Si quieres "cacharrear" un poco más, que sepas que también **tiene un servicio que te avisa** si alguna cuenta de correo aparece como comprometida en el futuro. También que sepas que muchos navegadores (como *Google Chrome*) empiezan a ofrecer los mismos servicios en las cuentas que eliges recordar dentro del navegador.



The screenshot shows the homepage of the Have I Been Pwned? website. The main heading is '';--have i been pwned?'. Below it is a sub-heading 'Check if you have an account that has been compromised in a data breach'. A search bar contains the text '.com' and a button labeled 'pwned?'. A red banner at the top says 'Oh no — pwned!' and 'Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)'. Below the banner, there are sections for 'Breaches you were pwned in' (listing Dropbox and Last.fm), and summary statistics: 233 pwned websites, 4,729,225,727 pwned accounts, 54,390 pastes, and 51,474,803 paste accounts.

Figura 1. Vaya movida...¡cambia la clave ya!

🔍 ¿Sabes que tengo un monográfico sobre el tema? Mira: <https://github.com/jose-r-lopez/Fraudes-y-Timos/blob/main/Case%20Files/T1E12.%20Y%20si%20ya%20te%20han%20robado%20la%20clave%20y%20no%20lo%20sabes.pdf?raw=true>

Si todo esto de los ataques a contraseñas y los distintos tipos de ataque que hay es algo que te llama la atención, el INCIBE te lo explica aquí: <https://www.incibe.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf>



Computación “sensata”

Ejercicio BULOS: Buscar una noticia patrocinada y compararla con una “normal”

Descripción de la actividad

Consiste en que busques y analices el contenido de una noticia o contenido que esté **patrocinado** para que te des cuenta de si realmente es una noticia al uso o un anuncio publicitario vestido de noticia

Resultados Esperados

Puedes contestar a estas preguntas:

- *¿Sabías que las empresas pueden pagar por aparecer en los periódicos como si fuesen noticias?*
- *¿Entiendes por qué no tienes que creerte los contenidos que aparecen como patrocinados?*

Otra información necesaria para su realización

Es bastante fácil encontrar contenidos patrocinados en muchos periódicos de tirada nacional y que los analices para darte cuenta de que realmente **están vendiendo una empresa, una idea o algo similar**. Que parezca una noticia no es más que un truco para que resulte más creíble y venderle la idea al lector. Puedes también buscar un enlace como el que aparece en la teoría donde se ven claramente los precios de contratar este tipo de servicios (o este otro: <https://www.eldiario.es/edcreativo/que-es-ed-creativo/>)el.

Piensa que esto no es realmente tan raro, estás acostumbrado a verlo en los videos de muchos streamers, ¿no? Pues aquí también

Si no tienes a mano una de esas noticias puedes usar esta: <https://www.elmundo.es/uestudio/2024/06/17/66703263e85ece234e8b45ac.html>. Fíjate en el “Ofrecido por” *¿Quién es la empresa y por qué pone esta noticia?*

Ejercicio COACHES: Escucha opiniones de cierto tipo de “coaches de desarrollo personal”

Descripción de la actividad

Consiste en qué escuches vídeos que analizan el mensaje de ciertos **coaches de desarrollo personal** que son tan populares hoy en día para que tengas un criterio por el cual puedas analizar sus mensajes con una perspectiva un poco más amplia

Resultados Esperados

Puedes contestar a estas preguntas:

- *¿Has entendido que hay coaches de desarrollo personal que realmente buscan que mejores, y otros que realmente buscan mejorar su propia cartera?*



- ¿Entiendes que cualquier programa negocio o similar que se base en buscar afiliados es en sí un negocio ruinoso para los nuevos suscriptores de la afiliación porque no deja de ser un esquema piramidal encubierto?

Otra información necesaria para su realización

Por mucho que yo te diga nadie mejor que un experto te puede explicar en qué consisten estos coaches de desarrollo personal y cómo distinguir los que verdaderamente te pueden ayudar de los que no. Por eso te recomiendo estos vídeos para que los veas y con eso te hagas tu propia opinión acerca de lo que venden y de cómo lo venden.

- <https://www.youtube.com/watch?v=Y9yEoOKMAhE&t=2s>
- <https://www.youtube.com/watch?v=leele31Bg44>
- <https://www.youtube.com/watch?v=wdlzKXtkSVM&t=213s>

Si quieras seguir a **streamers** que trata estos temas u otros interesantes similares, te recomiendo:

- <https://www.youtube.com/c/LagatadeSchr%C3%B6dinger>
- <https://www.youtube.com/@LordDraugr>
- <https://www.youtube.com/@TamayoStuff>





Uso de Internet



Usando el navegador de forma segura



Ejercicio NOTIFICACIONES. Buscar una web con notificaciones engañosas



Descripción de la actividad

Consiste en localizar noticias o artículos de **estafas** que han tenido lugar a través de una falsa ventana emergente



Resultados Esperados

Puedes desarrollar una **concienciación acerca de la peligrosidad de las ventanas emergentes** viendo ejemplos reales de momentos en los que se han usado para hacer algún tipo de estafa



Otra información necesaria para su realización

Las ventanas emergentes son una parte de las webs que, si bien las webs legítimas cada vez las usan menos, **son muy frecuentes en webs poco recomendables**. Muchos navegadores están preparados para bloquearlas automáticamente, pero es cierto que cada vez hay formas de presentar cosas que parecen ventanas emergentes de manera que el navegador no pueda impedir su uso. Por eso es importante que, cuando el navegador no es capaz de parar una ventana emergente, seamos capaces de parar un posible ataque nosotros con nuestra propia concienciación.

Lo primero que debemos hacer es siempre contestar que no cuando nos salgan avisos como los de la imagen (<https://www.infobae.com/america/tecnologia/2022/08/21/el-truco-para-desaparecer-las-ventanas-emergentes-de-google-chrome/>)

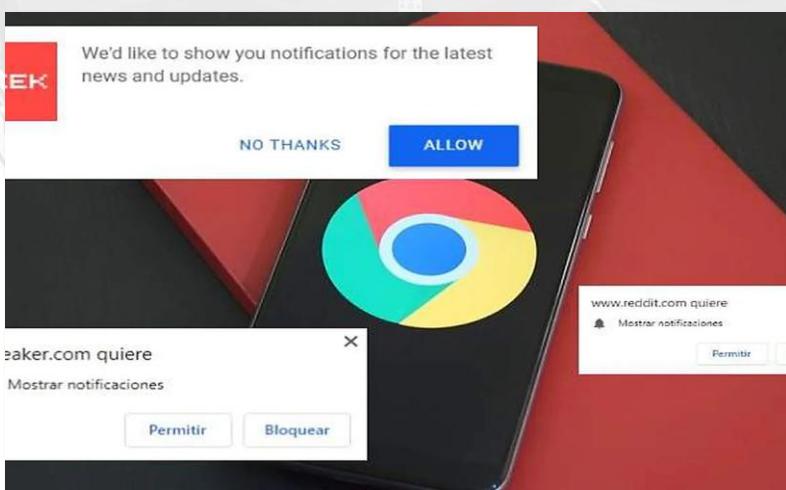


Figura 2. ¿Mostrar notificaciones? No, gracias. Bloquear y a pastar

Si el navegador muestra una a pesar de haberlas prohibido, es porque la página usa algún truco (probablemente de dudosa ética) para saltarse estas limitaciones. Entonces tendremos que usar nuestro propio sentido común para identificar ventanas emergentes falsas: <https://www.kaspersky.es/resource-center/threats/identify-and-remove-fake-pop-ups>. Ante la más mínima duda (o bien siempre 😊), no hagas caso a la ventana emergente.



- **Tiene errores ortográficos** y/o imágenes poco profesionales
- **Compara la ventana emergente** con una notificación legítima que conozcas por qué has visto algo similar en una página fiable. Las ventanas emergentes falsas suelen decir que vienen de una empresa conocida (antivirus, etc.). Es importante poder diferenciar las notificaciones legítimas de las ventanas emergentes falsas buscando imágenes de alguna legítima. No obstante, no tomes esto como algo definitivo, porque hay falsificaciones realmente buenas.
- **Intenta cerrar el navegador:** Las ventanas emergentes falsas pueden hacer que el navegador cambie al modo de pantalla completa. Si el navegador está en modo de pantalla completa y ves una ventana emergente sospechosa, intenta minimizar o cerrar el navegador. Si no puedes hacerlo, es probable que la ventana emergente que estás viendo sea una estafa.

Ten cuidado al intentar cerrar o minimizar la ventana emergente: los botones **que muestra normalmente no son reales**. Solo son imágenes de botones reales y, al hacer clic en ellos, estarás interactuando con la ventana emergente.

- **Verifica el número de teléfono:** La mayoría de las ventanas emergentes falsas dan un número de teléfono e indican que llames al mismo para resolver algo. Puedes **buscar ese nº de teléfono** para saber si es o no una estafa, porque es normal que otros afectados lo denuncien o pongan capturas de la misma ventana. Quizá también te encuentres que pertenece a una empresa real, en cuyo caso quizás hayas encontrado uno de los casos raros donde la ventana emergente no es una estafa...Pero normalmente lo es, así que mejor ignóralos y **no llames nunca si te lo piden**.
- **Una empresa de antivirus real nunca te va a pedir que la llames.** No importa lo que diga la ventana.

Más información:

- <https://www.mundopc.es/peligros-y-soluciones-para-las-ventanas-emergentes-de-publicidad-277.html#>
- <https://www.pcrisk.es/guias-de-desinfeccion/12207-error-code-0x80073b01-pop-up-scam>

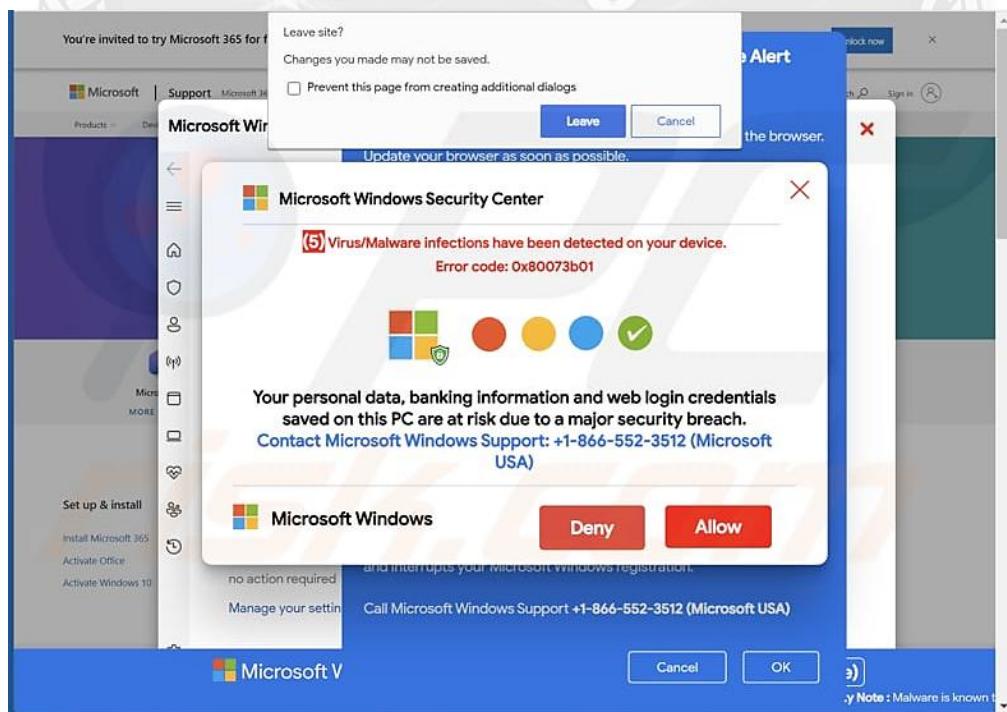


Figura 3. Falsísimo. En serio. Y como estas (ventajas que te alarman con alguna movida chunga para que cliques) muchas más. Todas falsas también



💡 ¿Sabes que tengo un monográfico sobre el tema? Lo tienes aquí: <https://github.com/jose-lopez/Fraudes-y-Timos/blob/main/Case%20Files/T1E32.%20Notificaciones%20web.pdf?raw=true>

🛠 Ejercicio ANUNCIOSGOOGLE: Hacer una búsqueda en Google de un programa que muestre un anuncio potencialmente peligroso

👤 Descripción de la actividad

Consiste en **entender el peligro que tiene en los enlaces patrocinados** en los motores de búsqueda u otros sitios

🎖 Resultados Esperados

Eres capaz de identificar enlaces patrocinados, y entender muy bien **lo que significan y por qué no debes fiarte de ellos.**

📋 Otra información necesaria para su realización

Un enlace patrocinado **no es más que un anuncio**. Lo que pasa es que, en lugar de ponerse en un trozo de una página web que tenga un hueco de contratar anuncios, aquí **se paga para aparecer el primero en una búsqueda** que se haga en *Google* (o en otro buscador) que admita este tipo de publicidad. Cuando una empresa paga la cantidad que le pide el buscador para aparecer el primero cuando se hagan determinadas búsquedas, tú verás un enlace como primer resultado de una búsqueda que hagas. La empresa anunciente sabe que mucha gente no se fija exactamente en lo que está haciendo clic, y que confía en la efectividad del buscador para saber que lo primero que encuentra es lo que está buscando.

No obstante los buscadores están obligados a informar de que un enlace está patrocinado, aunque hay bastante gente que no sabe lo que significa eso. Vuelvo a repetirlo: **es un anuncio y alguien ha pagado por aparecer el primero**. Ese anuncio puede ser **real**, y realmente ser un enlace a lo que tú buscas (la empresa que crea el programa que buscas ha hecho un anuncio legítimo del mismo), o puede ser **falso**, y ser un enlace a otra página que simula ser lo que buscas o es otra cosa completamente distinta y usa esa búsqueda como forma de dirigir clientes a ella, bien con objetivos legítimos o bien como engaño.

Como ya han existido **problemas debido a enlaces patrocinados que llevan a páginas falsas**, este ejercicio pretende que entiendas los problemas que supone que haya enlaces de ese tipo, para que no caigas víctima de un timo derivado de los mismos. Fíjate por ejemplo qué ocurre si buscamos camisetas de futbol en *Google*. Los primeros tres enlaces son patrocinados: 3 tiendas de camisetas han pagado lo que *Google* les pide para aparecer las primeras antes esa búsqueda. Esto hará que muy probablemente tengan muchas más visitas pero **¿son realmente tiendas legítimas o son un fraude?** *Google* no lo sabe, salvo que alguien le informe, y nosotros tampoco....

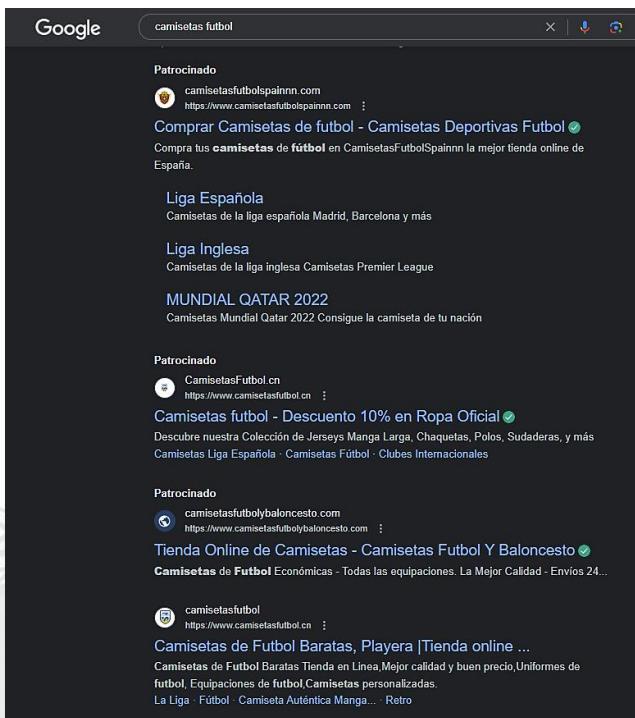


Figura 4. Enlace patrocinado de Google, mal rollo asegurado. ¡No los cliques!

No creas que esto solo ocurre con tiendas de nombre desconocido, sino que también ocurre **dentro de tiendas grandes de nombre muy conocido**. ¿Sabías que en 2023, durante unos meses, cuando intentabas comprar un disco duro en Amazon los enlaces patrocinados que salían en la búsqueda (que son anuncios pagados, pero a Amazon, para aparecer los primeros en ciertas búsquedas) eran a discos duros fraudulentos? **¡Error! Referencia de hipervínculo no válida.** . Amazon tardó bastante en eliminar estos productos fraudulentos de su web, y no porque no quisiera hacerlo, sino porque cada vez que lo hacían aparecían más. Quienes estaban detrás tenían una red muy compleja de tiendas fraudulentas y productos falsos. En general, si algo tiene un precio demasiado bueno para ser cierto, **¡lo es!** 😊

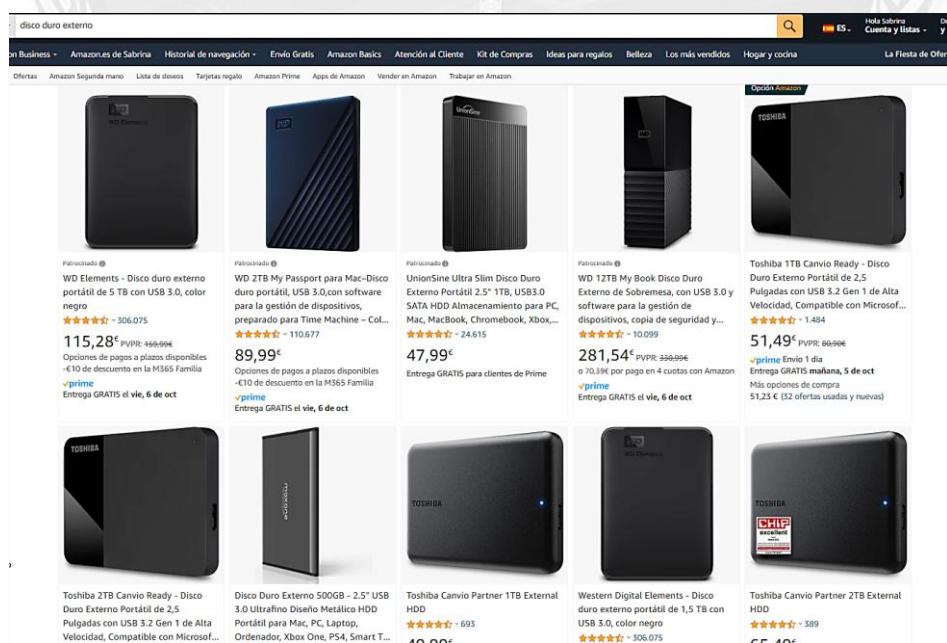


Figura 5. Toshiba, WD, son discos reales. Pero ¿UnionShine? ¿Sin marca? Malamente (tra, tra)

Los discos duros SSD de estos tamaños no tienen, ni por asomo, esos precios.

José Manuel Redondo López. Proyecto "F-74 'Asturias"



Tipo C y USB 2.0 OTG Flash Drive 64 GB 2 en 1 USB Pendrive Memory Stick para Smartphones Android, Windows, Android, PC, Tablets, Almacenamiento DE Datos Externos Etc (Verde)

12TB, 14TB, 16TB, 20TB DISMO Externo HDD, Disco Duro portátil Portable de Alta Velocidad 3.1, HDD Externo a Prueba de descargas para Mac, PC 20TB

57,99 €

Precio final del producto
Financia tus compras en 4 cuotas en 90 días con Cofidis a partir de 75€. Ver detalles
Capacidad: **20TB**

12TB	47,99 €
14TB	50,99 €
16TB	54,99 €
20TB	57,99 €

Detalles del producto

Tecnología de conectividad	USB
Marca	Heru
Dispositivos compatibles	Portátil, Ordenador de sobremesa
Material	Peltre
Tipo de paquete	Cartón

• [Experiencia eficiente] Pequeño rendimiento y gran volumen, transferencia de alta velocidad; La tecnología de algoritmo de desgaste de disco completo, mejorando significativamente la vida útil del SSD, mayor eficiencia. Lee y escribe, y hace que su

57,99 €

Entrega GRATIS entre el 30 de septiembre - 24 de octubre. Ver detalles

Enviar a Luis

En stock.

Cantidad: 1

Añadir a la cesta Comprar ahora

Transacción segura

Envío desde ZJZJUK Vendido por ZJZJUK

Política de devoluciones: Se puede devolver en un plazo de 30 días a partir de la fecha de recepción

Añadir a la Lista de deseos

Figura 6. Un disco SSD (los más rápidos que hay) con ese tamaño (que difícilmente se fabrican en masa hoy día) y a ese precio. ¡Grita timo!

Comprar estos dispositivos **no solo es un fraude económico**, sino que puede ser **dañino**. Por ejemplo, se sabe que estos dispositivos realmente tenían dentro una tarjeta SD de pocos Gb y tenían su circuitería alterada para informar de su capacidad de manera errónea (*Windows* los reconocía con la capacidad que se supone que tenían, pero era falsa). En consecuencia, no solo eran mucho más lentos de lo que anuncian, sino que al pasar de la capacidad real que tenían, los nuevos datos **destruirían los antiguos**. En definitiva, si se usasen para hacer copias de seguridad, estas serían inservibles 😞. <https://www.youtube.com/watch?v=NOphCCpTN2E>. Siendo además dispositivos alterados fraudulentamente, perfectamente podrían contener **incluso un malware de fábrica**.

Disco Duro Externo de 2 TB - Ultrafino 2,5" USB 3.1 metálico SSD portátil para Mac, PC,

39,99 €

Opinión Amazon destaca productos con una alta puntuación y un buen precio disponibles para su envío inmediato.

Opción Amazon de "disco duro externo"

39,99 € Prime Devoluciones GRATIS ~ Precio final del producto Color: Negro-SSD

39,99 €	59,95 € (6,00 € / unidad)
---------	---------------------------

Marca Sanford Color Negro-SSD Velocidad de transferencia de datos 1 Gigabit por segundo

Acerca de este producto

- Diseñado para funcionar con ordenadores Windows o Mac, este disco externo es ideal para realizar copias de seguridad en un abrir y cerrar de ojos, por arrastrar y soltar.
- Tecnología innovadora: el disco duro externo SSD está hecho principalmente de material metálico de alta calidad, con una textura metálica mate, moderna y duradera, con una vida útil prolongada. Diseño interno uso innovador de pegatinas de aluminio para envolver el disco duro para aislar las interferencias

Entrega Recogida

39,99 € Prime Devoluciones GRATIS ~ Entrega GRATIS el lunes, 6 de febrero. Ver detalles

Enviar a Ramon - Ciudad Real 13001

En stock.

Cantidad: 1

Añadir a la cesta Comprar ahora

Transacción segura

Envío desde Amazon Vendido por FDVHJ

Política de devoluciones: Se puede devolver en un plazo de 30 días a partir de la fecha de recepción

Protección adicional? Comprueba si este seguro cubre tus necesidades:

2 años Seguro daño accidental por 1,49 €

Figura 7. ¿Sin marca o marca rara impronunciable? Mira las valoraciones, y verás una lista de timados casi con un 100% de seguridad

💡 ¿Sabes que tengo un monográfico sobre el tema? Lo tienes aquí: <https://github.com/jose-lopez/Fraudes-y->



[Timos/blob/main/Case%20Files/T1E18.%20Buscadores%20que%20nos%20enga%C3%B1an.pdf?raw=true](https://timos.blob.main/Case%20Files/T1E18.%20Buscadores%20que%20nos%20enga%C3%B1an.pdf?raw=true) y
aquí: <https://github.com/jose-r-lopez/Fraudes-y-Falsedades-en-la-Inteligencia-Artificial>





Uso de Redes Sociales

Ejercicio ROBOCUENTAS: Leer acerca de los tipos de bots en redes sociales

Descripción de la actividad

Las cuentas en aplicaciones de mensajería no son una excepción a las que ya hemos visto y, aparte de la password segura, **también debemos activar el 2FA**.

Resultados Esperados

Además, eres capaz de identificar timos destinados a robarte tus cuentas (que es la razón por la cual haces lo primero).

Otra información necesaria para su realización

En esta actividad quiero que entiendas que en las redes **sociales hay una problemática relacionada con el robo de cuentas especial** que consiste en un timo de los que mucha gente ha sido víctima. Por suerte, el INCIBE tiene cubierto todo este tema aquí (apartado "Robo de cuenta"): <https://www.incibe.es/ciudadania/tematicas/virus-amenazas>

Indicadores de que te han robado la cuenta

¿Mensajes leídos? ¿Publicaciones no realizadas por ti? ¿Contactos desconocidos? ¿Cambios en los datos de recuperación de la cuenta? ¿No funcionan tus contraseñas de acceso?

Si te sientes identificado, sigue estos consejos:

- Recupera el control de la cuenta a través de los procedimientos que ofrece el servicio afectado.
- Revisa que los datos de recuperación de la cuenta son los correctos.
- Cambia la contraseña de acceso que estabas usando y también la de todos los servicios online en los que utilizas la misma.
- Avisa a tus contactos y conocidos de la situación.
- Activa la doble verificación.
- Si no has conseguido recuperar el acceso, denuncia ante las FCSE aportando las evidencias.

#OSIconsejo
incibe.es/ciudadania

Figura 8. ¿Te ha pasado algo de esto? Actúa. YA. Fuente:
<https://www.incibe.es/sites/default/files/images/concienciacion/imagen-indicadores-robo-cuenta.jpg>



Si tienes un dos 2FA en la red social, este tipo de timos es mucho más difícil de hacer, puesto que el atacante tendría que pedirte el código que te sale para poder entrar y eso ya es tremadamente sospechoso. Por tanto es una razón más para activarlo, pero esto lo veremos en el **módulo de defensa**.

💡 ¿Quieres saber más sobre el tema? Lee esto: <https://www.incibe.es/ciudadania/tematicas/virus-amenazas/robo-de-cuentas> y esto: <https://www.incibe.es/empresas/blog/suplantacion-y-robo-identidad-las-redes-sociales-riesgo-las-empresas>

🛠 Ejercicio COLABORACIONES: Leer acerca de estafas de falsas colaboraciones en redes sociales

👤 Descripción de la actividad

Consiste en que entiendas que el hecho de tener una red social puede hacerte una víctima de un timo en el que **te ofrecen dinero por promocionar algún tipo de producto** usando el alcance de tus contactos, pero que realmente acabas o pagando tu dinero o perdiendo la cuenta

🏆 Resultados Esperados

Puedes contestar a estas preguntas:

- *¿Entiendes que el hecho de tener una cuenta en una red social te hace objetivo de muchos timos y que si tienes bastantes seguidores es muy probable que te toque 1 de estos?*
- *¿Eres consciente de que este tipo tiene muchas variantes y por tanto es mejor informarse de ellas para estar preparado por si te toca?*

📋 Otra información necesaria para su realización

Este es uno de los casos en los que por mucho que yo te explique, teniendo en cuenta todas las variantes que hay, seguramente sea más efectivo que leas acerca de timos de este tipo que han tenido éxito para que sepas un poco el modus operandi de los delincuentes. Por eso te recomiendo que leas estas noticias:

- <https://maldita.es/timo/20221130/influencers-suplantacion-timos-falsos-concursos/>
- <https://maldita.es/timo/20230421/timos-y-enganos-mundo-influencer-como-detectarlos-y-como-actuar/>
- <https://www.20minutos.es/tecnologia/fraude-influencers-claves-detectar-cuentas-falsas-4858061/>



Uso de Sistemas de Mensajería

Email

Ejercicio MAILSFALSOS: Analizar mails fraudulentos de ejemplo

Descripción de la actividad

Consiste en poner en práctica **normas básicas de análisis de correos fraudulentos** sobre algún correo que hayas recibido, especialmente si se ha clasificado como *spam*, para ver si, de acuerdo con los criterios que te he dado en teoría, encaja como tal

Resultados Esperados

Puedes contestar estas preguntas:

- *¿Algunos de los emails detectados era obviamente spam?*
- *¿Has recibido alguno que sea una falsificación especialmente buena?*
- *Si es así, ¿entiendes por qué los criterios que te he dado son tan estrictos?*

Otra información necesaria para su realización

La calidad de las falsificaciones que nos llegan por email puede llegar a ser tan alta que **los criterios** que te he dado para detectar *spam*, aunque **son muy estrictos** y efectivamente **podrían clasificar como malicioso un mail legítimo**, es realmente la única forma de estar preparado para la mayoría de los fraudes que nos puedan llegar a nuestra bandeja.

Por otro lado, si alguien que conoces envía correos que puedan encajar dentro de lo que se pueda considerar *spam* (enviar enlaces o adjuntos sin aclarar por qué te los envía, con una excusa muy vaga o sin avisarte personalmente antes), **debes informarle** de que esa política de envío de correos es inadecuada porque es la misma que usan los criminales. Este póster es una buena guía para saber si algo que te llega puede ser un fraude rápidamente (<https://www.usecure.io/remote-resources>).



7 SIGNS THAT YOU'RE BEING PHISHED

Some common warning signs of a potential phishing email.

- The email is poorly written**


Although scammers can accidentally fall short in the grammar department, these 'mistakes' aren't always unintentional. Errors can be purposefully included in order to limit interaction with only the more 'observant'.
- It contains unsolicited attachments**


Typically, authentic institutions don't randomly send emails with attachments, especially when there is no previous relationship involved. If in doubt, contact the legitimate company by searching for their website.
- It requests sensitive information**


Emails that ask you to send sensitive info, such as banking details, tax scores or login credentials, are seriously phishy. You should search online and contact the organisation directly - not the sender.
- There's urgency involved**


Some scammers try to inflict urgency in their emails - often with threats of account expiration, fines or even prize giveaways - to encourage us to make rash decisions without proper thought.
- It sounds to good to be true**


Scammers often include 'limited' and 'unmissable' prize giveaways in their phishing emails in an attempt to blur our safety glasses. How does the old adage go? "If it sounds to good to be true...".
- It doesn't address you by name**


Many phishing scams are sent in their masses, with none (or limited) personalisation involved.
- The email address looks altered**


Scammers can make their email address look legitimate by including the company name within the structure of their email (e.g john@paypal123.com). Hover over links to make sure they don't look altered.

Figura 9. Este esquema es más concreto que el que te di en teoría y por tanto lo puedes aplicar más rápido. Acierta en un enorme nº de casos

Para que veas lo grave que es la situación, fíjate en estos ejemplos que te pueden servir para practicar si no tienes ninguno a mano:

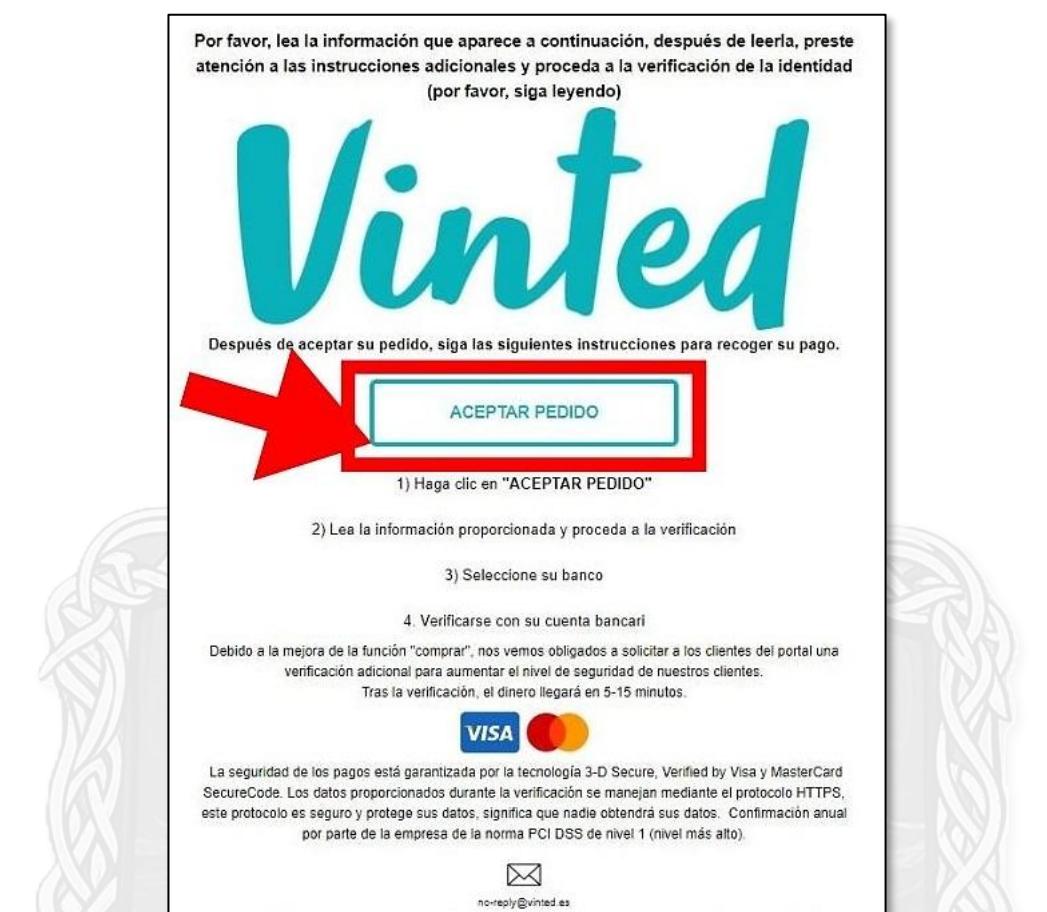


Figura 10. Esa copia exacta de un mail de Vinted con un botón peligroso...

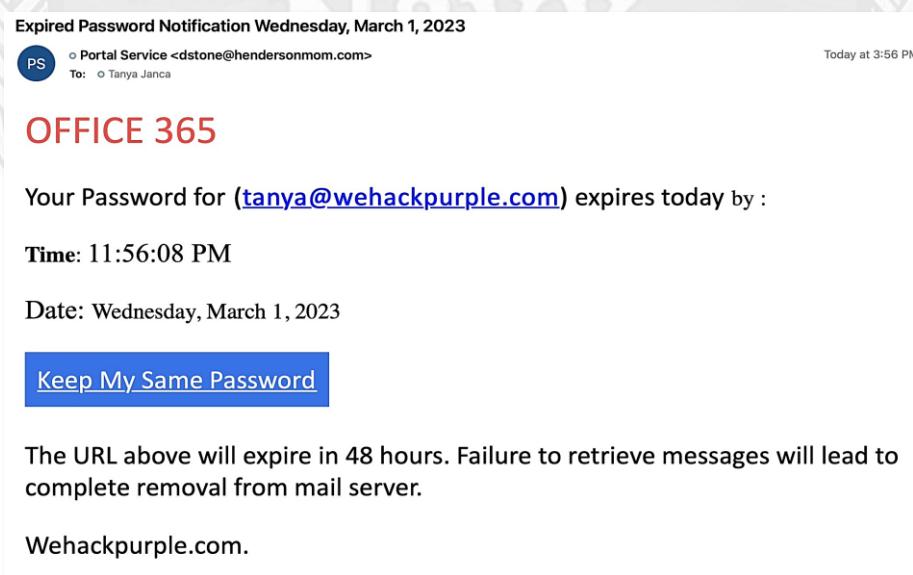


Figura 11. ¡Oh no, me caduca la clave y no quiero recordar otra! Voy a darle a este botón de un email que no tiene nada que ver con Office para que...me la roben :)



MS Maria-Elisabeth Schaeffler 6:37

Donación /4.700.000,00 euros

Ha recibido una donación de 4.700.000,00 euros, su dirección de correo electrónico se eligió al azar para recibir los 4.700.000,00 euros,

Póngase en contacto con el correo electrónico a continuación para obtener más instrucciones,
Correo electrónico: info.schaefflergroup@yahoo.com
Saludos amistosos

Maria-Elisabeth Schaeffler
SCHEFFLER AG.
Donación

Figura 12. Vaya, ¡soy rico! Voy a tener que irme a Andorra para no pagar impuestos

En realidad el envío de documentos adjuntos o de enlaces a través de correo **debería erradicarse** o limitarse a casos en los que ambos interlocutores están perfectamente avisados de lo que van a recibir. **Por ello, nunca debes aceptar algo así de un desconocido, o de alguien que crees qué conoces pero que te viene con una petición extraña o fuera de lo normal.**

Ejercicio MAILFALSOSSPEAR: Analizar mails fraudulentos dirigidos de ejemplo

⌚ Descripción de la actividad

Consiste en que destierres la creencia de que los intentos de estafa **son ataques por saturación masivos** a incautos a lo largo de todo el mundo que te pueden tocar por mala suerte, y que hay una variante de las estafas que van a por personas concretas expresamente.

⌚ Resultados Esperados

Puedes contestar a las siguientes preguntas:

- ¿Entiendes por qué este tipo de timos enfocados en una persona son más efectivos?
- ¿Comprendes también por qué puede interesar ir a por personas concretas en lugar de a por un *random* cualquiera?
- ¿Eres consciente de dónde van a sacar la información que van a usar luego contra ti?

▣ Otra información necesaria para su realización

El **spear phishing** es una variante de los engaños típicos en los que **se usan los datos conocidos de personas** (obtenidos por internet) para mandar a esas personas correos personalizados con dichos datos y con timos mucho más elaborados que los típicos que te pueden tocar y que se envían masivamente.

Timos hay muchos y la gente empieza a aprender un poco como van, pero cuando el timo menciona tu empresa, tu colegio, tu nombre, el nombre de tus familiares y **datos personales** que perfectamente se pueden sacar de una red social porque en muchos de nosotros los compartimos casi sin querer empieza a adquirir mucha más credibilidad y entonces llegan los problemas.



Para que entiendas bien cómo son estos timos puedes echar un vistazo a esta infografía:



Figura 13. Te investiga, te contacta, te engaña y...la has liado. Fuente: <https://us.norton.com/blog/online-scams/spear-phishing>

El INCIBE tiene estos enlaces para ayudarte a entender mejor el problema:

- <https://www.incibe.es/aprendeciberseguridad/spear-phishing>
- <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/falsa-solicitud-de-cambio-de-cuenta-de-nomina-traves-de-spear-phishing>
- <https://www.incibe.es/empresas/avisos/campana-spear-phishing-suplantando-al-servicio-web-11>

También tengo yo una imagen propia que te ayuda a entender cómo va el tema un poco mejor poniendo un mail real como ejemplo:



Figura 14. Un resumen de lo que es un fraude del CEO, un timo de spear phishing peligrosísimos

💡 ¿Sabes que tengo monográficos de variantes de estos timos? Mira:

- <https://github.com/jose-r-lopez/Fraudes-y-Timos/blob/main/Case%20Files/T1E25.%20Timo%20de%20las%20residencias.pdf?raw=true>
- <https://github.com/jose-r-lopez/Fraudes-y-Timos/blob/main/Case%20Files/T1E28.%20Falsas%20ofertas%20de%20empleo.pdf?raw=true>
- <https://github.com/jose-r-lopez/Fraudes-y-Timos/blob/main/Case%20Files/T1E2.%20Esta%20muy%20feo%20esto%20de%20los%20fraudes%20del%20CEO.pdf?raw=true>
- <https://github.com/jose-r-lopez/Fraudes-y-Timos/blob/main/Case%20Files/T1E8.%20La%20factura%20basura.%20El%20BEC.pdf?raw=true>



📲 Aplicaciones de Mensajería

🛠 Ejercicio MENSAJES FALSOS: Analizar unos mensajes fraudulentos de ejemplo

💻 Descripción de la actividad

Esta actividad consiste en **aplicar las normas para detectar fraudes que vimos**, pero con mensajes que te lleguen por mensajería instantánea (sea cual sea el programa usado para ello).

🏆 Resultados Esperados

Puedes contestar a estas preguntas:

- *¿Alguna vez te ha llegado un mensaje de esta clase?*
- *Si lo ha hecho, ¿era de un desconocido o de un conocido al que le habían intervenido o robado la cuenta de alguna forma?*
- *¿Entiendes por tanto que el hecho de que conozcas a un remitente (porque lo tengas en la agenda? no es garantía de que el mensaje sea auténtico?)*

📋 Otra información necesaria para su realización

Los programas de mensajería nos permiten un **contacto más estrecho** con personas, porque muchas veces son conversaciones uno a uno o de un grupo reducido entre ellos. Esto hace que psicológicamente podamos tener un **nivel de confianza mayor** en las cosas que nos lleguen por ellos puesto que, al otro lado, hay un círculo con una foto y alguien que técnicamente conocemos o tenemos mejor identificado que en un correo electrónico o una red social (al menos por lo general).

Los delincuentes saben esto, e intentan **robar cuentas** de redes sociales y aplicaciones de mensajería de personas **para inmediatamente “atacar” a sus contactos** aprovechándose de ello. Incluimos aquí algo de redes sociales porque los sistemas que tienen para **enviar mensajes privados** funcionan de forma muy parecida a las mismas. Por eso es importante también tener la guardia muy alta cuando recibamos mensajes por cualquier sistema de mensajería que tengan adjuntos o lleven enlaces.

En este caso voy a deciros incluso más: me han llegado casos de personas que envían enlaces a supuestas bromas o chistes de una manera completamente consciente y sin ánimo de ninguna maldad, pero que resulta que las páginas a las que dirigen **sí son maliciosas** y nos pueden meter en un lío si navegamos a ellas.

💡 **Por tanto, si un contacto te envía un video gracioso, un chiste, o algo similar lo mejor es no abrirlo y decirle que tenga mucho cuidado, porque es muy frecuente que este tipo de contenido se use para engañar a las personas y robarles su cuenta o su información.**

Como ejemplo de esto tenemos esta conversación privada por *Instagram*. *Instagram* no es una aplicación de mensajería pero, como decíamos antes, tiene un chat privado que funciona como una. No obstante, el mismo tipo de timo lo he visto en **WhatsApp** con una conversación muy parecida. Guarda dos similitudes:

- La persona que escribe es **supuestamente conocida** de la que ve los mensajes (aunque es otra que ha robado la cuenta a la persona real)
- Al final el objetivo es robarle la cuenta a la víctima para seguir propagando la estafa (el enlace que pide es el que se usa para resetear la clave de tu cuenta y, con él, se harán con ella):

José Manuel Redondo López. Proyecto “F-74 ‘Asturias’”



<https://maldita.es/malditobulo/20220519/instagram-cuentas-hackeadas-inversion-criptomonedas/.>

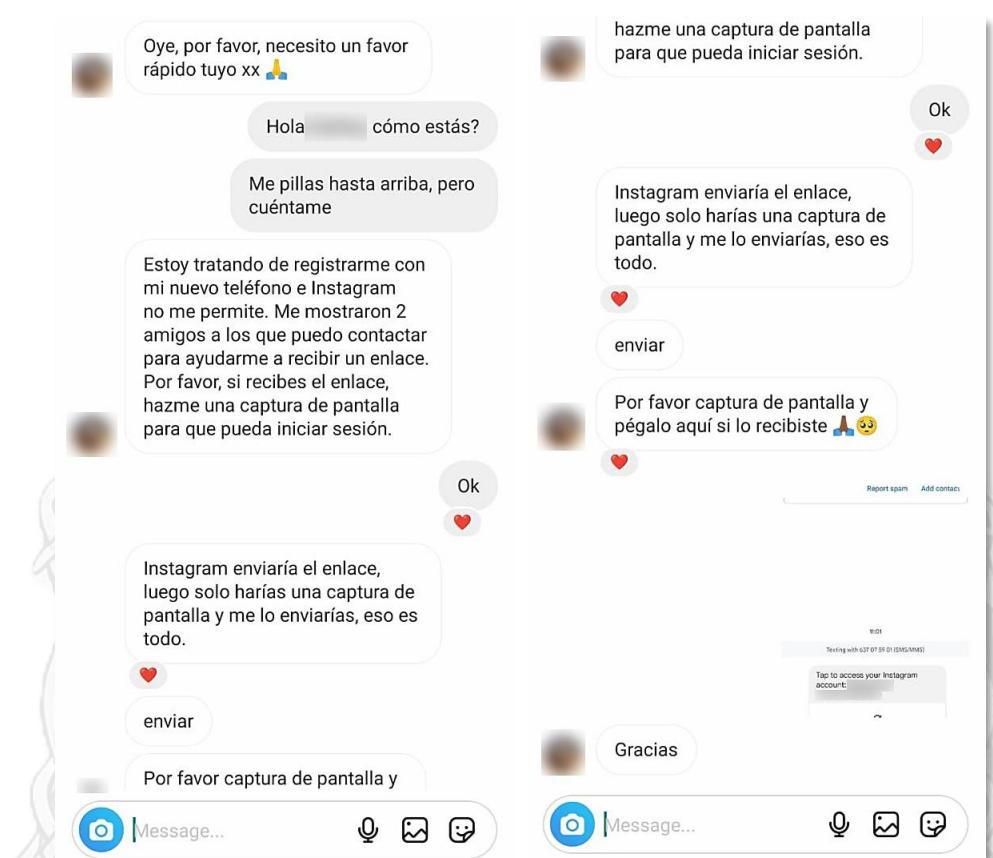


Figura 15. Como le hagas caso te quedas sin cuenta. El delincuente finge ser tú, pero no sabe tu clave así que usa "Recordar contraseña". Eso genera un enlace que te llega a ti, y si le pasas lo que sale al pulsar el enlace, entonces podrá completar la jugada, suplantarte completamente y hasta luego cuenta

En caso de WhatsApp o similar, lo que te suelen pedir es un código, pero el objetivo es el mismo:
<https://www.welivesecurity.com/la-es/2023/01/30/robo-cuentas-whatsapp-tendencia-crece-podcast/>

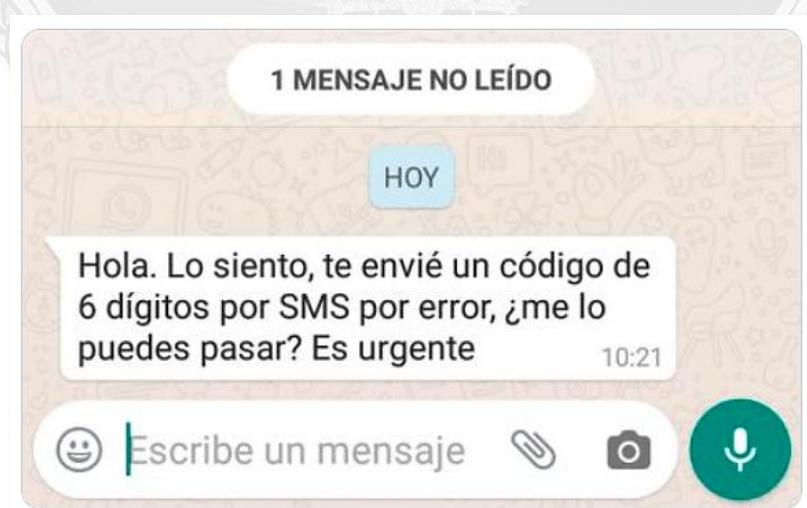


Figura 16. Mismo truco, diferente programa (se repite en todos prácticamente)



Y, como vemos en estas imágenes, **se aprovechan de la familiaridad para robar dinero** (todo lo que lees aquí son cuentas suplantadas). Observa el tipo de lenguaje que usan, con expresiones de familiaridad para mejorar el engaño:

Creo que es importante difundir esto. Ayer recibí un mensaje por WhatsApp de un familiar pidiéndome una transferencia. De entrada, el pedido me pareció extraño. Pregunté en un grupo y había personas que recibieron el mismo mensaje y habían transferido su dinero. Los estafaron.

Translate Tweet

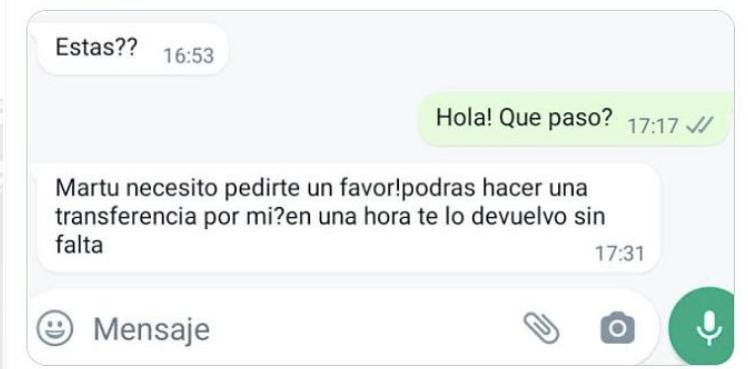


Figura 17. Pide dinero suplantando un familiar. Lo mejor es que si te pasa esto llames tu a ese familiar para confirmar. ¡Te sorprenderías la de gente que descubre que no era él realmente!



Figura 18. El mismo truco, pero ya con los datos de la transferencia. Es un timo muy común

El siguiente mensaje me sirve para recordar que este tipo de relaciones personales no están limitadas solo a las familiares, **sino también a las laborales**. En este mensaje la jefa de alguien está siendo suplantada para darle legitimidad a un correo electrónico que se ha enviado (o bien para luego “colarle” un documento malicioso). En este caso el lenguaje es atípico, pero como decía antes, eso cada vez es menos frecuente:



Figura 19. Aunque sea tu jefe, padre, profesor... el procedimiento es sencillo: Te pide algo raro, llámale tú al nº de siempre y confirma que es cierto

🛠 Ejercicio ROBOSCUENTAS: Investigar métodos de robo de cuentas documentados

👤 Descripción de la actividad (AQUÍ)

Las cuentas en aplicaciones de mensajería no son una excepción a las que ya hemos visto y, aparte de la password segura, **también debemos activar el 2FA**.

🏆 Resultados Esperados

Puedes configurar **una password segura y un 2FA** en cualquier cliente de redes sociales que estés usando. Además, eres capaz de identificar timos destinados a robarte tus cuentas (que es la razón por la cual haces lo primero).

📋 Otra información necesaria para su realización

En esta actividad no solo queremos repetir lo que hemos hecho con otros servicios acerca de passwords y 2FA sino también que entiendas que en las redes **sociales hay una problemática relacionada con el robo de cuentas especial** que consiste en un timo de los que mucha gente ha sido víctima.

Esta problemática consiste en que una persona (conocida o no) te escribe diciendo que **te ha enviado un código de 6 dígitos por SMS por error** y que si se lo puedes pasar de forma urgente. Conviene que sepas que ese código es una petición para cambiar la contraseña de tu cuenta qué ha hecho el delincuente. La aplicación usa un 2FA para confirmar que eres tú (esa es precisamente la función de ese código que recibes). Dicho de otra forma: un delincuente que sabe tu contacto ha fingido ser tú, le ha dicho a la aplicación de mensajería que no recuerda su password (porque es la tuya) y ahora la aplicación te está pidiendo confirmación de que efectivamente eres tú el "olvidadizo" real antes de dejarte poner una contraseña nueva.



¿Qué ocurre? Que al ser un 2FA, si le pasas el código WhatsApp, Telegram o la aplicación que sea entenderá que has sido tú el que quiere cambiar la clave de tu cuenta, y por tanto **el atacante podrá poner la contraseña que él quiera** y hacerse con tu cuenta de la aplicación de mensajería. Esto es un timo clásico en el que no debes picar por muy pesado o borde que se ponga quien te envía ese mensaje, aunque sea alguien conocido. Ten en cuenta que ese alguien conocido pudo haber sido una víctima de este mismo timo y que el atacante esté intentando obtener más cuentas a través de él, usando el mismo truco con sus contactos. **Más información:**

- <https://www.xatakamovil.com/seguridad/timo-codigo-6-digitos-sms-whatsapp-como-identificarlo-evitar-ser-victima-estafa>
- www.genbeta.com/seguridad/te-envie-codigo-6-digitos-error-como-protegerte-nueva-estafa-whatsapp-para-robarte-cuenta

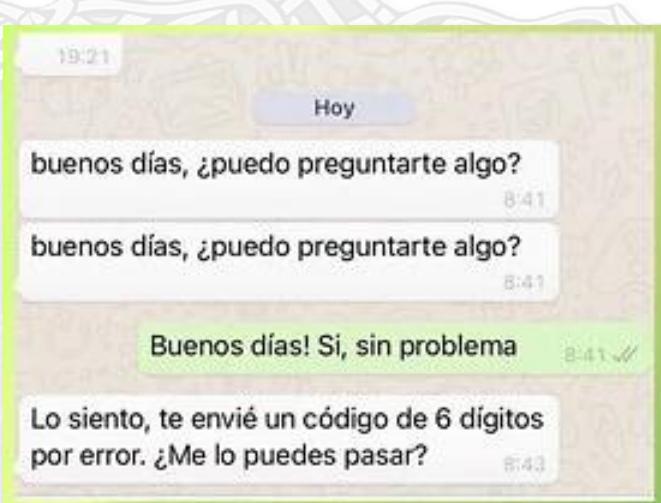


Figura 20. Esto es una trampa clásica. ¡No caigas!

Por tanto, si tienes un 2FA en la red social, este tipo de timos es mucho más difícil de hacer, puesto que el atacante tendría que pedirte el código que te sale para poder entrar y eso ya es tremadamente sospechoso (especialmente si sabes que estas cosas pasan). Por tanto es una razón más para activarlo y el motivo por el que se inventan esta historia para engañarte.

🔍 ¿Sabes que tengo monográficos sobre el tema? Mira:

- <https://github.com/jose-r-lopez/Fraudes-y-Timos/blob/main/Case%20Files/T1E15.%20El%20timo%20del%20falso%20hijo.pdf?raw=true>
- <https://github.com/jose-r-lopez/Fraudes-y-Timos/blob/main/Case%20Files/T1E28.%20Falsas%20ofertas%20de%20empleo.pdf?raw=true>
- <https://github.com/jose-r-lopez/Fraudes-y-Timos/blob/main/Case%20Files/T1E22.%20Familiar%20con%20cuenta%20robada.pdf?raw=true>



⚙️ Dispositivos de Computación

📱 Telefónica Móvil

🛠️ Ejercicio PLAYSTORE: Mirar alguna aplicación con mala pinta en la Play Store

👤 Descripción de la actividad

Consiste en entender y ser capaz de **ver indicios de que una aplicación** es falsa y está intentando suplantar a una verdadera o bien es un malware que te puedes descargar de una tienda de aplicaciones oficial.

🏆 Resultados Esperados

Eres capaz de **identificar aplicaciones falsas** que puedas ver incluso en la tienda oficial de aplicaciones, primero para no instalarlas tú mismo, y segundo para prevenir a otros. Puedes contestar estas preguntas:

- *¿Te queda claro que estar en una tienda oficial no es garantía de que una aplicación no tenga "bicho"?*
- *Por lo que has visto ¿Son frecuentes este tipo de aplicaciones en la tienda en la que has buscado?*
- *¿Ves alguna de estas falsificaciones tan buena que hubieras "caído" antes de saber que este tipo de cosas existían?*

📘 Otra información necesaria para su realización

Es un hecho que muchas aplicaciones falsas y que habitualmente contienen *malware se aprovechan de la fama de otras* para que, en un despiste o por desconocimiento, haya personas que las instalen creyendo que son la verdadera. También es un hecho que muchas aplicaciones se aprovechan de estar en una tienda oficial para hacerse pasar por inofensivas. Fiarnos es en ambos casos un error. Hay varios indicios de cosas que se usan habitualmente para hacer estas falsificaciones y que las víctimas piquen e instalen la aplicación que no es. Podemos enumerar unos cuántos:

- Usar el **mismo ícono** o uno muy parecido a una aplicación conocida.
- Tener un **nombre muy similar**
- Tener un conjunto de **valoraciones falsas**, basadas en tener siempre 5 estrellas sin comentarios o con el mismo comentario varias veces (señal que se ha hecho con un bot, y no una persona)
- Tener el **mismo nombre que la aplicación real** pero con algún añadido que la haga parecer una versión avanzada como "*extra*", "*plus*" o "*gold*"
- **Hacerse pasar por una versión gratuita** de una aplicación comercial que realmente no existe, como por ejemplo poniéndole "*free*" detrás del nombre real. El fabricante no ofrece realmente una versión gratuita de la aplicación, pero el delincuente se aprovecha de que mucha gente no lo sabe.
- **Hacerse pasar por una versión "recortada"** de una aplicación comercial haciendo creer a los usuarios que es una versión con menos prestaciones, pero igualmente funcional, aunque en realidad el fabricante original no ofrezca este tipo de versiones.
- Directamente **recurriendo al engaño** y poner una aplicación con el mismo ícono, el mismo nombre y añadiéndole "*tutorial*", "*cheat*", "*trucos*", etc., siendo entonces una aplicación que no tiene nada que ver con lo original, sino que es un mero añadido a la misma (potencialmente peligroso) o un supuesto "manual de instrucciones". Normalmente no ofrecen ningún tipo de contenido reseñable y solo se aprovecha del nombre para que algún incauto se la instale por despiste (aunque quizás no sea *malware* en este caso, y solo una que ofrece este contenido).



Para hacer esta actividad se recomienda entrar en la tienda de aplicaciones de tu teléfono móvil y buscar algunas que cumplan con esos criterios para ver qué valoraciones tienen y si los usuarios han detectado el engaño, para así ser consciente de cómo aparecen y estar más atento a este tipo de problemas. Mira en la imagen cuantas aparecen relacionadas con WhatsApp en forma de anuncio pagado nada menos 😕.

💡 **Ni siquiera hace falta que uses tu móvil. Por ejemplo, puedes ir a la tienda de aplicaciones de Android desde cualquier navegador entrando aquí: <https://play.google.com/store/apps?hl=es> o a la de Microsoft aquí: <https://apps.microsoft.com/home?hl=es-es&gl=ES>.**



Figura 21. Menudo panorama tenemos en las tiendas de aplicaciones con los dichosos iconos parecidos para jugar al despiste e instalarte lo que no quieras :(

Si alguna de las que encuentras te ofrece dudas, puedes ver su ficha de permisos (o bien usar **Exodus Privacy** <https://reports.exodus-privacy.eu.org/en/>) para ver si pide demasiados permisos para lo que se supone que hace. Por ejemplo, fíjate en esta aplicación que se supone que servía para cambiar el ícono de la red social X por el antiguo ícono de Twitter... ¿No te parece que pide demasiadas cosas para hacer solo eso? ¿No será que hace algo más? 😕

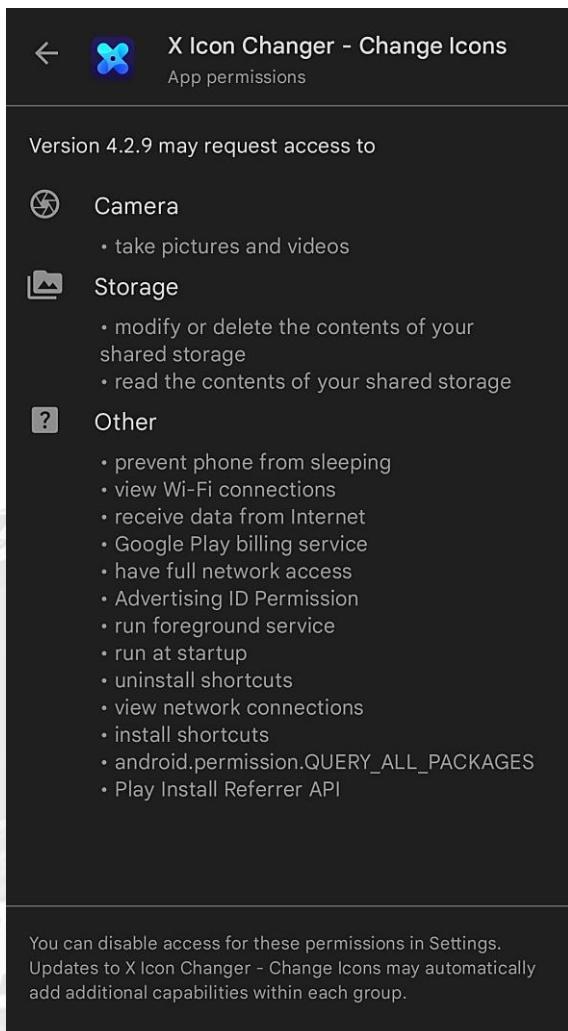


Figura 22. ¿Todo eso para cambiar el icono de una aplicación? Venga ya, por favor...

🛠 Ejercicio APPSMALICIOSAS: Mira noticias de streamers / periódicos etc. que han recomendado aplicaciones maliciosas

💡 Descripción de la actividad

Con este ejercicio quiero que te des cuenta de que no todas las recomendaciones son igual de buenas, y que la persona que recomienda un producto tiene que ser verdaderamente experto en él para así poder saber **cuándo te puedes fiar de él/ella y cuando no**. Con eso quiero decir que, aunque muchos streamers que te caigan genial te recomiendan una cosa, **hay que ver si esa persona tiene conocimientos en ese campo o no.**

🏆 Resultados Esperados

Puedes contestar a estas preguntas:

- ¿Entiendes que una recomendación de un *streamer* tiene validez si ese *streamer* realmente es experto en el tema?
- ¿Sabes que muchos *streamers* simplemente promocionan cualquier cosa por la cual les paguen y que aunque asegure que usa el producto y que es un experto en él no tiene por qué ser cierto?

José Manuel Redondo López. Proyecto "F-74 'Asturias"



Otra información necesaria para su realización

Que los *streamers cobran por hacer colaboraciones* es algo que todo el mundo sabe. Que algunas veces esas colaboraciones **se hacen sin probar realmente el producto**, y que simplemente quieren hacer el anuncio recomendarlo a su audiencia y nada más también es una posibilidad. Y con esto no pretendo acusar a nadie, porque no tengo motivos, simplemente te quiero decir que ya ha pasado, y que no debes fiarte ciegamente de las recomendaciones que te hacen los *streamers* por si acaso. Mira esta noticia para entender cómo lo hacen: <https://unaaldia.hispasec.com/2022/09/el-virus-que-utiliza-youtube-como-medio-de-propagacion.html>





Ordenadores

Ejercicio DESCARGAAPP: Consultar un procedimiento para descargar aplicaciones de forma más más segura

Descripción de la actividad

Se trata de buscar noticias o artículos donde **la descarga de un crack para piratear un software** haya llevado una infección y pérdidas para la persona que lo hizo

Resultados Esperados

Puedes contestar estas preguntas:

- *¿Alguna vez te has planteado descargar algún tipo de software de esta clase?*
- *¿Has pensado bien qué tipo de garantía ofrece este tipo de software tanto sobre lo que hace como lo que no hace?*
- *¿Crees que la gente que hace este software lo hace por amor al arte, o que busca sacar algún tipo de beneficio económico directo o indirecto?*

Otra información necesaria para su realización

Realmente la descarga de programas que intentan quitar las protecciones contra copia a programas legítimos se ha convertido en **una de las formas más típicas de transmitir malware** en el mundo, debido a que estos programas no solo pueden estar creados por personas sin escrúpulos, sino que también pueden ser fácilmente falsificados y **carecen de cualquier tipo de comprobación o prueba** de que realmente hacen lo que hacen.

Por otro lado, no es raro que sean de tipo **troyano**, en el sentido de que realmente quiten la protección contra la copia del programa, pero **además instalen algún tipo de software espía**, o que use tu máquina para algún tipo de acción criminal o algo que saque algún beneficio para el que creó el programa.

Piensa que, aparte de los problemas legales que esto conlleva, realmente **no tienes ningún tipo de garantía** acerca de lo que hay detrás de ese programa, de cómo se ha creado, o de que hace lo que debe hacer. Por tanto puedes considerar que es como instalar una “**bomba de relojería**” que te puede estallar en tu disco duro. Buscar noticias de esta clase es una forma de demostrarte que así es. Para saber más: <https://www.cronup.com/cracks-una-solucion-temporal-o-una-excelente-forma-para-desplegar-malware/>



The figure consists of two side-by-side screenshots of websites that provide cracked versions of popular software for download. The left website, titled 'Cracked PC software,s Direct Download links', offers IDM Crack 6.40 Build 8 Patch + Serial Key Free Download, 4K Video Downloader Crack 4.20.0.4740 With Key Download [Latest], and Windows 10 Activator TXT Free Download [March 2022 Updated]. The right website, titled 'Software Crack Download', offers IDM Crack 6.40 Build 8 Patch With Serial Key Free Download, Adobe Illustrator Crack v25.4.1A98 With Full version 2022 Free Download, Nord VPN Crack 6.40.5.0 With Serial Key Free Download, and Wondershare PDFelement Pro Crack 8.2.211064 Free Download. Both sites feature a search bar, categories dropdown, and a 'CRACK DOWNLOAD' button.

Figura 23. Todo esto suena muy bonito para tu bolsillo en primera instancia, hasta que de repente te descargas algo y lleva sorpresa no muy agradable :(

No quiero caer en tampoco en el clásico consejo que puedes considerar algo mojigato de “no te descargas cosas piratas” sin darte realmente razones de peso para que no lo hagas. Voy más allá del hecho de que es delito, y que realmente estás descargando algo que es propiedad de una empresa que ha pagado por su desarrollo y que luego quiere venderlo para sacar un beneficio de todo lo que ha invertido. Si esto no te parece suficientemente grave, con este ejercicio quiero que te des cuenta de que realmente estás sometiéndote a un riesgo importante. **No estoy de broma, mira** (y esto solo es uno de tantos ejemplos): <https://www.3djuegos.com/juegos/minecraft/noticias/decenas-mods-populares-minecraft-estan-infectados-malware-sigue-estos-pasos-para-comprobar-tu-pc-esta-peligro>

Mira, no voy a negar que evidentemente hay toda una corriente de gente que favorece las descargas ilegales usando para ello distintas justificaciones para convencer a más gente de que lo hagan: monopolios, licencias abusivas, subidas de precio arbitrarias y otras razones que no voy a entrar a discutir si son o no verdad, por qué no me corresponde a mí. Pero, en último caso, **estás obteniendo gratis algo que está a la venta en un comercio**.

Sí en lugar de un programa fuesen unas zapatillas o una camiseta seguro que entendías mejor que eso no se debe hacer...

Pero vamos a suponer que esas razones te convencen, y aun así quieres hacerlo. Ahora es cuando yo te digo que **eso es peligroso** porque puedes tener un *malware* de cualquier tipo en tu PC o móvil con todos los problemas que eso te puede causar. *¿No me crees?* Fíjate en estos dos enlaces que tienen una enorme cantidad de instrucciones, precauciones y acciones que debes hacer para **tratar de descargarte algo pirata de forma segura**. Y date cuenta de que digo de **tratar**, porque en este escenario **la seguridad al cien por cien nunca la vas a tener**. Créeme nunca. Quien haya puesto eso pirata ahí no tiene que cumplir con ningún



tipo de restricción y requisito legal, ni está sometido a ningún tipo de normativa que, aunque te parezca increíble, también es parte del precio que pagas.

- <https://www.reddit.com/r/Piracy/wiki/megathread/>
- <https://rentry.org/pgames>

🔍 Si piratear seguro fuese tan fácil, ¿crees que existirían páginas como estas?

Y es que sí puede sonar muy de la vieja escuela a decir que “**no pirates**”. Que las compañías se pasan con el precio que cobran por sus programas o juegos (aunque sabes que la inmensa mayoría **baja de precio estratosféricamente a los pocos meses** una vez que haya pasado el “efecto novedad”). Pero créeme si te digo que **esta es la mayor causa probablemente de tener malware en equipos de todo el mundo**. *¿De verdad te la vas a jugar por intentar jugar a algo que seguramente en pocos meses tendrás a un precio mucho más pequeño probablemente con las protecciones de copia quitadas como les pasa a muchos juegos cuando llevan varios meses en el mercado y en su caja y embalaje original libres de todos estos problemas? Piénsatelo seriamente por favor. No es un juego.*



🛠 Ejercicio PUP: Consultar casos donde ha habido descarga de PUPs con otro producto

👤 Descripción de la actividad

Consiste en **localizar alguna noticia o artículo** donde se hable de **programas técnicamente legales** que, a la hora de instalarlos, instalaban también otros que podían ser perjudiciales o simplemente no deseados, sin que el usuario tuviera fácil no hacer esa instalación, o bien por defecto se instalase sin que se hiciese un aviso claro de que eso iba a ocurrir.

🏆 Resultados Esperados

Puedes localizar programas **que hacen este tipo de instalaciones adicionales no deseadas** y contestar a las siguientes preguntas:

- *¿Tienes alguno actualmente instalado que cumple con estos requisitos?*
- *¿Podrías desinstalar el programa que viene añadido siguiendo la actividad anterior o ambos son inseparables?*
- *¿Entiendes por qué es importante siempre descargarse un programa de su web oficial, aunque eso no te asegure al 100% que no lleven estos programas “acompañantes”?*

📋 Otra información necesaria para su realización

Por favor, ten en cuenta que el hecho de que un programa legal venga con este tipo de software **añadido no significa que el software añadido sea malware** o un virus. Simplemente en muchas ocasiones implica que las dos empresas han hecho un acuerdo comercial para que ambos se instalen de forma conjunta a cambio de dinero. No deja de ser **un acuerdo de publicidad**, pero claro a ti te cuesta espacio en el disco duro y tener programas que no vas a usar nunca muy probablemente, lo que entra en conflicto con lo dicho anteriormente.

🔍 Vamos, que una se aprovecha del “tirón” de la otra



OPTIONAL OFFERS



- Yes, install the free McAfee Security Scan Plus utility to check the status of my PC security. It will not modify existing antivirus program or PC settings. [Learn more](#)
- Yes, install McAfee Safe Connect to keep my online activities and personal info private and secure with a single tap. [Learn more](#)

GET MORE OUT OF ACROBAT:

- Install the Acrobat Reader Chrome Extension

By checking the above, I agree to the automatic installation of updates for Acrobat Reader Chrome Extension
[Learn more](#)



Adobe Acrobat Reader DC

The leading PDF viewer to print, sign and annotate PDFs.

[Download Acrobat Reader](#)

263 MB

By clicking the 'Download Acrobat Reader' button, you acknowledge that you have read and accepted all of the [Terms and Conditions](#). Note: your antivirus software must allow you to install software.



Figura 24. Hasta no hace tanto tiempo, estas casillas venían marcadas por defecto. Alguien debió darles el toque (probablemente la ley europea anti-prácticas de monopolio)

Debes también tener en cuenta que es más probable encontrarse en esta situación **si te descargas programas fuera de sus páginas oficiales**. Muchos sitios de descarga de programas que funcionan como "bibliotecas", suelen añadirles software con publicidad u otro tipo de software no deseado a su instalación para financiarse, u otros motivos más "oscuros" 😕 .





Hardware y Redes

Redes de Comunicaciones

Ejercicio ROBLOX: Leer sobre los problemas que hay en juegos sociales cuando se mete "gentuza"

Descripción de la actividad

Con esta actividad quiero que entiendas que existe una serie de personas que usan los juegos sociales como **Roblox para “cazar” a sus víctimas**. La mayoría de ellos no son simples estafadores, sino que son **groomers**. Y eso puede ser muy dañino para ti,

Resultados Esperados

Puedes contestar a estas preguntas:

- ¿Entiendes qué Roblox es un juego muy divertido, pero que alguna gente lo usa como excusa para contactar con posibles víctimas menores y arruinarles la vida?
- ¿Comprendes que en ese sentido debes tener las mismas precauciones que en cualquier red social por mucho que estés en un juego?

Otra información necesaria para su realización

Quiero que entiendas que **Roblox no es un juego malo en sí**, lo que es malo son algunas de las personas que juegan a él haciendo pasar normalmente por menores de edad. Lo que buscan estas personas, aparte de estafas, es hacer **grooming**. Si no sabes lo que es el grooming tengo un monográfico sobre ello aquí que te explica todo: <https://github.com/jose-r-lopez/Fraudes-y-Timos/blob/main/Case%20Files/T1E34.%20Grooming%20y%20ataques%20a%20la%20infancia.pdf?raw=true>

 También tengo un video de menos de 5 minutos donde te cuento, tal y como lo dije en la radio, en qué consiste este problema en Roblox <https://youtu.be/-BJE0ctTMe8>

Y ojo, que esto no es algo que me invente yo, lee estas noticias para saber a qué nos estamos enfrentando:

- **Roblox: Denuncian acosos a menores en el popular juego** (7/10/2020): <https://vandal.elespanol.com/noticia/1350738601/roblox-denuncian-acosos-a-menores-en-el-popular-juego/>
- **Guía para padres: Cómo proteger a los hijos en Roblox** (26/06/2023): <https://www.infobae.com/tecnologia/2023/06/27/guia-para-padres-como-proteger-a-los-hijos-en-roblox/>
- **Ciberacoso sexual: Pensaba que mi hijo jugaba a un videojuego inocente pero le enviaban imágenes pornográficas** (30/5/2019): <https://www.bbc.com/mundo/noticias-48464190>



🛠 Ejercicio ASISTENCIA: Investigar lo que hace un programa de asistencia remota

💻 Descripción de la actividad

La idea de tener asistencia integrada en *Windows* no es en absoluto mala. Muchas veces te puede servir para sacar de un aprieto a alguien que tenga mucho menos experiencia manejando ordenadores que tú, y por ello es una herramienta muy útil usada para el bien. Lo malo es que en muchos estafadores lo saben y lo usan para el mal.

🏆 Resultados Esperados

Puedes contestar a estas preguntas:

- ¿Entiendes que la asistencia remota básicamente te da el control total de un equipo si consigues que la persona que controla ese equipo te den los datos necesarios para poder usarla?
- ¿Comprendes que la asistencia remota se puede hacer tanto para el bien como para el mal porque básicamente es lo mismo que Estar sentado delante de un teclado del PC?

📋 Otra información necesaria para su realización

Esto de la asistencia remota es un aspecto muy polémico, porque si bien es una gran idea y tiene sus usos legales y legítimos, también se abusa mucho de ello para hacer estafas. Ten en cuenta que tomar el control del PC no solo consiste en poder descargarte lo que sea y ejecutarlo (con lo cual el delincuente podría instalar un *malware* donde quiera) sino que además puede mirar datos privados, como contraseñas cuentas del banco, etc. y, en definitiva, cualquier cosa valiosa que puedas tener en el ordenador. Por ello es muy importante que te mentalices de que este tipo de permisos no se le pueden dar a cualquiera.

La asistencia remota de *Windows* se usa así: <https://support.microsoft.com/es-es/windows/solucionar-problemas-del-equipo-de-forma-remota-con-asistencia-remota-y-conexi%C3%B3n-f%C3%A1cil-cf384ff4-6269-d86e-bcfe-92d72ed55922>. Si alguien te pide hacer esto y no lo conoces, **ni caso**.

💡 El uso de programas de asistencia es muy típico del timo de Microsoft. Si quieres saber más sobre este timo tengo un monográfico aquí: <https://github.com/jose-r-lopez/Fraudes-y-Timos/blob/main/Case%20Files/T1E5.%20No%2C%20te%20prometo%20que%20no%20es%20Microsoft.pdf?raw=true>



⌚ Dispositivos “Smart”

🛠 Ejercicio CVEs: Mirar vulnerabilidades de programas conocidos

💻 Descripción de la actividad

Necesitas saber si una página web está ejecutando productos/frameworks con **vulnerabilidades conocidas** sin usar herramientas especiales

🏆 Resultados Esperados

Esta actividad se completará cuando localices **la lista CVE de vulnerabilidades conocidas** de cualquier producto que prefieras (preferible desde encabezados HTTP, pero vale cualquier producto si no tienes suerte encontrando una página web "indiscreta").

📋 Otra información necesaria para su realización

Siempre que nos conectamos a una web, aparte del contenido (HTML) también recibimos información adicional: **las cabeceras HTTP**. Estas cabeceras contienen información necesaria para que "las tripas" de Internet funcionen pero, a veces, también contienen información excesiva que podemos aprovechar muy fácilmente: información de **tipo de producto y versión**. Esta información puede parecer trivial, pero se puede usar para localizar las vulnerabilidades conocidas de las versiones de los productos que el servidor web usa, y que nos está proporcionando amablemente de forma gratuita 😊

🔍 *Ni siquiera se necesita un software especial para hacer esto, ya que el propio navegador puede mostrar esta información. El siguiente diagrama muestra cómo hacer esto en Firefox, pero otros navegadores también tienen esta opción.*

Una vez hagas esto solo tienes que localizar una página web que proporcione este exceso de información al navegador (no todas lo hacen) y contrastar esa información contra bases de datos CVE como las que se muestran en teoría:

- <https://cve.mitre.org/>
- <https://www.cvedetails.com/>



The screenshot shows the Firefox Developer Tools interface. On the left, the 'Desarrollador web' menu is open, with 'Desarrollador web' and 'Herramientas' highlighted with red boxes. A red arrow points from the 'Herramientas' item to the right-hand sidebar. The right-hand sidebar lists various developer tools with their keyboard shortcuts. Below the menu, the main window displays the Network tab of the developer tools. It shows a list of network requests for 'main.css?browserId=firefox&themeld=' with status codes 200 and GET methods. The last request in the list is highlighted with a blue selection bar. The Network tab has columns for Estado, Método, Dominio, Archivo, Causa, Tipo, Transferido, Tamaño, and Headers. The Headers section for the selected request shows the following:

Header	Value
Cache-Control	max-age=315360000, public
Connection	Keep-Alive
Content-Encoding	gzip
Content-Length	37040
Content-Type	text/css
Date	Fri, 28 Feb 2020 09:27:09 GMT
Etag	"19ba08f"
Filter-class	com.liferay.portal.servlet.filters.header.HeaderFilter
Keep-Alive	timeout=15, max=100

Figura 25. ¿Ahora sí que te sientes hacker eh? :)

Esto puede ser una vulnerabilidad de seguridad grave, así que no esperes que páginas web de empresas importantes te de esta información gratuita fácilmente (¡aunque nunca se sabe! 😊). Mira un ejemplo práctico real:

The screenshot shows the Chrome DevTools Network tab. It displays a list of requests with their status, method, and URL. One specific response header is highlighted with a red box. The highlighted header is 'Liferay-Portal: Liferay Portal Standard Edition 5.2.3 (Augustine / Build 5203 / May 20, 2009)'. The Network tab has tabs for Headers, Preview, Response, Cookies, and Timing.

Figura 26. Curiosamente, dar esta información es completamente innecesario: La página funciona igual aunque no la des. Créeme. Pero aquí está, "cantándolo todo"

Y si te pones a mirar el producto, mete miedo lo que te encuentras:
https://www.cvedetails.com/vulnerability-list/vendor_id-2114/product_id-12592/version_id-109268/Liferay-Portal-5.2.3.html



🛠 Ejercicio SHODAN: Buscar una IP en Shodan y ver qué pasa

💻 Descripción de la actividad / Aplicación práctica

Puedes usar el motor de búsqueda de máquinas *Shodan* para averiguar información acerca de cualquier dispositivo en Internet.

🏆 Resultados Esperados

Esta actividad se completará cuando puedas hacer una petición en *Shodan* sobre una sola URL o IP, analizando la salida que se obtiene y por qué crees que su información puede ser un peligro para el objetivo.

🔍 **Tienes más libertad si creas una cuenta gratuita, pero no es necesaria para hacer este ejercicio si te limitas a IPs individuales.**

📘 Otra información necesaria para su realización

Shodan (<http://www.shodanhq.com/>) es un buscador capaz de encontrar dispositivos en lugar de páginas web: routers, servidores, cámaras de grabación CCTV, semáforos, Para un uso básico basta con poner una IP (que la puedes sacar como te comentaba en la teoría) y esperar a ver qué te dice. Por ejemplo mira lo que pasa con esta dirección: <https://www.shodan.io/host/156.35.94.10>.

Country	Spain
Organization	Entidad Pública Empresarial Red.es
ISP	Entidad Pública Empresarial Red.es
Last Update	2020-11-05T08:59:33.859619
Hostnames	petra.euitio.uniovi.es
ASN	AS766

⚡ Web Technologies

- Moodle
- PHP
- Polyfill
- RequireJS

⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2019-0215	In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.
CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2019-0217	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Servers that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0196	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts

Figura 27. Si, esta máquina "cantaba" todas sus vulnerabilidades con Shodan. No te preocunes, ya no está en servicio :P



Si decides hacerte una cuenta y te apetece experimentar un poco, puedes usar este *cheatsheet* para hacer búsquedas, practicar un poco y ver qué pasa. No te olvides que una cuenta gratuita tiene un límite diario de búsquedas, así que mejor “no te ansíes” 😊.

SHODAN Cheat Sheet

Cyber Writes

what is Shodan?

Shodan is a publicly available search engine which scans the entire Internet for a limited number of services and enumerates any discovered services by their banner responses, indexes that data and makes it searchable.

Shodan stores the information and indexes across five main fields: data, ip_str, port, org and location.country_code.

Be sure to use the 'View Raw Data' option on any discovered host to see all of the data Shodan has stored and learn possible new techniques of use.

While not always required, surround each search term in quotes to reduce confusion and broken queries.

Physical Location

Country - Search by country code
Example:
`country :"US"`

City - Search by city name
Example:
`city :"New York"`

State - Search by state code abbreviation
Example:
`state :"NY" or region :"NY"`

Zip Code - Search by postal ZIP code
Example:
`postal:"92127"`

Geo - Search by GPS coordinates
Example:
`geo:"40.759487,-73.978356"`

Geo - Search by GPS (within a range of 2 km)
Example:
`geo:"40.759487,-73.978356,2"`

Web Apps

Page's Title - Search for text in page's title
Example: `title: "Index of /ftp"`

Page's HTML Body - Search body of webpage for text string
Example: `html:"XML-RPC server accepts"`

Web Technologies - Search for specific web technologies
Example: `http.component:"php"`

SSL/TLS - Search for SSL/TLS versions supported
Example: `ssl.version:"sslv3" or ssl.version:"tlsv1.1"`

Expired Certificates - Search for expired HTTPS certs
Example: `ssl.cert.expired:"true"`

IP Addresses & Subnets

Single IP Address - Search findings on single IP
Example: `52.179.197.205`

Hostname - Search for string in any hostnames
Example:
`hostname:"microsoft.com"`

Subnet - Search across a specific subnet range
Example: `net: "52.179.197.0/24"`

Port - Find any instances of active services on a port
Example: `port:"21"`

Service - Search for instances of specific services
Example: `"ftp"`

Service on Specific Port
Example: `"ftp" port:"21"`

Internet Service Provider - Search by ISP name
Example: `isp:"Spectrum"`

Autonomous System Number (ASN) - Search by ASN
Example: `ASN:"AS8075"`

Operating Systems, Products

Operating System - Search by operating system type
Examples: `os:"Windows Server 2008"` or `os:"Linux 2.6.x"`

Organization/Company - Search by organization name
Example: `org:"Microsoft"`

Product - Search by known product name
Example: `product:"Cisco C3550 Router"`

Version - Search for specific version number
Example: `product:"nginx"` or `version:"1.8.1"`

Category - Search by Shodan category
Example: `category:"ics"` or `category:"malware"`

Microsoft SMB - Search for specific SMB versions
Example: `smb:"1" or smb:"2"`

Microsoft Shared Folders - Find exposed shared folders
Example: `port:"445" shares:""`

Other

Date: After - Search for findings that appear after a date
Example: `after:"01/01/18"`

Date: Before - Search for findings that appear before a date
Example: `before:"12/31/17"`

Screenshot - Display results which only have screenshots
Example: `port:"80"`
`has_screenshot:"true"`
* Watch the webcams roll in!

`port:"3389"`
`has_screenshot:"true"`
* Watch for exposed Window domain & users!

Limited Access

There are number of useful operators that require premium paid accounts (Enterprise, Academic, etc)

Vulnerability - Search by CVE ID number
Example: `vuln:"CVE-2017-0143"`

Tags - Search based on Shodan tagged data
Example:
`tag:"ics" or tag:"database"`

Figura 28. Si te pones creativo/a y le dedicas tiempo, este motor puede ser una auténtica mina

💡 Si tras usar Shodan te preguntas como es posible que Internet siga funcionando después de lo que sacas con él, que sepas que yo me hago la misma pregunta a diario



🏃 Seguridad “En el Mundo Real”

👀 Seguridad “Física”

🛠 Ejercicio QR: Escanear un QR con tu teléfono

👤 Descripción de la actividad

Consiste en que entiendas que **no se puede escanear códigos QR que veas por ahí a la ligera**, puesto que pueden esconder una trampa que haga que o te roben datos o te infectes con un *malware*.

🏆 Resultados Esperados

Puedes contestar a las siguientes preguntas:

- ¿Entiendes que escanear un código QR consiste básicamente en decirle a tu teléfono que vaya a una dirección web que está representada por ese código QR?
- ¿Entiendes también que no sabes quién ha puesto ahí ese código QR, y que esa dirección web puede ser lo mismo o algo legítimo que algo malicioso?

📋 Otra información necesaria para su realización

Es necesario que entiendas que ahora que todos los teléfonos móviles tienen integrada la función de escanear códigos QR en su cámara, y que el proceso es más o menos automático, se ha introducido un nuevo riesgo en la sociedad simplemente yendo por la calle, dado que **cada vez se usan más los códigos QR para todo**

Es muy importante que sepas que un código QR no es más que **una imagen que representa un texto**. Ese texto normalmente es la dirección de una página web. Si la persona que ha puesto un código QR en una farola, o pegado en algún sitio, te convence para que lo escanees irás a esa página web. Aquí te pueden pasar dos cosas:

1. Que la página web suplante algo legítimo y te engañe para que des datos privados tuyos, y entonces te los robe (por ejemplo un falso concurso promoción etcétera) (malo)
2. que la página web se aproveche de alguna vulnerabilidad que tengas en tu navegador o tu móvil para descargarse y **ejecutar automáticamente un malware** y entonces te infectes (¡peor!)

Como comprenderás es un poco jugársela escaneando algo desconocido, así que el mejor consejo que se puede dar es **no escanear a la ligera**. Esto el INCIBE lo tiene muy bien especificado en esta infografía



incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD 017 OSi Oficina de Seguridad del Internauta

¿Cómo identifico un QR malicioso?

Si quieres evitar problemas de seguridad:

- 1 No escanees códigos QR a la ligera, solo si tienes una mínima certeza de quién lo ha generado y para qué fin.
- 2 No proporciones información personal o bancaria sin estar seguro de la autenticidad del sitio que visitas.

#OSIconsejo www.incibe.es/ciudadania

Activa la función que permite previsualizar la URL antes de acceder a ella.

SOSPECHA

Si la URL/dirección web a la que te redirige no se corresponde con el nombre de la empresa o servicio al que se supone que vas a acceder.

También si el enlace que esconde el QR se trata de una URL acortada.

O si al escanear el QR te solicita descargar un archivo con extensiones como .apk.

Figura 29. Si el INCIBE se ha molestado en crear una infografía tan detallada es por algo, créeme...

Si quieras saber más información el INCIBE también tiene este apartado que te habla más del tema:
<https://www.incibe.es/node/494006>

🛠 Ejercicio HACKUSB: Leer sobre USBs para “hacking”

💻 Descripción de la actividad

Consiste en que compruebes tú mismo a través de las noticias **como el uso de dispositivos USB maliciosos puede realmente meterte en un auténtico lío** en lo relativo a la seguridad de tu sistema o el de tu organización

🏆 Resultados Esperados

Puedes localizar noticias en las que **un equipo o red de equipos completos se ha visto comprometido por la acción de un USB** especialmente preparado para extender algún tipo de infección o malware, o bien simplemente por tener uno en alguno de sus ficheros y abrirlo en un PC. Puedes contestar a estas preguntas:

- *Has encontrado algún caso en el que el hardware quedase dañado y el equipo inoperable por la acción de un dispositivo USB malicioso?*



- ¿Alguna vez has metido los USB de tus alumnos en tu PC? ¿Volverías a hacerlo ahora teniendo en cuenta que no sabes en cuantos PCs ha estado y lo que tiene dentro?

Otra información necesaria para su realización

El motivo de esta actividad no es otro que compruebes que, aunque suena un poco de ciencia ficción, **esta amenaza es muy real** y por tanto algo a tener muy en cuenta, especialmente si te encuentras con un dispositivo USB tirado por la calle y tienes la tentación de comprobar qué tiene dentro. Créeme si te digo que **es una trampa más común de lo que parece**, y que además amenaza especialmente a empleados de grandes empresas, puesto que es una forma de sacar información de estas casi sin darte cuenta.

Quiero además aprovechar para recordarte **que te mentalices de no usar lápices o discos USBs para la transferencia de archivos entre máquinas desconocidas o aceptar USBs de desconocidos**, porque te estás sometiendo a un enorme riesgo, mayor de lo que crees. Pide que te compartan la información por *email* o por mecanismos para compartir enlaces en servicios de nube y no introducir un dispositivo físico infectado y potencialmente peligroso en tu PC.

- Finalmente, si lo de los lápices con “bicho” no te acaba de convencer, puedes echar un ojo a lo que es un **Rubber Ducky**: <https://shop.hak5.org/products/usb-rubber-ducky>. Aquí te explican lo que es: <https://www.redeszone.net/tutoriales/seguridad/rubber-ducky-ataque-dispositivo/>
- Y si esto no te parece suficiente, mira un **USB Killer**: <https://unaaldia.hispasec.com/2022/11/usb-killer-el-enchufable-que-puede-freir-tu-equipo.html>

 **De verdad, esto va mucho más allá que el clásico “lápiz USB con bicho”, créeme.**





Seguridad Financiera

Ejercicio ESTAFAS: Leer sobre estafas de segunda mano

Descripción de la actividad

Lo cierto es que el mercado de la segunda mano **está plagado de estafas** y que hoy en día vender cualquier cosa en cualquiera de esas tiendas requiere que tengas 1000 ojos y mucho cuidado. Esta actividad pretende que te mentalices de ello.

Resultados Esperados

Puedes contestar a las siguientes preguntas:

- ¿Te has dado cuenta de que los mercados de segunda mano son básicamente un nido de delincuentes tratando de estafar de diferentes formas?
- Por ello, ¿has asumido que en el momento que compres o vendas algo en la segunda mano debes tener muchísimo cuidado con las interacciones que hagas con un posible comprador o vendedor?
- ¿Entiendes que, hagas lo que hagas, no debes nunca dar datos privados a tu interlocutor ni hacerle caso para salir de la plataforma de ventas, haciendo la transacción por WhatsApp (por ejemplo), porque es ahí donde empiezan a hacer las estafas?

Otra información necesaria para su realización

Los mercados de segunda mano son un peligro **tanto en la compra como en la venta**. El número de estafas que existen en estos mercados es tan alto que es muy difícil enumerarlos todas. No obstante **el modus operandi sí que es fácilmente identifiable** y para ayudarte tengo este monográfico que te explica un poco cómo se hacen estas cosas: <https://github.com/jose-r-lopez/Fraudes-y-Timos/blob/main/Case%20Files/T1E33.%20Estafas%20en%20la%20segunda%20mano.pdf?raw=true>