TU GUÍA DE ANDAR POR CASA

Navega y compra de forma segura y asegura tu información digital

Protege ordenadores, smartphones, tablets y redes sociales

CIBERSEGURIDAD en el día a día

Julen Linazasoro

Educación Digital macsonrisas

Capítulo 1

Malware

Una de las principales amenazas que existen es el denominado “malware” o software malicioso antes llamado virus informático. Se ha detectado una evolución en el software malicioso y en los ciberdelincuentes. Hace tiempo, los ciberdelincuentes tenían como objetivo la vulneración de sistemas de seguridad con la motivación de conseguir entrar donde nadie había podido hacerlo antes o de ser “famosos”. Hoy en día los ciberdelincuentes son grupos organizados sin escrúpulos que han descubierto todo un mercado en la venta de información y mucho software malicioso está diseñado exclusivamente para recopilar información.

Una gran diferencia entre el software malicioso de antes y el de ahora es que ahora no siempre necesitan una interacción del usuario para infectar el ordenador o dispositivo. Es decir, antes siempre necesitábamos darle permiso para instalarse en el ordenador, pero ahora, la mayoría de veces no nos damos cuenta porque el malware ya no viene solamente a través de programas que instalamos, también puede venir en un archivo que abrimos o una imagen que descargamos.

Stegware: Desde hace un par de años, los ciberdelincuentes han conseguido añadir código malicioso dentro de imágenes y audios. A partir de ahora debemos tener cuidado con las imágenes y audios que nos llegan, y si no sabemos quién los ha creado o de dónde han salido, no se recomienda compartirlos ya que podríamos poner en riesgo a nuestros contactos.

Ransomware: Su misión es bloquear el ordenador, cifrar archivos y pedir rescates para que podamos recuperar nuestra información. Viene en forma de troyano, en archivos adjuntos o aplicaciones gratuitas. El más famoso es “el virus de la policía”.

Básicamente lo que hacia “el virus de la policía” es que de repente el ordenador se bloqueaba y aparecía un mensaje de la policía en la pantalla diciendo que el ordenador había sido bloqueado porque habíamos infringido la ley, y que para desbloquearlo había que pagar la multa correspondiente. Claro, aquí cada uno

empezaba a pensar si había descargado películas, canciones, aplicaciones pirata, visto películas online... un montón de posibilidades de haber infringido la ley, con lo que muchos usuarios pagaban la multa que no era muy elevada. Evidentemente el mensaje no era de la policía y los ciberdelincuentes ganaron mucho dinero.

Spyware: Su misión es espiarnos, recopilar toda la información que pueda y mandársela a su dueño. Viene en archivos adjuntos o aplicaciones gratuitas. A veces modifica los navegadores instalando automáticamente herramientas propias en la barra de herramientas del navegador y modificando el buscador. A veces obtienen control de la webcam, viendo a través de ella cuando estamos desprevenidos o grabando lo que hacemos con el objetivo de extorsionarnos.

Rogueware: Se hace pasar por un antivirus. Su misión es infectar el ordenador para que compremos productos o servicios para desinfectarlo. De repente vemos un mensaje en internet de un antivirus que simula escanear el ordenador y nos dice que nuestro ordenador va lento, que descarguemos el programa para mejorar su velocidad. Es muy importante entender que una página web no puede escanear nuestro ordenador o dispositivo.

Cuando descargamos el programa lo que hace es ralentizar realmente el ordenador para vendernos soluciones y productos. También viene en aplicaciones gratuitas (códecs...) y en descargas de archivos de internet.

Troyano: No es lo que parece ser. Su misión es engañarte para que lo instales en el ordenador, y así se pueda hacerse con su control. Cuando un ciberdelincuente tiene muchos ordenadores controlados crea lo que se llaman “botnets”, redes de ordenadores a través de las cuales delinquen de diferentes formas.

Una de ellas es utilizar nuestro ordenador para realizar ataques de denegación de servicios o ataques DDoS, que básicamente es que los ciberdelincuentes utilizan un montón de ordenadores comprometidos como el nuestro para intentar entrar en una página web determinada, con lo que la página web “se bloquea” y no ofrece el servicio, los verdadero usuarios no pueden entrar. Puede venir disfrazado en programas gratuitos.

Este tipo de malware también controla nuestros dispositivos para hacer cosas sin que nos enteremos: Hacer clic en anuncios de diferentes páginas, mandar más malware o extorsionar a otras personas, visitar páginas ilegales y guardar información ilegal en nuestros dispositivos...

Cryptomining: Su misión es utilizar los recursos de nuestros dispositivos (electricidad, potencia...) para minar o crear criptomonedas (bitcoins…). De repente empezamos a notar que nuestros dispositivos van más despacio, que la batería se acaba pronto, internet va más lento... Al utilizar nuestros recursos de una manera tan brutal puede que nuestros dispositivos se sobre calienten o se estropeen.

Bankers: Su misión es recopilar información bancaria. Generalmente actúan contra empresas. Después de estudiar a las víctimas crean una página falsa del banco con el que trabaja la víctima y le redirigen allí cuando esta quiere acceder a su banco de forma online. Al meter su información de acceso en la página falsa se la regala a los ciberdelincuentes.

Dentro de la página falsa crean movimientos ficticios indicando que por ejemplo tienen un saldo de -3.000€ y muestran un teléfono de ayuda. Al llamar a ese teléfono los ciberdelincuentes logran sacar toda la información privada: “Para verificar que es usted dígame cuál es su clave de firma, su tarjeta de crédito…”.

Adware: El adware como tal no está catalogado como malware pero roza la ilegalidad. Son programas que están constantemente mostrándonos anuncios. Se hacen dueños de los navegadores, cambian los buscadores y cada vez que buscamos algo en internet empiezan a mostrarnos tal cantidad de anuncios que a veces hacen imposible la navegación. Vienen en programas gratuitos.

En los smartphones tienen una variante llamada Hiddad (Hidden adware) cuyo nombre viene porque el programa que genera ese comportamiento se esconde y no lo podemos encontrar.

¿Cómo consiguen propagarse y cumplir sus misiones?

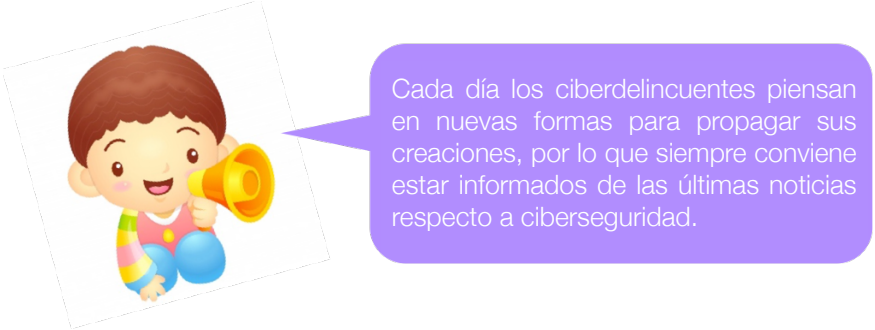
El malware suele propagarse a través de las descargas de archivos, a través de links, a través de correos electrónicos y archivos adjuntos, a través de las redes Wifi…

Descargas: Podemos encontrar malware en descargas de ficheros o programas. En este país se ha creado la cultura de conseguir todo gratis, creemos que tenemos derecho de tener todo lo que queramos gratis por lo que si no podemos pagar algo que nos interesa lo "pirateamos", es decir, lo conseguimos de forma ilícita, y aunque lo podamos pagar también lo hacemos porque "¿Para qué pagar algo que puedo tener gratis?".

Los ciberdelincuentes se aprovechan de esta visión y la mayoría de descargas suelen tener software malicioso, ya sean películas, canciones o programas. Muchas aplicaciones gratuitas también contienen software malicioso con lo que hay que tener cuidado de donde se descargan. Siempre conviene hacerlo desde tiendas oficiales o páginas de los desarrolladores.

Archivos adjuntos: Hoy en día recibimos muchos mails fraudulentos con archivos infectados. Los veremos más detenidamente en el capítulo de Ingeniería social, pero en resumen son mails de desconocidos que se inventan cualquier cosa para que tengamos curiosidad y abramos el archivo adjunto que nos han enviado.

Apps de mensajería y redes sociales: Las apps de mensajería y las redes sociales se han convertido en una herramienta de comunicación muy utilizada entre todos, y los ciberdelincuentes también se aprovechan de eso para intentar propagar sus creaciones.



Es muy habitual mandar y reenviar imágenes por Whats App que nos parecen divertidas pero que no sabemos de dónde vienen y no somos conscientes de que ya hay malware que se propaga a través de fotos, y que al guardar esa foto que nos ha llegado en nuestro teléfono ya la hemos liado.

Se están viendo “bulos” que nos llevan a descargar apps maliciosas, imágenes que contienen malware y que todos compartimos de forma inconsciente porque son graciosas o bonitas, cadenas de mensajes con links maliciosos…

Links o enlaces: Otra de las formas en las que podemos resultar infectados es a través de links, enlaces. No sabemos lo que puede pasar al pinchar en un enlace. Puede ser que nos lleve a una página legítima, puede ser que nos lleve a una página fraudulenta, puede ser que al pinchar descarguemos un archivo infectado... Por eso debemos prestar atención en dónde pinchamos.

Muchos links maliciosos pueden venir a través de anuncios. Vemos un anuncio que nos interesa y clicamos sin pensarlo dos veces.

Otras veces estamos navegando por internet, queremos ver un video legítimo o una película “pirata” online y en la página en cuestión aparece un mensaje diciendo que tenemos que actualizar el reproductor para poder ver el contenido. Al pinchar para actualizar el reproductor ya estamos descargando “cositas”.

Estos links también los podemos encontrar en las redes sociales o en los mails. Mucha gente comparte cosas muy alegremente cuya procedencia desconoce, sin pensar en que eso puede tener graves consecuencias.

Hay páginas web concretas, que debido a la afluencia de visitantes, son más propensas a que ciberdelincuentes las intenten utilizar para poder propagar su software malicioso. Estas páginas son páginas para ver películas y series online, páginas para adultos, páginas de juego online... En el caso de visitar este tipo de páginas se recomienda aumentar las precauciones ya que tenemos más probabilidades de resultar infectados.

Wifi: Las redes wifi se han convertido en un elemento más de nuestro día a día, pero debemos utilizarlas con cautela ya que nos pueden traer más de un quebradero de cabeza.

Debemos ser extremadamente cautelosos al usar redes wifi públicas. Las redes wifi públicas son aquellas que no tienen contraseña, a las que

cualquiera se puede conectar. Precisamente por eso, porque cualquiera se puede conectar, son peligrosas, ya que ciberdelincuentes podrían estar monitorizando todo lo que hacemos y recopilando datos. Además, hay software malicioso que puede propagarse a otro equipo si comparten la misma red wifi simultáneamente.

También tendremos cuidado cuando nos conectemos a una red wifi privada de un lugar público. Por ejemplo, una red wifi de un restaurante puede estar protegida por una contraseña, pero puede haber mucha gente conectada a la vez.

Anuncios: Los anuncios online son una forma de distribuir malware cada vez más utilizada, ya que en la propia naturaleza de los anuncios está el llegar al mayor público posible. Los ciberdelincuentes aprovechan estas estructuras para distribuir sus creaciones. Además, es posible insertar este tipo de anuncios en páginas web fiables, con buena reputación y cientos de miles o millones de visitantes, donde los usuarios suelen bajar la guardia ya que entienden que se encuentran en un entorno online seguro. Y también es posible insertar estos anuncios sin comprometer directamente esas páginas web, de modo que es más difícil detectar el código malicioso porque la página web en sí permanece inalterada lo que hacer creer a los administradores que todo está bien y permite que el malware continúe distribuyéndose.

Este tipo de ataques están en aumento a una velocidad vertiginosa, según un informe de la empresa de ciberseguridad Cyphort, este tipo de anuncios maliciosos aumentaron un 325% en 2015. Hay páginas muy conocidas con millones de usuarios que han sufrido este tipo de ataques, dos ejemplos pueden ser The Financial Times o Spotify.

¿Cómo funcionan este tipo de anuncios?

Generalmente, los cibercriminales envían anuncios “limpios” para generar confianza. Luego inyectan código malicioso (malware) en el código del anuncio, y después de una infección masiva de usuarios, retiran el código malicioso del anuncio.

Este tipo de ataques es muy peligroso porque no requiere de ningún tipo de interacción por parte del usuario. Hasta hace poco, los anuncios maliciosos tradicionales eran links que al pinchar encima nos redirigían a otras páginas, y los ciberdelincuentes aprovechaban para redirigir a los usuarios a páginas fraudulentas donde nos intentaban engañar de diferentes formas para que hiciéramos click sobre un enlace que nos descargaba el malware, o directamente el virus se

descargaba al pinchar en el link o al llegar a la página fraudulenta. Pero ahora, cuando la página donde está el “anuncio malicioso” se carga, el malware (virus) se autoejecuta y se descarga sin que el usuario tenga que hacer nada, solamente visitar la página.

¿Cómo me puedo proteger?

Descargas

Evitaremos las descargas de archivos como películas, canciones y programas "pirata". Tampoco se aconseja el uso de páginas para ver películas o series online gratis o hacerlo con cautela porque esas páginas web, al tener gran número de visitas, son objetivos habituales de ciberdelincuentes.

Hay diferentes servicios online que por una pequeña cantidad al mes (que ronda de 7 a 18 euros) nos permiten acceder a contenido multimedia como películas, series o música como Netflix, HBO, Spotify o Deezer. La mayoría de cadenas de TV también nos ofrecen la opción de acceder a los contenidos que emiten a través de sus páginas web correspondientes.

Se recomienda descargar aplicaciones únicamente desde las tiendas oficiales o desde las páginas de los desarrolladores de las aplicaciones.
Si las aplicaciones que queremos no se encuentran en estas tiendas, iremos a la página web del desarrollador del producto. Por ejemplo, si quiero la app Skype para el ordenador, iré a la web www.skype.com, para VLC www.videolan.org y así sucesivamente.

Protección de navegadores

Cuando usamos ordenadores para acceder a internet, los navegadores suelen tener diferentes complementos o extensiones que podemos usar para protegernos. Son pequeños programas que les ofrecen funciones adicionales, y algunas de ellas nos ayudan a navegar de forma más segura. Las más recomendadas son Adblock y Traffic Light.

Adblock es una extensión cuya función es evitar la aparición de publicidad. Se agradece bastante, ya que cada vez más, la publicidad es más intrusiva y a veces desagradable. También nos aseguramos de que no van a aparecer links sospechosos, y con ello vamos a reducir la posibilidad de introducir cosas en el ordenador que no son aconsejables.

Traffic Light nos indica si alguna página es fraudulenta, con lo que es una medida más de protección contra el Phishing y también analiza los links de las páginas webs. Además, no ralentiza la velocidad de navegación.

Video protege navegadores

Emails

- Debemos ser cautelosos con los mails que decidimos abrir, y también con los archivos adjuntos que contienen esos mails. Algunas pautas para detectar mails maliciosos son las siguientes.

- Prestar atención al remitente del mail, quién lo envía. Una cosa es el nombre que aparece cuando leemos el mail y otra cosa es la dirección que realmente lo envía. Debemos mirar siempre la dirección desde la que se envía clicando encima del remitente.

- Debemos prestar atención a la redacción del mail. Muchos mails maliciosos suelen tener fallos ortográficos y suelen estar mal redactados.

- Los mails maliciosos suelen tener destinatarios generales ya que son enviados de forma masiva. Es decir, en vez de decir “Hola María, ¿qué tal?”, suelen decir “Hola, ¿qué tal?”. O “te mando esto” en vez de “te mando el trabajo de física del que hemos hablado antes”…

- Aunque el remitente sea un contacto debemos fijarnos en el contenido del mail, ya que muchas veces cuando alguien es infectado, el virus se auto envía a los contactos de esa persona.

- Evitaremos las cadenas de mensajes en general. Los ciberdelincuentes se aprovechan mucho de esto, y empiezan a generar cadenas del tipo “Este niño tiene cáncer terminal, pincha aquí para apoyarle”, “Necesitamos tu ayuda después de que el tifón haya asolado este país”, “manda este mensaje a 20 personas para apoyar no se qué”…

- Debemos ser extremadamente precavidos con los archivos adjuntos cuya procedencia desconocemos. Los ciberdelincuentes aprovechan cualquier situación para engañarnos: Durante el confinamiento de 2020 se detectaron emails fraudulentos que decían tener la cura para el Covid-19, o emails que supuestamente vendían tests baratos, emails falsos que en archivos adjuntos supuestamente indicaban qué había que hacer para cobrar los ERTEs…

- Al detectar un mail sospechoso que no esperamos, lo mejor es borrarlo.

Ejemplos de mails sospechosos:

AgenciaTributaria
Agencia Tributaria - Recordatorio de pago
Para: info@macsonrisas.es

EJEMPLOS 16 de septiembre de 2019, 10:17

Agencia Tributaria

PROVIDENCIA DE APREMIO - RECORDATORIO DE PAGO

Notificaci&#65533;n de Impuestos

Estimado contribuyente,

Se han detectado irregularidades en su declaraci&#65533;n jurata de Renta correspondiente al 2018. Adjunto a este mensaje va su factura con la deferencia que debe abonar. En caso de no realizar el pago en fecha puede incurrir en cargos y multas extras.

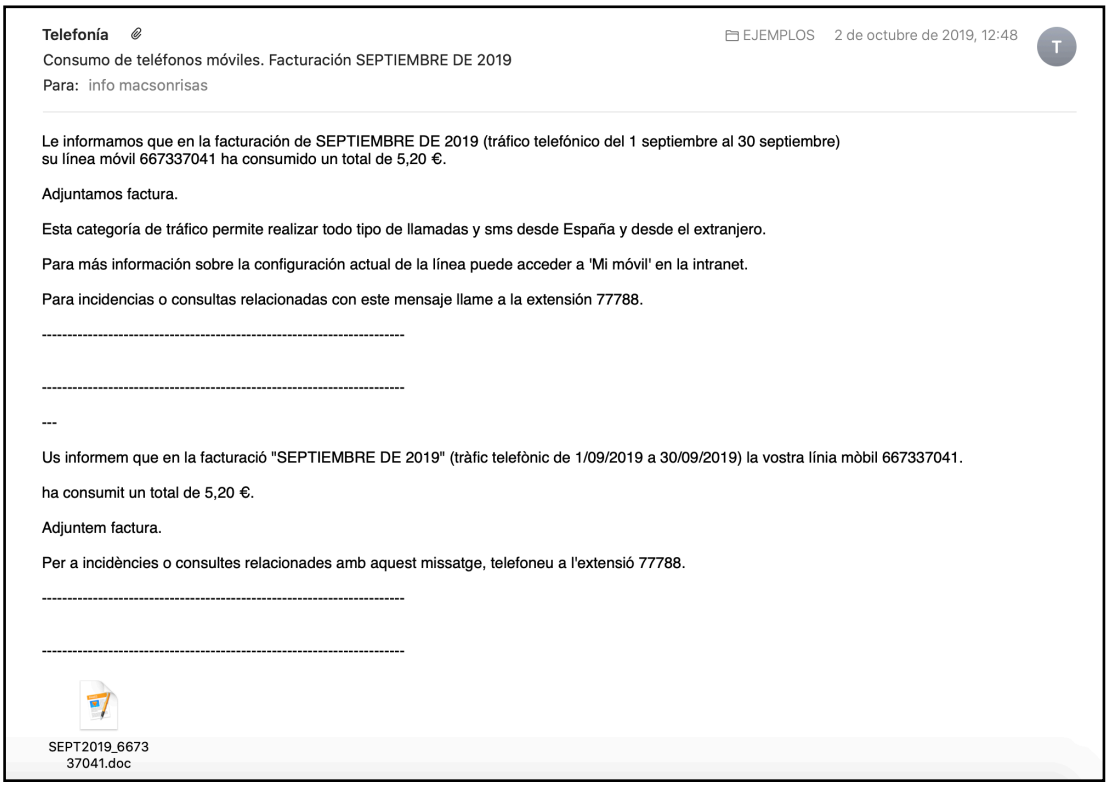
PDF Descargar Factura
Protegido por Avast Antivirus

Que tenga un buen d&#65533;a!

Documento de referencia: (9134483)
Agencia Tribunaria

Email suplantando a Hacienda

Si descargamos la factura que nos indican el archivo viene infectado.



Telefonía
Consumo de teléfonos móviles. Facturación SEPTIEMBRE DE 2019
Para: info macsonrisas

EJEMPLOS 2 de octubre de 2019, 12:48

Le informamos que en la facturación de SEPTIEMBRE DE 2019 (tráfico telefónico del 1 septiembre al 30 septiembre) su línea móvil 667337041 ha consumido un total de 5,20 €.

Adjuntamos factura.

Esta categoría de tráfico permite realizar todo tipo de llamadas y sms desde España y desde el extranjero.

Para más información sobre la configuración actual de la línea puede acceder a 'Mi móvil' en la intranet.

Para incidencias o consultas relacionadas con este mensaje llame a la extensión 77788.

Us informem que en la facturació "SEPTIEMBRE DE 2019" (tràfic telefònic de 1/09/2019 a 30/09/2019) la vostra línia mòbil 667337041.

ha consumit un total de 5,20 €.

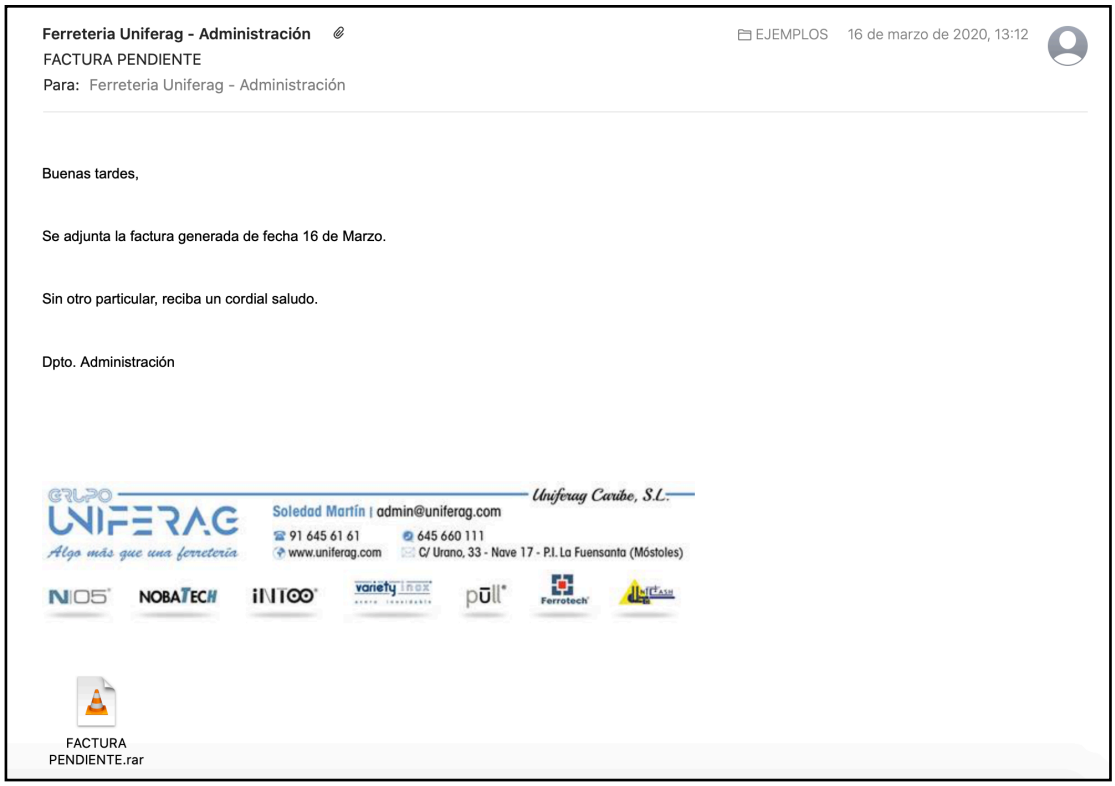
Adjuntem factura.

Per a incidències o consultes relacionades amb aquest missatge, telefoneu a l'extensió 77788.

SEPT2019_667337041.doc

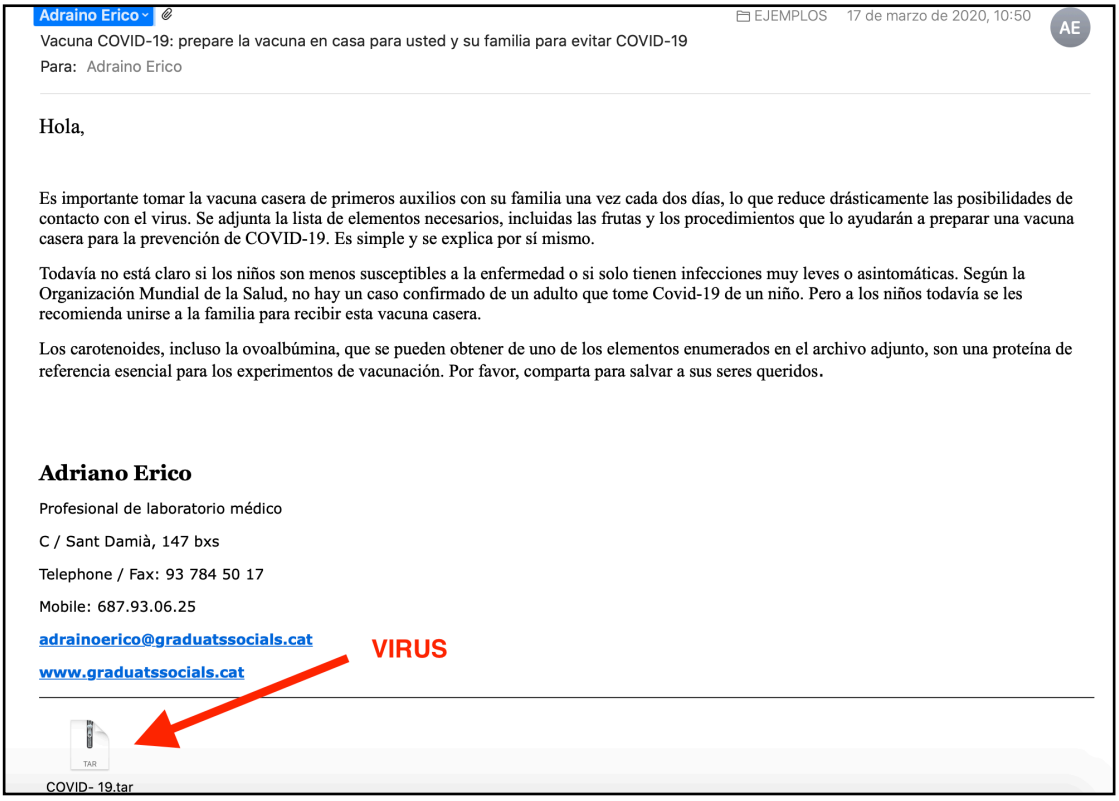
Virus en archivo adjunto

Intentan generarnos curiosidad para que pinchemos en su archivo e infectemos nuestros dispositivos diciendo que nos mandan una factura.



Adjunto infectado

Otro intento de estafas a través de supuestas facturas.



Email falso coronavirus

Aprovechando la pamdemia se hacen pasar por sanitarios para que abramos su archivo en el que supuestamente viene la receta crear la vacuna.

Apps de mensajería

Las pautas para evitar ser infectados a través de emails se aplican también para evitar ser infectados a través de apps de mensajería en teléfonos móviles y tablets. Evitaremos compartir imágenes y mensajes cuyo origen desconocemos, así como cadenas de mensajes.

Además no haremos caso de rumores que nos incitan a descargar apps de fuera de las tiendas oficiales. Hay casos muy conocidos de diferentes tipos de malware que se instalaban en dispositivos a través de falsos programas o links que aseguraban poder ver cuanta gente visita el perfil de twitter o tener funciones adicionales en Whats App, entre otras.

También usaremos el sentido común no usando los enlaces que nos llegan en mensajes desde números desconocidos ni responderemos mensajes de desconocidos, a veces simplemente por hacerlo nos suscribimos a un servicio de mensajería premium.

Wifi

Evitaremos conectarnos a redes Wifis públicas, aquellas que no están protegidas por una contraseña ya que cualquiera puede ver lo que enviamos o recibimos a través de programas llamados Sniffers (también en redes privadas donde hay mucha gente conectada), y los creadores de esas redes también pueden ver el contenido de los dispositivos conectados.

Si nos urge consultar algo, al estar conectados no nos loguearemos, es decir, no introduciremos el nombre de usuario y contraseña de ningún servicio: Correo electrónico, redes sociales, servicios financieros...

Apagaremos los servicios de sincronización que tengamos activados, ya que al sincronizarse datos pueden quedar expuestos: Programas como Dropbox, Google Drive, iCloud…

También andaremos con precaución y evitaremos loguearnos cuando estemos conectados a redes Wifis privadas de sitios públicos en las que más personas puedan estar conectadas, como cafeterías, bibliotecas, hoteles...

En casa, siempre cambiaremos la contraseña de la red wifi que genera el router. Las contraseñas que vienen por defecto son públicas, eso quiere decir que cualquiera con un mínimo conocimiento podría conectarse a la red y usarla, ver lo que enviamos y recibimos e incluso ver el contenido de nuestros dispositivos. La oficina de seguridad del internauta (www.osi.es) tiene un servicio que detecta si la red wifi a la que estamos conectados forma parte de una botnet o no.

Terminología

Aunque en nuestro nivel de usuarios normales es muy difícil entender conceptos informáticos avanzados, simplemente con el objetivo de que cuando los escuchemos sepamos más o menos de lo que están hablando, vamos a ver algunas de las formas de ataques a servidores, sistemas de seguridad y páginas web que existen:

APT: Amenaza Persistente Avanzada, en inglés Advanced Persistant Threat. Una APT es un conjunto de ataques informáticos sigilosos y continuados en el tiempo con el objetivo de explotar puntos débiles en los sistemas utilizando malware. Sus objetivos son organizaciones, empresas o naciones. El fin de estos ataques es colocar código personalizado malicioso en uno o varios ordenadores para tareas específicas, como el espionaje, y para no ser detectados durante el período más largo posible.

Una APT generalmente involucra a un grupo organizado, tanto con la capacidad como con la intención de dirigirse de forma persistente y eficaz contra una entidad específica.

Ataques de fuerza bruta: Es una forma de descifrar o “adivinar” una contraseña para entrar a un servicio protegido. En un ataque de fuerza bruta se usa software automatizado para ir generando un gran número de diferentes intentos de combinaciones hasta dar con la contraseña correcta.

Ataques Día 0 (0 Day): Es un tipo de ataque que se caracteriza por infectar equipos informáticos con código malicioso aprovechando vulnerabilidades desconocidas por los creadores y los usuarios de las aplicaciones. Es muy grave porque como no habían sido descubiertas, aún no existen soluciones.

Ataque DDoS o denegación de servicios: Un ataque DDoS tiene como objetivo que una red o servidor deje de estar disponible. Es un ataque que

intenta interrumpir un servicio online temporal o indefinidamente. Este tipo de ataque consiste en que un grupo de sistemas comprometidos (también conocidos como “ordenadores zombie” que pueden pertenecer a una Botnet) atacan a un solo objetivo para causar una denegación de servicios a los usuarios que sí son legítimos.

Se crea una enorme cantidad de solicitudes que se envían al objetivo para que este se sobrecargue y sea forzado a cerrarse. Como resultado se le niega el servicio a los verdaderos usuarios.

Cookies: Las cookies son pequeños archivos que se guardan en nuestro ordenador o dispositivo cuando navegamos por internet y que almacenan información sobre los sitios que visitamos, preferencias y otra información personal.
La utilidad de las cookies es facilitar la navegación, por ejemplo recordando nuestra identificación y preferencias para que no tengamos que volver a introducirlas la siguiente vez que visitamos una página.

Para que no resulten peligrosas, las cookies deben cumplir una serie de características como por ejemplo, almacenar sólo texto ya que el problema fundamental de las cookies para la privacidad es la posibilidad de almacenar cualquier tipo de información. Esto, junto a que las cookies se instalan de forma automática en el ordenador o dispositivo del usuario, puede fomentar que algunas organizaciones las quieran usar para la recolección de datos personales.

Conociendo toda esta información, diferentes empresas nos pueden ofrecer productos que nos interesan mientras navegamos por internet, pueden almacenar esa información para crear campañas publicitarias, o incluso pueden vender esa información a otros.

¿Por qué es importante cerrar sesión de los servicios online al terminar?

Todos los servicios online requieren que iniciemos sesión para poder utilizarlos introduciendo nuestro nombre de usuario y contraseña. De la misma forma todos los servicio online requieren que salgamos de las sesión después de utilizarlos.

Cuando pinchamos en ese botón (cerrar sesión), se le ordena al navegador que borre la cookie de la sesión que acabamos de realizar. Una vez que esa cookie es borrada, el navegador ya no recuerda la sesión que acabamos de tener. Pero a veces se nos olvida cerrar la sesión y cuando volvemos, automáticamente

volvemos a la sesión que habíamos iniciado, entramos en nuestra cuenta sin meter nuestro nombre de usuario y nuestra contraseña, ya que no habíamos cerrado la sesión. Esto puede provocar que alguien que esté cerca de ese ordenador pueda acceder a toda nuestra información de ese servicio online, o copiar las cookies y consultar toda esa información más tarde. Algunas páginas web cierran la sesión en curso al cerrar el navegador, pero otras no.

El Spyware u otro tipo de malware (software malicioso) también puede acceder de forma remota a esas cookies y puede mandar toda esa información a cibercriminales. Las cookies generalmente no están protegidas por lo que es muy fácil recoger la información que guardan.

¿Puede alguien saber todo lo que hago en internet?

Sí. Nuestros proveedores de servicios de internet (ISP) llevan un registro de todo lo que hacemos, ya que todo nuestro tráfico, la información que consultamos o subimos, pasa a través de sus servidores. Como las empresas privadas no tienen acceso a esos registros, lo que hacen para saber qué paginas visitamos, cuales son nuestros gustos… es estar presentes en todas las páginas web que pueden a través de anuncios, botones para compartir o widgets de redes sociales. De esta forma consiguen poner código propio en las páginas que visitamos. Así, sólo tienen que ir leyendo las cookies de nuestro navegador para recopilar la información almacenada y añadir la página que estamos visitando a sus registros.

Casi todos los navegadores tienen herramientas que permiten desactivar o eliminar cookies. Generalmente podemos elegir entre aceptar siempre las cookies, no aceptarlas nunca o aceptar solo aquellas de los sitios web que visitamos. Además, podemos eliminar cuando queramos las cookies de los lugares que hemos ido visitando desde las preferencias de los navegadores. Se recomienda aceptar solo aquellas de las paginas web que visitamos y de vez en cuando borrarlas todas y “empezar de cero”.

Capítulo 2
Antivirus

Hoy en día desgraciadamente se hace imprescindible el uso de un antivirus tanto en ordenadores como en nuestros dispositivos móviles.

La información es poder, y el malware está diseñado para espiar y robar información de todo aquello que sea digital.

Todos los sistemas operativos Mac, Windows y Linux son objetivos de ataques cibernéticos y en el ámbito de los dispositivos móviles no se libra ningún sistema, ni iOS ni Android. En el sistema operativo del iPhone no se recomienda hacer el Jailbreak, ya que elimina de un plumazo toda su seguridad. Si no sabes lo que es no te preocupes, mejor.

Características de los antivirus

Las caracteristicas en los que nos tenemos que fijar a la hora de instalar un antivirus que nos ayude y proteja son:

- Detección en tiempo real, es decir, que el antivirus sea capaz de detectar el software malicioso en el momento de introducirse en el sistema y elimine la amenaza ipso facto.

- La capacidad de extracción y eliminación del software malicioso, cuanto más capacidad y más rápida mejor.

- La sencillez a la hora de utilizarlo.

- El soporte técnico. Es muy importante asegurarnos de que la empresa que nos presta el servicio tenga un buen soporte técnico en el idioma que deseamos, disponibilidad horaria, que el teléfono al que haya que llamar no sea de pago...

- Detección de intentos de phishing y correos Spam. Esta opción aumenta los servicios de seguridad que nos ofrecen.

- Protección cuando navegamos por internet. La tranquilidad a la hora de navegar no tiene precio.

Los antivirus tienen como media un coste de 40€ anuales y merece la pena pagar por nuestra protección. También ofrecen licencias para dispositivos móviles. Los ataques a dispositivos Android, sobre todo a móviles, son cada vez más habituales.

¿Cómo funciona un antivirus?

Los antivirus utilizan diferentes técnicas para detectar malware en nuestros dispositivos, estas son las más comunes:

Firma digital

Los programas antivirus van comprobando constantemente cada archivo del sistema (escaneo en segundo plano o detección a tiempo real), especialmente archivos recién descargados de Internet o de correos electrónicos, y comparan el código de cada archivo con un una base de datos que tienen donde están todos los códigos de malware conocidos hasta esa fecha. En esta base de datos están las “firmas” de los virus o “vacunas” donde se describe al detalle el código de cada virus.

Si un trozo del código de un archivo concuerda con código de malware conocido, el antivirus puede realizar varias acciones: Puede desinfectar el archivo (el antivirus reescribe su código siguiendo la información contenida en las “firmas” o “vacunas” para eliminar el virus sin perder la información); el programa también puede poner ese archivo detectado en cuarentena si no sabe qué hacer con él (dejarlo a parte sin acceso a ningún programa hasta que el antivirus encuentre una solución para su desinfección); el programa puede eliminar el archivo cuando considera que no queda otra solución.

Para que los antivirus funcionen al 100%, las base de datos de virus deben ser actualizadas cada poco tiempo, ya que solamente pueden detectar el malware cuya “firma” posean.

Aunque estas comprobaciones son muy efectivas, los creadores de malware siempre intentan estar un paso por delante creando “virus polimórficos” que encriptan parte de su código o se modifican a sí mismos para que no puedan ser identificados en las bases de datos de los antivirus. Un ejemplo de este tipo de malware es el recientemente descubierto “Cerber", que mutaba

cada 15 segundos para evitar ser detectado.

Detección heurística

El análisis heurístico tiene un comportamiento basado en reglas para diagnosticar si un archivo es potencialmente peligroso. Busca secciones de código maliciosas conocidas que se encuentren dentro de los archivos sospechosos. Si encuentra una de estas secciones, el programa le asigna una probabilidad de peligro basándose en el número de veces que ese código ha aparecido en muestras de malware que ya están confirmadas. Este técnica ayuda a detectar los “virus polimórficos”.

Revisiones de “comportamientos sospechosos”

Estas revisiones consisten en encontrar modificaciones o comportamientos en archivos poco habituales producidos por malware, como puede ser la escritura en archivos ejecutables. Estas revisiones pueden detectar malware que aún no están en ninguna base de datos. Es posible que el antivirus se equivoque algunas veces y confunda ciertos programas legítimos con malware. A este error se le llama Falso Positivo.

Ejecución controlada en sandbox

Se ejecuta el programa o archivo sospechoso en un entorno controlado. Al acabar la prueba, el entorno es analizado en busca de cambios que puedan indicar la presencia de malware.

¿Cuál es el mejor antivirus?

Diferentes programas antivirus tienen diferentes ratios de detección de malware realizados por las dos tipos de revisiones principales, las definiciones de virus (firmas digitales) y los comportamientos. Algunas empresas puede que tengan las revisiones de comportamientos más efectivas, con lo que aumentan su ratio de detección, pero estos ratios suelen cambiar con el tiempo, no existe ningún

antivirus que sea mejor que otro durante mucho tiempo. Si queremos saber cómo de efectivo es un programa antivirus debemos fijarnos en los ratios de detección. Actualmente, las grandes marcas de antivirus tienen una efectividad parecida: Norton, Avira, Avast, Eset, Panda, Bitdefender, Kaspersky…

Antivirus gratuito vs Antivirus de pago

ANTIVIRUS GRATUITO	ANTIVIRUS DE PAGO
Muestra publicidad	No muestra publicidad, ya lo hemos pagado
Venden datos de uso a terceras empresas: historial de búsqueda en red, el historial del navegador…	No necesita vender datos, ya lo hemos pagado
Consume más recursos, puede que provoque lentitud	Consume menos recursos
Protección básica, protege contra malware	“Suite de seguridad”: Protección web, protección mail…
No tiene servicio de atención al cliente	Tiene servicio de atención al cliente

Recursos públicos

Incibe es el Instituto de Ciberseguridad de España que y en su página web cuenta con un montón de recursos para empresas en materia de ciberseguridad.

Su equivalente para particulares es OSI, la Oficina de Seguridad del Internauta donde podemos encontrar un montón de información como avisos de seguridad, artículos sobre ciberseguridad, recursos para identificar fraudes, para proteger nuestros dispositivos, soporte técnico, juegos educativos...

Capítulo 3
Ingeniería social

La Ingeniería Social es una forma de intentar engañarnos para que a través de diferentes medios ofrezcamos nuestros datos privados ciberdelincuentes. Estos datos pueden ser nombres de usuarios y contraseñas de diferentes servicios, datos financieros como números de cuentas, números y códigos de tarjetas, accesos a nuestros dispositivos, datos sanitarios...

En este libro nos vamos a centrar en las tres más habituales que son el Phishing, el Spam, sus derivados y el fraude.

Phishing

Los ataques de Phishing están diseñados para robar o “pescar” detalles de inicio de sesión y contraseñas de redes sociales, correos electrónicos y diferentes servicios online entre los que se encuentran los financieros.

Este tipo de ataques se dan principalmente a través de correos electrónicos y apps de mensajería.

Se habla de Spam cuando un ciberdelincuente envía correos electrónicos diseñados para que una víctima gaste dinero en productos falsificados o falsos.

¿Cómo podemos detectar este tipo de ataques?

Para detectar este tipo de ataques, debemos prestar atención a los siguientes puntos:

1. ***Dirección del remitente:*** Esta es la pauta más importante. Debemos fijarnos en quién envía el mail. Pueden ser diferentes el nombre que aparece en el remitente cuando leemos el mail y la dirección que realmente lo envía cuando pinchamos encima de ese remitente. Debemos mirar siempre la dirección desde la que se envía. Si la dirección de email no contiene el nombre de la empresa que dice mandar el mail, es un correo electrónico no fiable. Por ejemplo, una dirección real de iTunes es: do_not_reply@itunes.com. Por tanto, aunque el nombre del remitente sea iTunes, si el email es info@informatica.es, se trata de un caso de Phishing (ver ejemplos a continuación).

2. ***Dirección del destinatario:*** Muchas personas disponen de varias cuentas de correo electrónico. Si recibimos un correo electrónico de esas características a una dirección que no utilizamos para acceder a ese servicio, o que no hemos proporcionado, es un intento de Phishing.

3. ***Saludo general:*** Los mails profesionales suelen estar personalizados con el nombre del destinatario. Hay que sospechar de emails que empiecen por ‘Estimado cliente’ o ‘Estimado usuario’. Los profesionales suelen empezar con “Estimada Maria” o “Estimado Juan”.

4. *Errores gramaticales o de ortografía:* Un mail de una empresa seria nunca tendrá fallos ortográficos o gramaticales. Muchas veces este tipo de mails se escriben en un idioma y se traducen literalmente a otros por lo que aunque no tengan fallos ortográficos o gramaticales a veces pueden estar redactados incorrectamente.

5. *Divisas incorrectas:* En algunos tipos de Phishing, el error suele estar en el tipo de divisa que aparece. Si hemos realizado una compra en euros y el mensaje nos muestra el precio de un servicio en dólares, debemos sospechar.

6. *Urgencia:* Las empresas nunca van a "amenazarnos" con borrar o desactivar una cuenta. De hecho, su objetivo es tener nuevos clientes, no perder los que ya tienen.

7. *Links (Enlaces):* Un ataque de Phishing contiene generalmente un enlace en el que el nombre de la empresa que dice mandar el mail no coincide con el mostrado en el link. Otras veces, el nombre de la empresa coincide con el mostrado en el link, pero si mantenemos el cursor encima de ese link, veremos que la página a la que lleva no coincide con la que dice el link (ver ejemplos a continuación).

8. *Archivos adjuntos:* Debemos ser muy cuidadosos con los archivos adjuntos. Una empresa nunca nos va a pedir que rellenemos datos personales a través de un documento word, a no ser que previamente nos hayan avisado por teléfono. Es mucho más fácil hacerlo con formularios online.

Nunca debemos abrir archivos adjuntos en emails de desconocidos que no esperemos. Si por ejemplo nos hemos apuntado a un curso y estamos esperando un email con información, datos de acceso... al recibir el email de una dirección desconocida no habrá problema, siempre que esté relacionado con aquello que estábamos esperando.

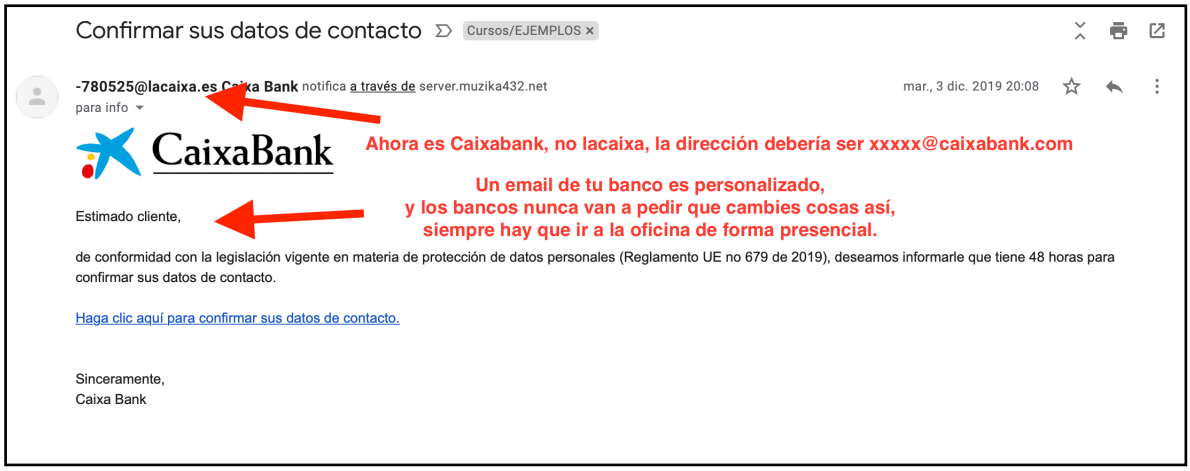
Curiosidad: Los mails de Phishing van evolucionando con el tiempo y hay correos y páginas que obviamente son de Phishing y otras que no lo son tanto. Pues bien, según Google Security Blog, un 3% de los usuarios pican en páginas obvias de phishing, un 14% pica en páginas no tan obvias y un 45% de los usuarios hacen clic en páginas creíbles de phishing. De ese 45% que pica, un 14% rellena los formularios y un 4% es finalmente estafado.

Al 20% de las cuentas robadas se accede en 20 minutos, y los ciberdelincuentes pasan una media de 30 minutos en cada cuenta robada.

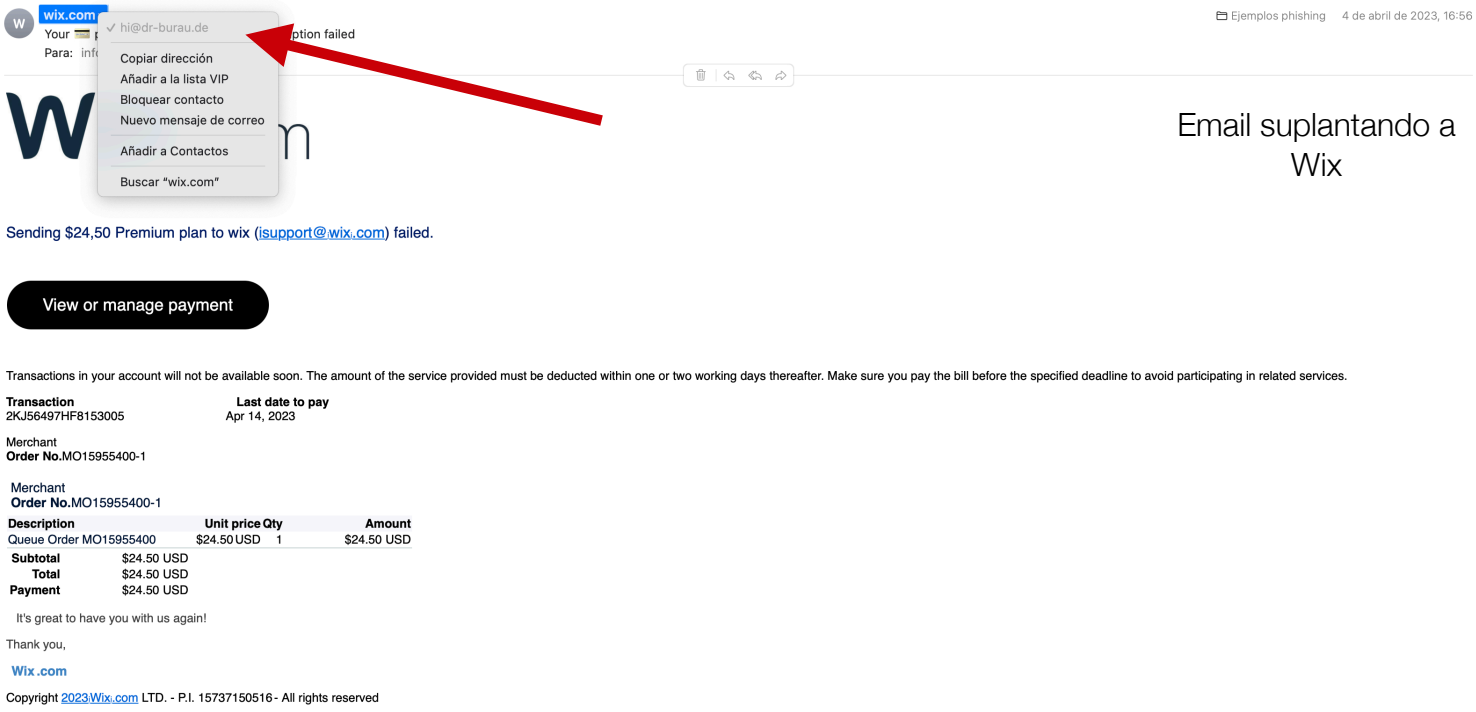
Mensajes fraudulentos

A veces se utilizan mensajes de texto para intentar engañarnos, bien para comprar algún servicio falso, para ir a una página web falsa y robar nuestros datos de acceso, para robar nuestra información bancaria o infectar nuestros dispositivos. Vamos a ver unos ejemplos de emails fraudulentos y de mensajes fraudulentos:

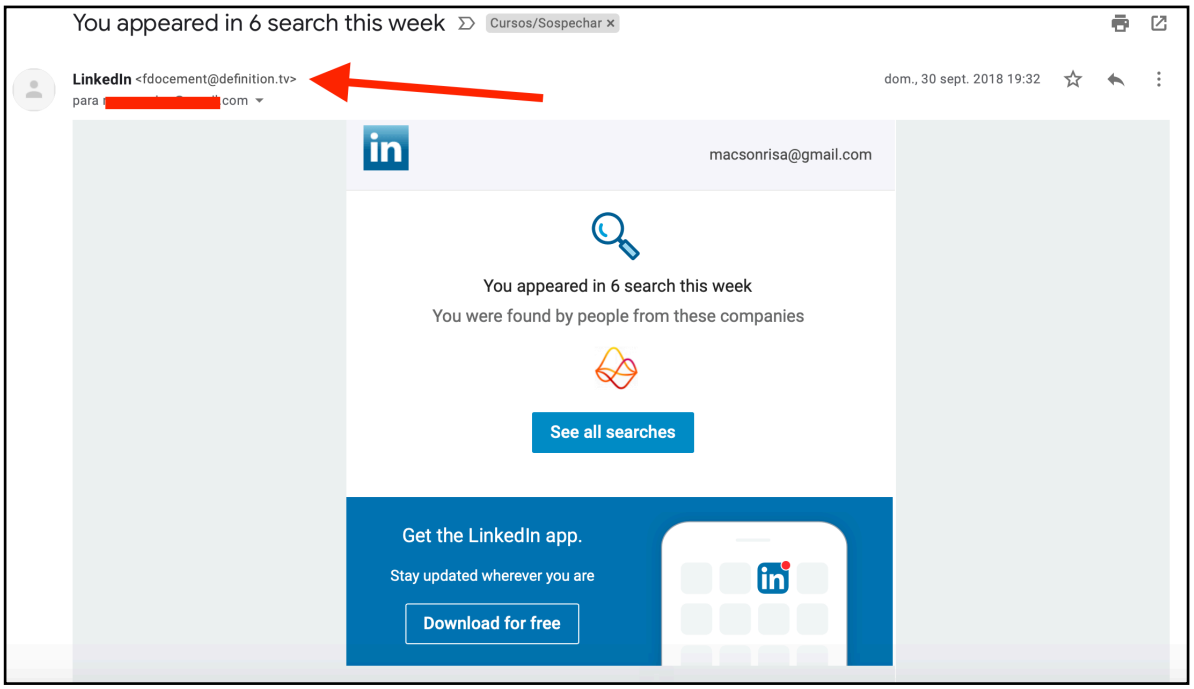
Emails:



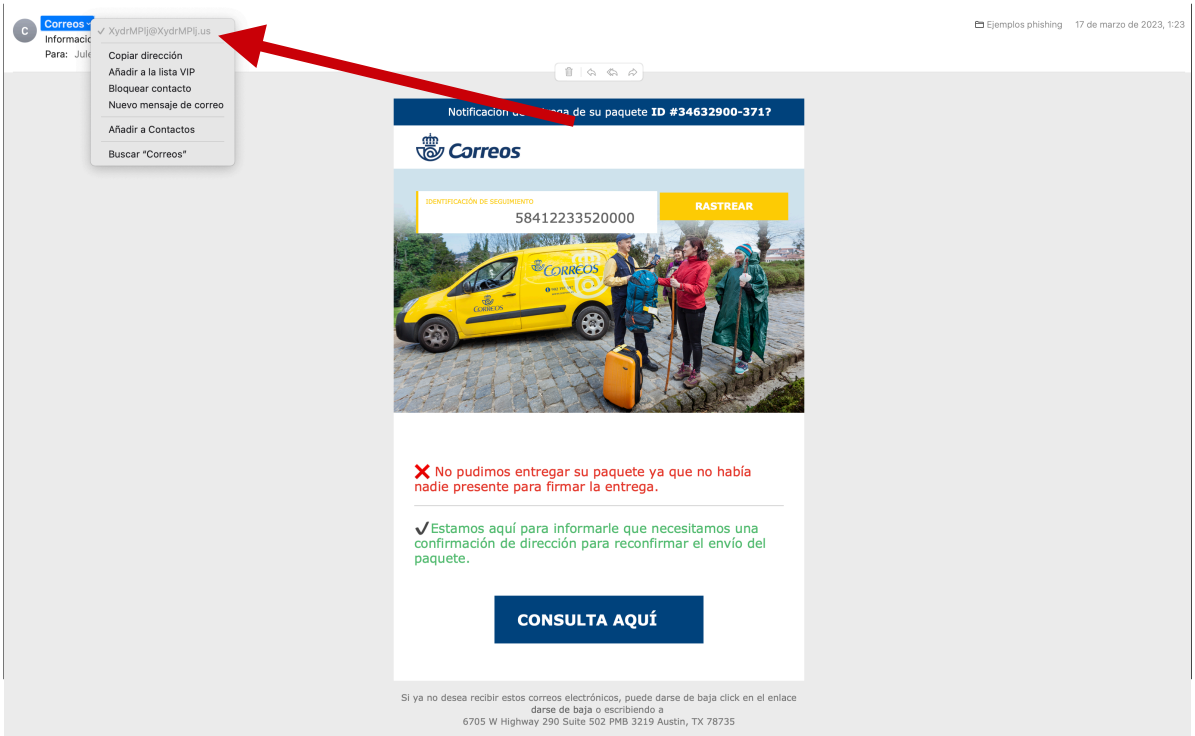
Email suplantando a Caixabank



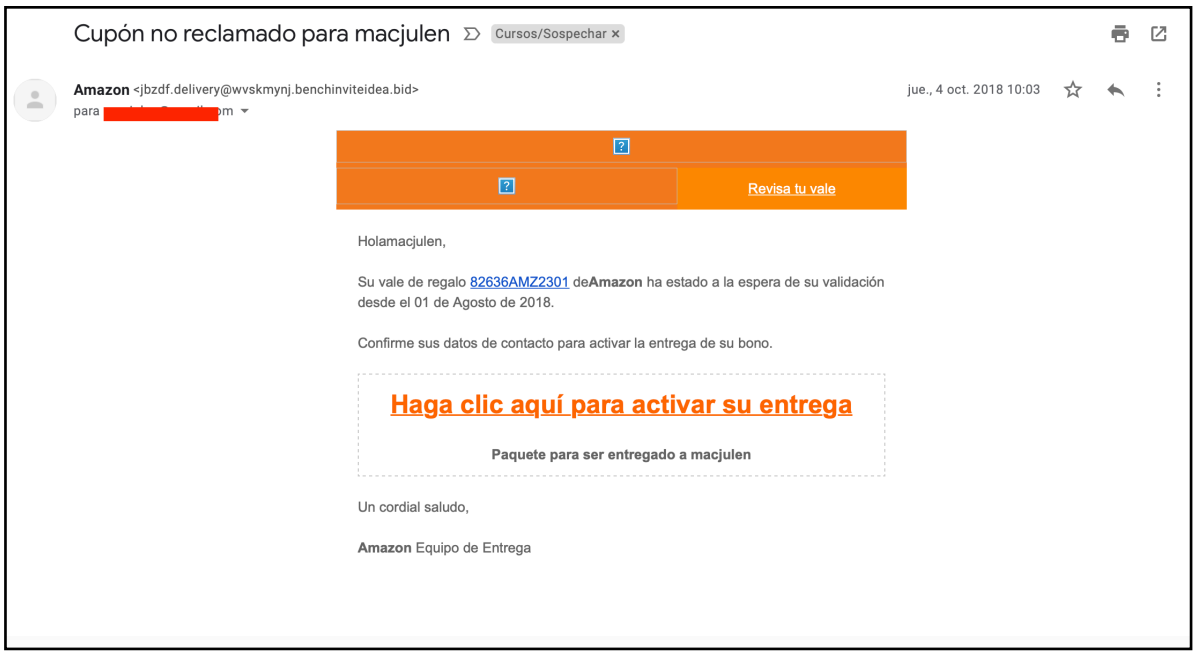
Email suplantando a Wix



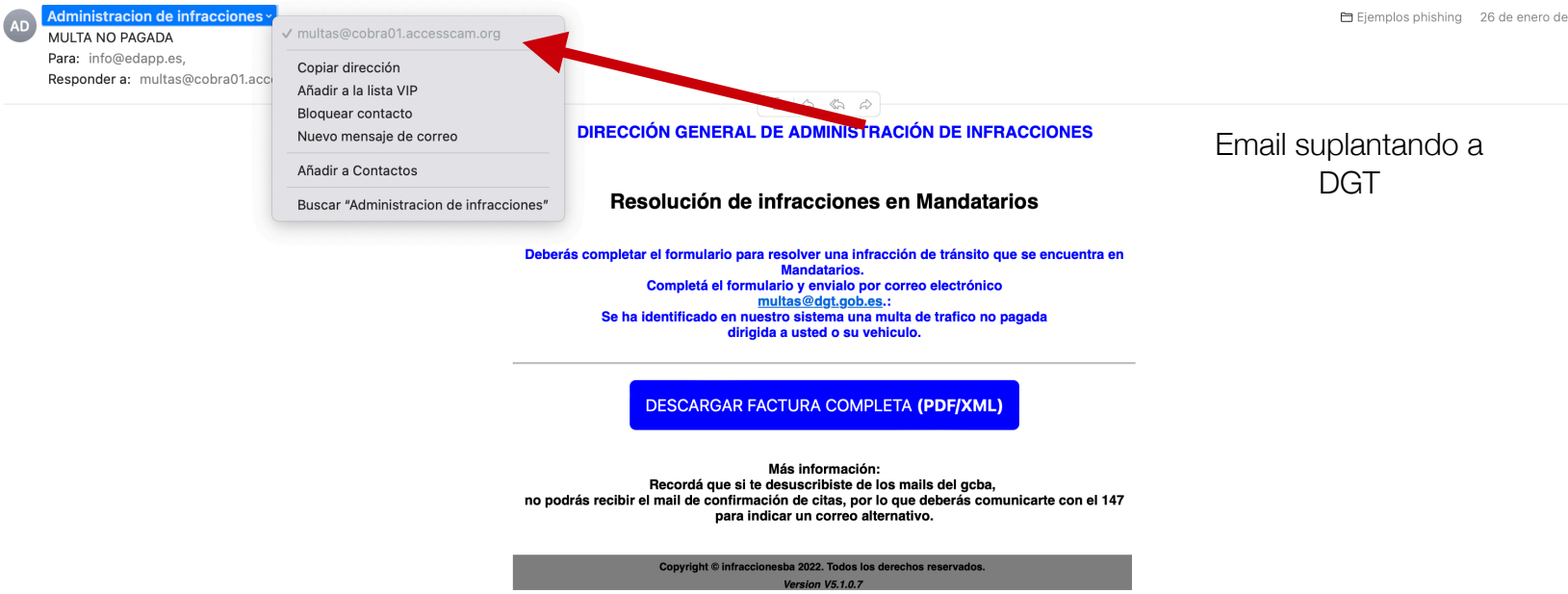
Email suplantando a LinkedIn



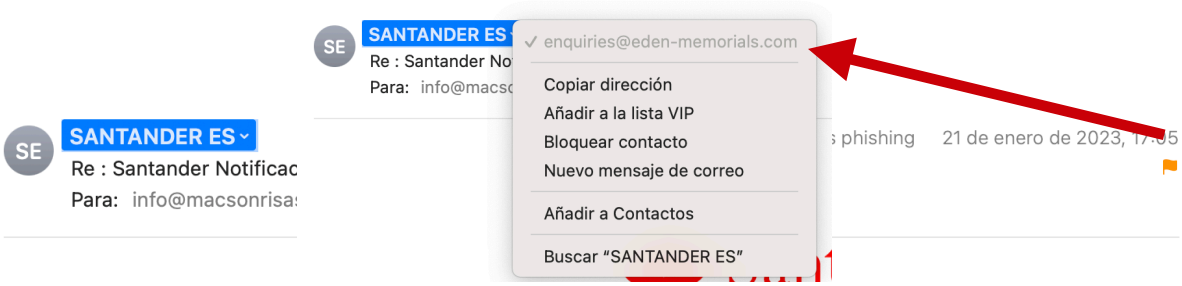
Email suplantando a Correos



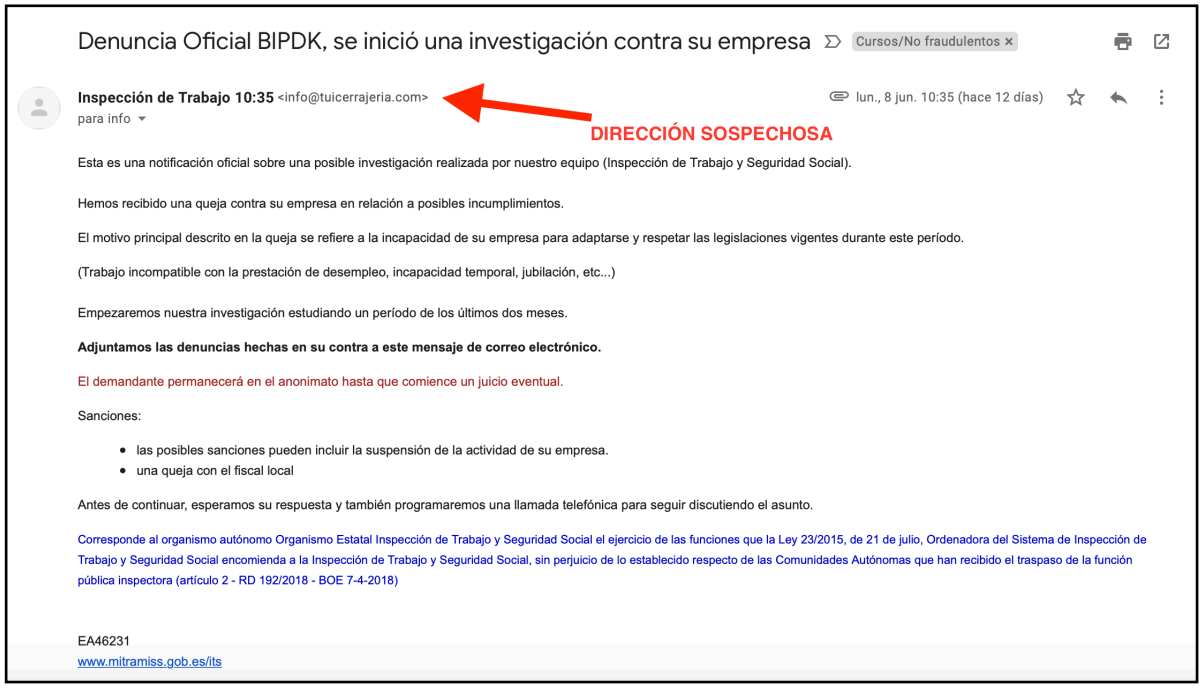
Email suplantando a Amazon I



Email suplantando a DGT

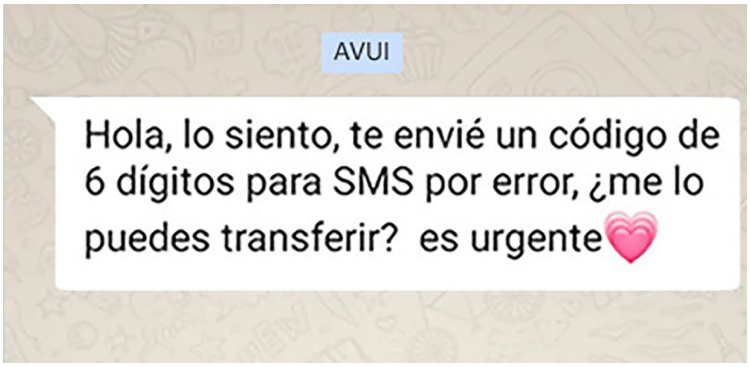


Email suplantando al banco Santander



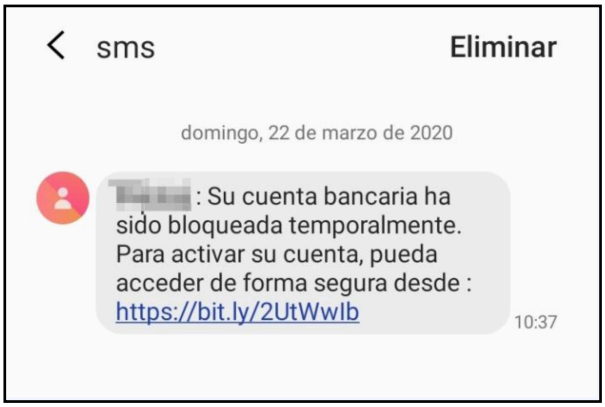
Email suplantando al Ministerio de Trabajo

Mensajes:



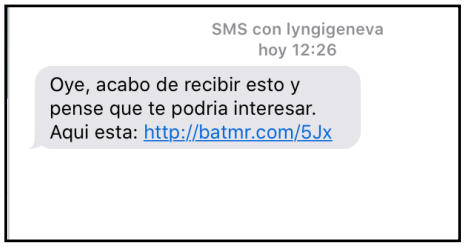
Mensaje fraudulento

Si mandamos el código, damos permiso a alguien para que nos robe la cuenta de Whatsapp



Sms fraudulento suplantando a un banco

Al pinchar en el enlace vamos a una página falsa del banco y al meter la información se quedan con ella o intentan otro tipo de fraudes.



Sms fraudulento

El link de este mensaje lleva a una página falsa que suplanta a El Mundo informando de unas supuestas inversiones que son una estafa

Estafa suplantando a Mercadona

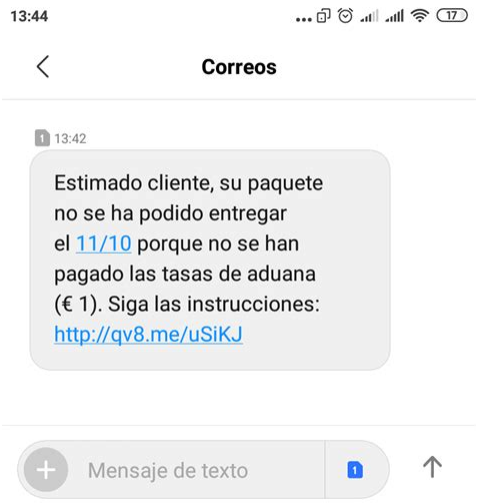
Al pinchar en el enlace vas a una página falsa de Mercadona donde corres el riesgo de descargar un virus, caer en diferentes estafas...

Estafa suplantando a Mercadona

Al pinchar en el enlace de antes llegas aquí y te piden que llames a un número de teléfono de pago para escuchar y contestar, cuanto más escuchas más pagas.

Mensaje falso

El enlace lleva a una página falsa de Lancome.



Otra estafa más

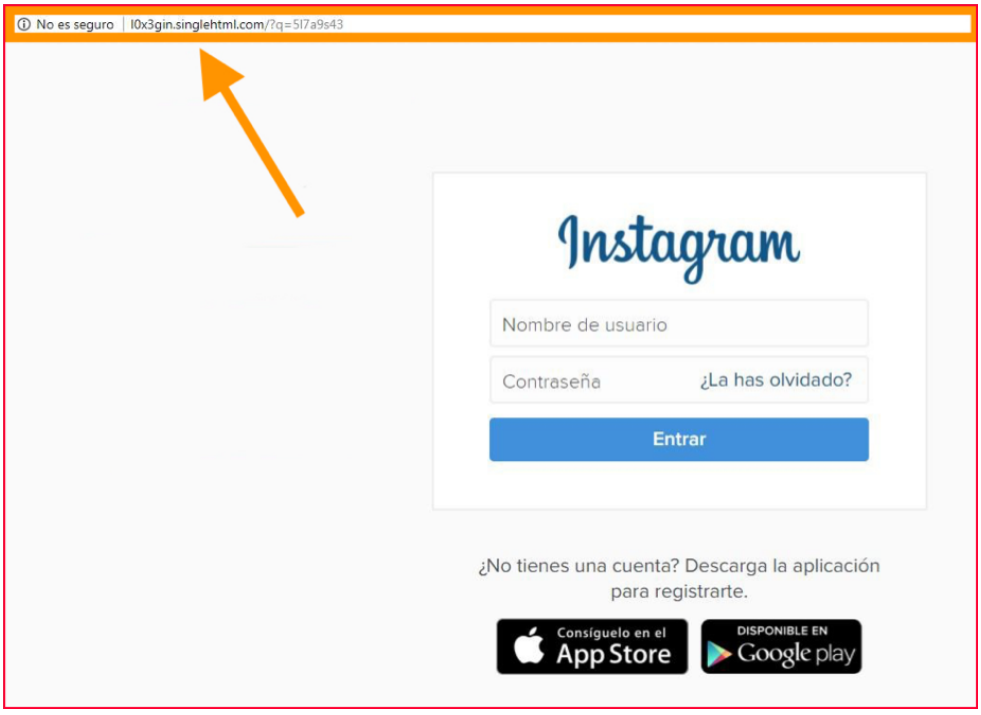
Nos hacen bajar una app desde cualquier sitio y al hacerlo estamos instalando un virus. Apps solo desde tiendas oficiales.

Estafa suplantando a un familiar

Nos hacen ingresar dinero en una cuenta fingiendo que son un familiar en apuros.

Para saber si una página en la que estamos es real o falsa, siempre nos fijaremos en la dirección de la misma. Si la dirección no es la que nosotros queremos, estamos en una página falsa.

A continuación podemos ver una página falsa de Instagram. La apariencia de la página es idéntica a la real, pero la dirección es otra diferente, no es instagram.com.



En la siguiente imagen vemos una página que se asemeja a la de el medio de comunicación español “El Mundo”, pero realmente es una página falsa porque en la dirección no viene elmundo.com o elmundo.es, la página en la que nos encontramos es mirrornewstrack.com, una página falsa que han creado para difundir una estafa con la intención de que aquellos que lo vean piensen que esa información ha sido publicada en un medio oficial e inviertan en la estafa.

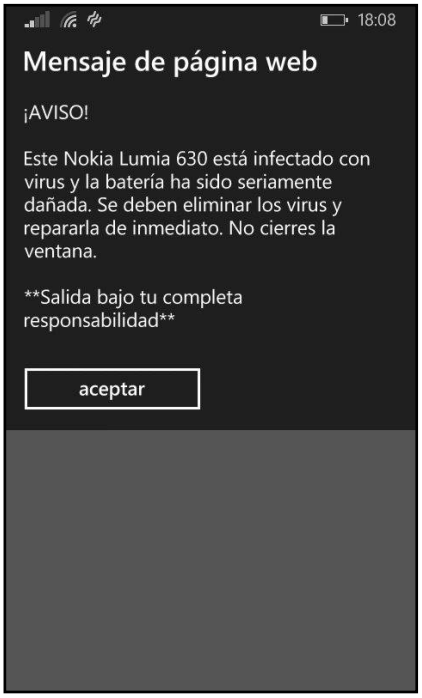
Al contrario de lo que mucha gente piensa, cuando vemos el candado a la izquierda de la dirección de la página no nos está indicando que la página sea segura, el candado nos indica que la comunicación con la página es segura. Es decir, que desde que introducimos nuestra información (nombre de usuario, contraseña, información bancaria...) en nuestro dispositivo hasta que llega al servidor donde está alojada la página, en el medio nadie la va a ver o interceptar.

Pero si la página es falsa, la información llegará de forma segura con la página falsa.

Al ir a cualquier página lo primero en lo que nos fijaremos será en la dirección de la página. Si es la correcta, una vez en la página correcta miraremos si la página tiene candado, y si no lo tiene no introduciremos nuestra información porque alguien se la puede llevar.
En el caso de la última imagen, vemos que la página que está haciéndose pasar por la página de El Mundo tiene un candado a la izquierda de la dirección, pero aún así es falsa porque la dirección es mirrornewstrack.com.

Anuncios trampa

Otras veces, cuando estamos navegando por Internet saltan anuncios intrusivos de muchos tipos que al pinchar en ellos nos llevan a páginas fraudulentas. Aquí algunos ejemplos:



Anuncio falso indicando que el móvil está infectado

Anuncio falso Amazon

Al pinchar en el botón que nos ofrece descargamos un programa que viene infectado. Cuando veamos un anuncio parecido, directamente cerraremos la ventana, no pulsaremos sobre los botones que nos ofrece: "descargar", "aceptar", "cerrar"...

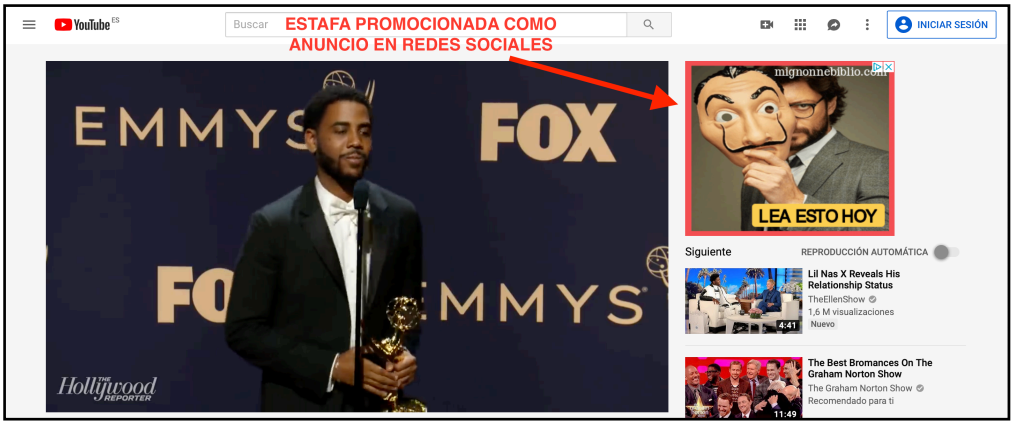
Anuncio - engaño

Cuando vamos a la página web nos empiezan a liar para que rellenemos formularios, demos información privada e incluso nos suscribamos a cosas.

Anuncio suplantando a una actualización

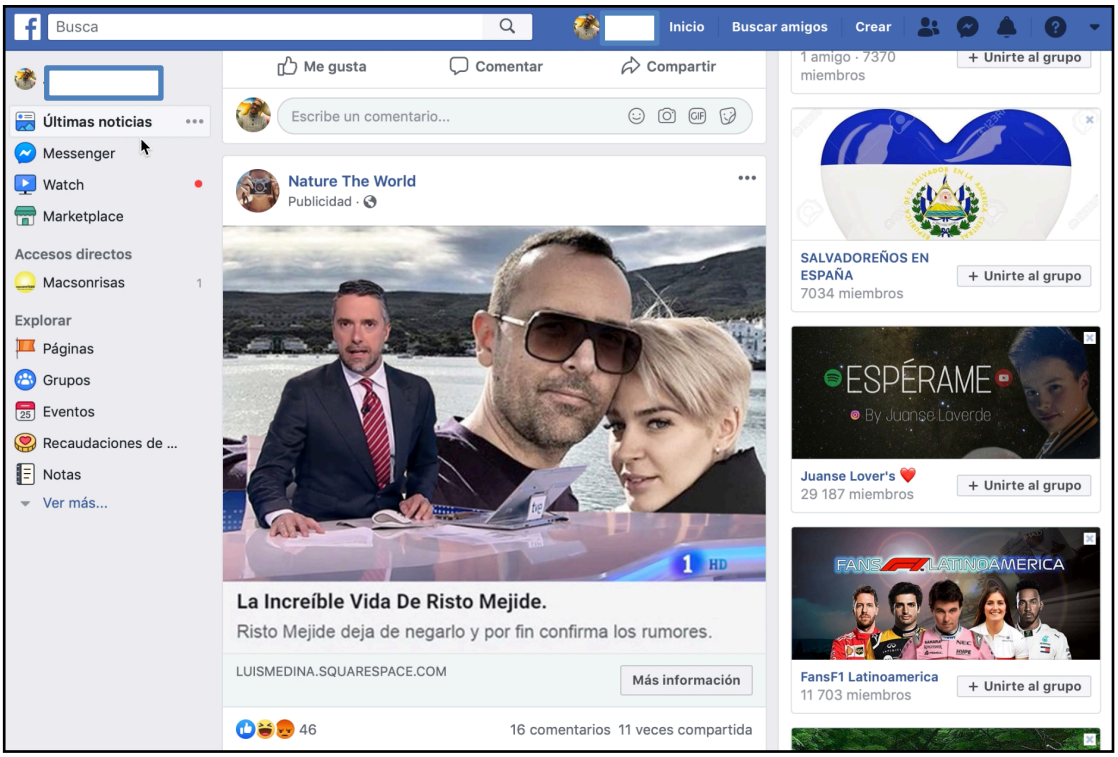
Las actualizaciones siempre se hacen desde los ajustes del teléfono, no desde páginas web.

Anuncio suplantando a Mediamarkt



Estafa promocionada como anuncio

Ese anuncio lleva una página falsa de una estafa sobre inversiones en Bitcoin (imagen). Lo grave es que está promocionada como anuncio, y la he visto ya en Facebook y en Youtube.

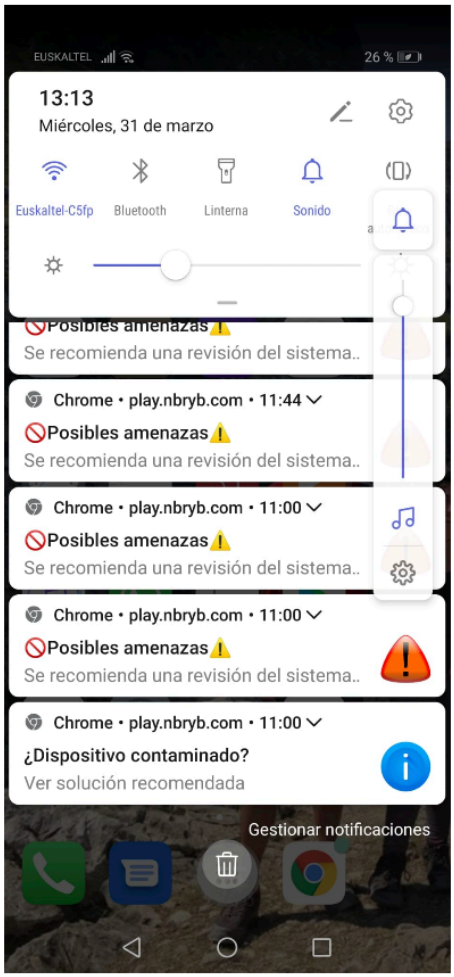


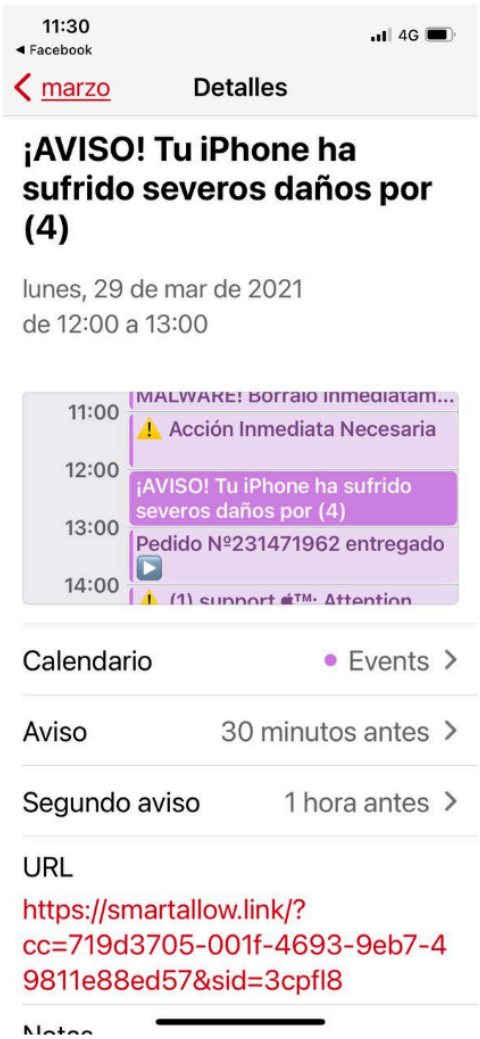
Anuncio en Facebook que lleva a la misma estafa

Notificaciones

Los ciberdelincuentes han puesto en marcha una nueva forma de ingeniería social: De repente comenzamos a recibir un montón de notificaciones diciéndonos que el teléfono o el ordenador está infectado, que el sistema está dañado, que hay problemas...

Lo que realmente está pasando es que sin darnos cuenta nos hemos suscrito a un calendario y estamos recibiendo las notificaciones de ese calendario. Para solucionar el problema iremos a la aplicación Calendario de nuestro teléfono, y allí eliminaremos la suscripción que sin querer hemos hecho al calendario que sea.





Vishing

Esta práctica es parecida al Phishing pero los ciberdelincuentes utilizan mensajes de voz. Recibimos una llamada de un número desconocido. Cuando la llamada es contestada, comienza una grabación y nos alerta de que nuestra tarjeta de crédito está siendo utilizada de forma fraudulenta y que debemos llamar al número que sigue inmediatamente. El número puede ser un número gratuito falseado para la compañía financiera que se pretende representar. Al llamar a este número, nos contesta un robot que nos indica que nuestra cuenta necesita ser verificada y nos pide que ingresemos los 16 dígitos de nuestra tarjeta de crédito, el pin, la fecha de expiración o todo.

También puede ser que nos llame directamente una persona diciendo que llama de nuestra oficina bancaria y que necesita nuestros datos para comprobar nuestra identidad, al dárselos se los estamos dando al ciberdelincuente.

Una variante de esta estafa es llamarnos diciendo que llaman de una empresa (por ejemplo Microsoft) y que hand detectado que desde nuestro ordenador se están enviando virus o malware. Nos dicen que tenemos que comprar un servicio o instalar un programa para solucionarlo. La compra es una estafa, no pasa nada y les damos nuestros datos bancarios, y al descargar el programa estamos instalando malware en nuestros dispositivos.

Otra modalidad de esta estafa son los secuestros exprés. Alguien nos llama y nos indica que han secuestrado a un familiar y que si no pagamos 2.000€ en un par de horas lo van a matar. Esto pasó durante una temporada en el 2018-2019 en Navarra, España. Todo era mentira.

Otras estafas habituales

Estafas navideñas

En festividades concretas como las Navidades, los ciberdelincuentes se ponen manos a la obra y preparan nuevas formas de delinquir. Cada año mejoran estas estafas y es más difícil detectarlas si no prestamos atención.

Apps Navideñas

Con la llegada de las Navidades un montón de apps navideñas van a hacer acto de presencia en nuestros smartphones y tablets. Entre ellas, habrá muchas apps maliciosas ocultas esperando a ser descargadas. Estas apps pueden robar nuestra información privada, e incluso espiar los mensajes que mandamos, las fotos que mandamos, las claves de acceso que introducimos en los bancos…

Por ello, siempre se recomienda descargar apps solamente desde tiendas oficiales y vigilar a qué información piden acceso. Además, hoy en día nadie regala nada, por lo que deberíamos empezar a desconfiar de las apps que son gratuitas. No de aquellas que ofrecen una versión gratuita o un periodo de prueba, sino de aquellas que son gratuitas y no vienen de desarrolladores conocidos. Nada es gratis, lo que no cuesta dinero, cuesta información personal.

Regalos y promociones de Navidad

Con la llegada de la Navidad, muchos ciberdelincuentes crean promociones falsas, o fingen realizar regalos haciéndose pasar por marcas reales. La forma de actuar suele ser mandarnos un mail o crear un concurso en las Redes Sociales donde para participar solo hay que hacer click en un link y rellenar el formulario que nos va a aparecer. Si clicamos en el enlace pueden pasar dos cosas. La primera, que ese enlace nos lleve a una pagina maliciosa donde al visitarla descargaremos malware (software malicioso) en el ordenador o dispositivo que estemos utilizando. La segunda es que ese link nos lleve a una página donde hay un formulario, pero al rellenarlo solamente estaremos regalando nuestros datos introducidos a los ciberdelincuentes: Número de teléfono, correo electrónico, dirección…

Chollos navideños

Tenemos que tener claro que los chollos no existen en el mundo online. La proliferación de los smartphones y tabletas nos ayuda a poder realizar compras desde cualquier lugar en cualquier momento, y los ciberdelincuentes los saben, por lo que muchas veces nos mandan mensajes y mails falsos o crean anuncios en las Redes Sociales con ofertas irresistibles de duración limitada. Pueden ser productos, viajes, hoteles… Al pinchar en el anuncio llegamos a una página web con la apariencia de una tienda online real donde pueden pasar dos cosas. La primera es que realicemos el proceso de compra entero, paguemos y que nunca recibamos el producto. La segunda es que durante el proceso de compra los ciberdelincuentes simulen un formulario falso y al introducir el número de tarjeta con la clave, les regalemos la información a los ciberdelincuentes.

Si vamos a realizar compras online, antes de introducir los datos en ningún sitio, tenemos que asegurarnos de que en la barra de direcciones veamos un candado o que la dirección de la página empiece por https://. También debemos fijarnos en la barra de direcciones para saber en qué página estamos. Si el anuncio era de Amazon y al pinchar en el enlace nos lleva a www.amezon.es, la página es falsa. La dirección tiene que ser www.amazon.es. Si es amazon.1.es ya no es la correcta.
Por último debemos buscar referencias de la supuesta tienda y evitar las que no son conocidas. También debemos evitar pagar por transferencia bancaria, siempre a través de pasarelas seguras de pago o a través de Paypal.

Suplantación de ONGs o similares

El espíritu Navideño y la solidaridad también son utilizados para engañar a las víctimas. Ciberdelincuentes suplantan a ONGs y crean campañas falsas de ayuda en Redes Sociales y a través de mails y anuncios online. Al pinchar en los enlaces para colaborar, las víctimas son redirigidas a páginas falsas donde al introducir sus datos o credenciales bancarias son estafadas. Si alguien quiere colaborar, que vaya a la página web oficial de la ONG (escribiéndola, sin hacer clic en ningún enlace, y siempre fijándose en la dirección de la página web y en el candado antes de hacer ningún pago o meter ningún tipo de información) o que se presente en alguna de sus oficinas físicas.

También me gustaría recordad que Facebook no hace, ni nunca ha hecho, donaciones en función del número de veces que una publicación se comparte o en función del número de “Me gusta” que una publicación tiene, ni niños con cáncer,

ni terremotos, ni nada. Los ciberdelincuentes se aprovechan de la bondad de la gente y de su desconocimiento del mundo online.

Falsos mails de facturas o cargos en cuenta

Aprovechando que mucha gente viaja en Navidades y que se realizan muchas compras online, los ciberdelincuentes también crean campañas de mails relacionadas con viajes, cargos falsos en tarjetas de crédito… haciéndose pasar por bancos, agencias de viajes, aerolíneas…Siempre se recomienda mirar el remitente de los mails y fijarse si el saludo principal es genérico o personalizado. Si es genérico suele ser falso. Por ejemplo una notificación personal de un banco empezará "Estimado Julen", en lugar de "Estimado cliente". Ese mail siempre traerá consigo un link en el que nos invitan a pinchar para solucionar problemas, o ver cargos… Se recomienda no pinchar nunca. Si tenemos dudas o curiosidad, teclearemos nosotros la dirección de la empresa o del banco en la barra de direcciones o llamaremos por teléfono, pero debemos tener cuidado con los links.

E-cards peligrosas

Existen muchas compañías en internet que crean felicitaciones interactivas cuyo texto podemos personalizar y mandarlas por mail de forma gratuita. No hay ningún problema con este tipo de compañías, pero debemos estar atentos por si recibimos estas tarjetas de desconocidos ya que al pinchar en el link para ver la tarjeta nos puede llevar a una página web donde descargaremos software malicioso.

Compras online

Muchas veces pagamos un producto que nunca recibimos o recibimos cosas que no tienen nada que ver con lo que habíamos visto en la página web, y al ir a reclamar nos damos cuenta de que esa empresa a la que hemos comprado no existe. Otras veces compramos artículos de segunda mano a personas que no los mandan o recibimos otros artículos en su lugar.

He aquí algunos consejos para tener en cuenta a la hora de realizar compras online:

- Lo primero que tenemos que hacer siempre, antes de introducir nuestro datos (bien sea el nombre de usuario y la contraseña en una web o los datos de la tarjeta para comprar algo) es fijarnos en donde estamos, mirando la barra de direcciones. Conviene comprobar si el lugar en el que nos encontramos es el que queríamos visitar. Por ejemplo, si queríamos ir a Amazon, pero estamos en www.amezon.es, o www.amazon.com1.com claramente no es la página que nos interesa aunque en apariencia sea exactamente igual.

- Para que introduzcamos datos de forma segura, siempre, la dirección de la página tiene que empezar por https//: (nos fijamos en que esté la s) o tiene que aparecer un candado. Eso nos indica que la comunicación con esa página es segura, está certificada.

- Conviene realizar compras en tiendas online conocidas. Si no las conocemos, debemos asegurarnos de que son reales y no ficticias. Para ello debemos verificar el número de teléfono o la dirección física o buscar información en internet sobre esa tienda.

- Conviene revisar la política de privacidad y de devoluciones. Parece obvio, pero tenemos que saber cuánto vamos a pagar y qué vamos a pagar. Esto quiere decir que miraremos si los precios que aparecen son con IVA o sin IVA y siempre tenemos que sumar los gastos de envío. También miraremos la letra pequeña de los productos para saber exactamente qué es lo que se vende. Si compramos algo fuera de nuestro país debemos asegurarnos de que no pagaremos gastos de aduana cuando llegue el paquete.

- Si compramos algo, nunca vamos a pagar a través de transferencias ni vamos a enviar dinero en efectivo, ni vamos a mandar nuestra información financiera por mail. Siempre realizaremos los pagos a través de Paypal o a través de la pasarela de pago de cada comercio online, fijándonos que en la barra de direcciones aparezca el candado blanco o verde o https://. Si alguna vez nos fijamos en que no esta ni https:// ni el candado, directamente saldremos de la página.

- También es importante realizar estas compras utilizando la tarifa de datos de nuestros dispositivos o conectándonos a redes wifi seguras, evitaremos las redes wifi públicas que no tienen contraseña, y aquellas de lugares donde se conecta mucha gente como restaurantes, bibliotecas, hoteles…

Ofertas de empleo

Según un informe de Adecco, uno de cada cuatro fraudes que hay en Internet proviene de una oferta de empleo falsa.

Estas ofertas prometen trabajos muy inmediatos o salarios muy superiores al de los perfiles que se solicitan en la oferta. Además prometen grandes beneficios sin necesidad de tener ninguna experiencia laboral o cualificación profesional.

Algunos anuncios animan a los buscadores de empleo a encontrar un trabajo llamando a un teléfono de tarificación adicional para que soliciten información sobre los requisitos del proceso de selección donde están esperando mucho tiempo.

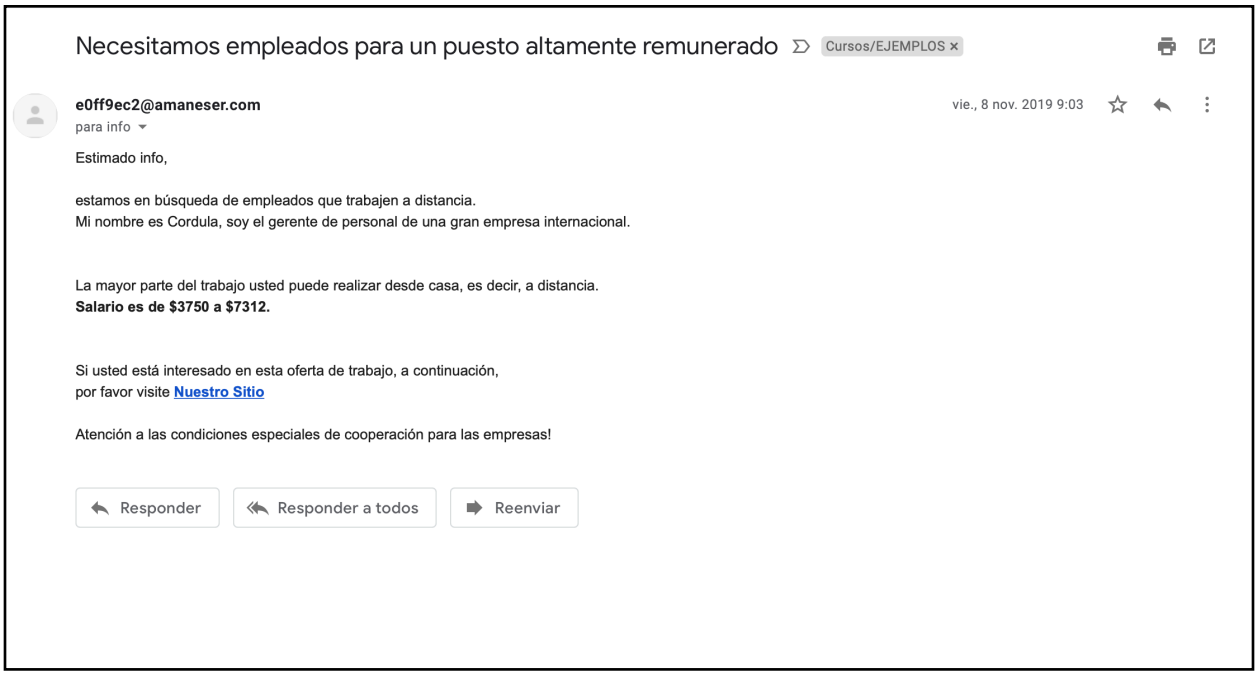
Algunas ofertas requieren el envío de uno o varios SMS como forma de contacto que no serán respondidos por la empresa responsable del supuesto proceso de selección.

También podemos encontrar cursos estafa, que requieren a los desempleados el desembolso de dinero (en algunos casos de miles de euros) para recibir un curso de formación online a través del que podrán encontrar trabajo.

Hay ofertas de trabajo en el sector de la construcción en el extranjero que requieren un pago para hacer frente a los gastos de gestión de un trabajo muy bien pagado en un país extranjero.

Hay otra modalidad de estafa que utiliza el correo electrónico para la divulgación de una oferta de empleo fraudulenta. Normalmente, se trata de "empleos" en los que se puede trabajar desde casa realizando operaciones bancarias, "de forma cómoda y con altos beneficios".

En realidad, esta es una forma de blanqueo de dinero por parte del empleado a quien siempre se le exige disponer o abrir una cuenta bancaria. El trabajo en sí consiste en recibir trasferencias a esa cuenta para su posterior reenvío al extranjero pero en realidad lo que se produce (con el desconocimiento del empleado) es el blanqueo de dinero obtenido gracias a estafas bancarias.


Necesitamos empleados para un puesto altamente remunerado
Cursos/EJEMPLOS ×
e0ff9ec2@amaneser.com
para info
vie., 8 nov. 2019 9:03
Estimado info,
estamos en búsqueda de empleados que trabajen a distancia.
Mi nombre es Cordula, soy el gerente de personal de una gran empresa internacional.
La mayor parte del trabajo usted puede realizar desde casa, es decir, a distancia.
Salario es de $3750 a $7312.
Si usted está interesado en esta oferta de trabajo, a continuación,
por favor visite Nuestro Sitio
Atención a las condiciones especiales de cooperación para las empresas!
Responder
Responder a todos
Reenviar

Estafas sentimentales

En este libro entendemos también como red social aplicaciones como Skype o aplicaciones de mensajería como Whats app.

Ciberdelincuentes se ponen en contacto con nosotros y simulan empezar una relación de amistad. Pasado un tiempo y después de haberse ganado nuestra confianza poco a poco enviándonos fotos (falsas) y estableciendo una relación (a través de mentiras), empezarán a pedirnos dinero para pagar el avión, tren... y venir a vernos, evitar algún problema que les pueda surgir o cosas como estas.

Estos ciberdelincuentes hacen muy bien su trabajo, y muchas veces hacen creer a las víctimas que tienen una verdadera relación a distancia. Más ejemplos.

Estafas de caridad

Los ciberdelincuentes se hacen pasar por organizaciones de caridad pidiendo donaciones tras catástrofes naturales, ataques terroristas, enfermedades o para atender gente enferma. Pueden hacerlo a través de mails o anuncios falsos en diferentes páginas web.

Sextorsión

Mandamos fotos o videos íntimos a un desconocido (Redes Sociales, Apps mensajería, Juegos online, Apps Citas) o una persona conocida (pareja, amante, amigo/a...).

Las imágenes se difunden de forma intencionada o no intencionada y una persona des conocida o conocida no amenaza con publicar el nuestro material íntimo si no le pagamos una cantidad determinada, o no hacemos algo que esa persona quiere, o tenemos sexo con ella, o le mandamos material pornográfico personalizado…

Épocas de compras masivas

En fechas en las que se compran muchas cosas (Navidades, Black Friday, reserva de viajes en verano y navidades...) hay campañas de emails fraudulentos

suplantando a empresas de mensajería. Son emails como los que hemos visto en el apartado anterior “Phishing”.

Campaña de la renta

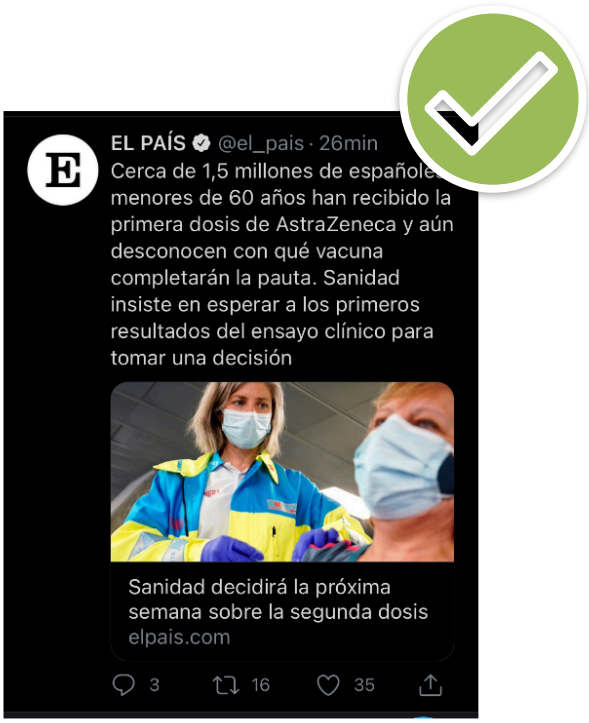
Durante la Campaña de la Renta circulan muchos emails y mensajes falsos suplantando a Hacienda.

Cuentas falsas

En diferentes redes sociales podemos encontrar multitud de cuentas falsas suplantando a empresas o personas reales para realizar diferentes tipos de estafas

Por poner un ejemplo hace unos meses Elon Musk, el empresario estadounidense, anunció a través de Twitter que su compañía Tesla iba a adquirir Bitcoin por un valor de 1,5 billones de dólares. Ese tuit, que tuvo gran repercusión, tuvo muchos comentarios y entre uno de los primeros había uno de una cuenta falsa suplantando a Elon Musk que animaba a los seguidores que quisieran a invertir en Bitcoin con él. Añadían un enlace al tuit que llevaba una página falsa de inversión con lo que todas las personas que invirtieron perdieron su dinero. En dos horas los ciberdelincuentes fueron capaces de estafar 400.000$. La cuenta falsa utilizaba la misma foto en su perfil, pero el nombre de usuario era diferente.

También hay muchas cuentas falsas que buscan difundir desinformación. En el siguiente ejemplo vemos dos tweets de dos cuentas de Twitter diferentes, la primera suplantando a el diario el país, y la segunda la cuenta real del diario El País. Más que la primera es una cuenta falsa porque el nombre de usuario está mal escrito, tiene un _ al final y además la cuenta no está verificada. Las empresas y personas famosas generalmente suelen tener las cuentas verificadas con el símbolo de verificación en todas las redes sociales menos en Twitter, donde recientemente Elon Musk, después de comprarla ha decidido cobrar por el símbolo de verificación y lo tienen todos aquellos usuarios que paguen, tengan cuentas reales o falsas.



Conviene recordar que todos los medios de comunicación añaden enlace a la noticia que están difundiendo.

Una pauta para detectar la desinformación es mirar si ese mensaje o esa publicación tiene un enlace a un medio comunicación fiable o a una entidad pública que esté compartiendo la noticia. Si no tiene ese enlace no nos queremos lo que estamos leyendo o iremos a contrastarlo. Si tiene enlace leeremos a la noticia entera para corroborar que realmente están informando de eso de lo que nos están informando en el mensaje.

Para detectar cuentas falsas en redes sociales es muy importante fijarnos en el nombre de usuario de la cuenta, ya que en la misma red social no puede haber dos cuentas con el mismo nombre de usuario.

Hay muchas estafas relacionadas con cuentas falsas a través de los mensajes directos en las redes sociales. Por ejemplo hay cuentas oficiales que realizan sorteos diciendo: “para participar comparte la publicación y menciona a tres personas”. Esos sorteos son legítimos. El problema es que al participar en esos sorteos compartiendo la publicación, cuentas falsas se ponen en contacto con nosotros a través de mensajes directos y viéndonos más información o más cosas para continuar en el sorteo.

En los mensajes directos es no se suele ver a simple vista el nombre de usuario de la cuenta que nos está mandando el mensaje. Suele aparecer solamente la foto de

perfil de esa cuenta y el nombre de quien ha creado la cuenta, no el nombre de usuario de la cuenta, y todas las cuentas falsas usan la foto de perfil de la cuenta real. Tenemos que fijarnos en la verificación (en caso de tenerla) y tenemos que entrar en el perfil de quien nos ha enviado el mensaje para ver su nombre de usuario.

Muchas veces hay cuentas falsas que suplantan a la policía o a las propias redes sociales. Nos escriben informándonos de que alguien ha denunciado nuestra cuenta y nos exigen nuestro nombre de usuario y nuestra contraseña para poder acceder y comprobar que todo está bien. Si alguien pica y le proporciona la información, le roban la cuenta.

También abundan las estafas relacionadas con las apuestas online y con todo tipo de inversiones, no solamente relacionadas con las Criptomonedas como el ejemplo que acabamos de ver de Elon Musk.

Estafa del CEO

En esta estafa un ciberdelincuente suplanta a la persona al mando de una empresa, asociación, ayuntamiento, centro educativo y manda un email a la persona encargada de hacer los pagos para que haga un ingreso en un número de cuenta determinado.

Esta estafa tiene dos variantes:

9. El ciberdelincuente utiliza una dirección de correo similar a la de la persona suplantada, la persona encargada de hacer los pagos no se fija y cae en la trampa haciendo el pago en la cuenta de los ciberdelincuentes.

10. El ciberdelincuente logra entrar en la cuenta de la persona encargada, y manda el correo desde allí.

En el primer caso, con seguir la primera pauta para detectar emails fraudulentos es suficiente, miramos la dirección desde la que se están enviando todos los emails que recibimos y podemos detectar los falsos.

En el segundo caso es más complicado porque el email ha sido mandado realmente desde la cuenta de la persona encargada. Lo que se recomienda aquí es utilizar siempre saludos personalizados concretos para poder detectar cualquier cambio y tener protocolos de pago seguros, como por ejemplo verificar de dos formas diferentes que los pagos de más de x cantidad de dinero.

Esta estafa ya ha costado más de 2.000 millones de dólares a empresas de todo el mundo.

EL PAÍS

SUSCRÍBETE INICIAR SESIÓN

La EMT de Valencia sufre una rocambolesca estafa de cuatro millones de euros

Una directiva transfiere la suma a una cuenta externa tras ser víctima presuntamente del fraude del CEO

66

IGNACIO ZAFRA

Valencia - 28 SEP 2019 - 13:42 CEST

Fila en una parada de autobús en Valencia. MÒNICA TORRES

NEWSLETTER
Recibe el boletín de Actualidad

TE PUEDE INTERESAR

La directiva despedida de la EMT declara que fue "una engañada más" en la millonaria estafa

Valencia bloquea 150.000 euros de los cuatro millones estafados a la EMT

Caixabank responde a la EMT que no es responsable de los fraudes a sus clientes

20 minutos

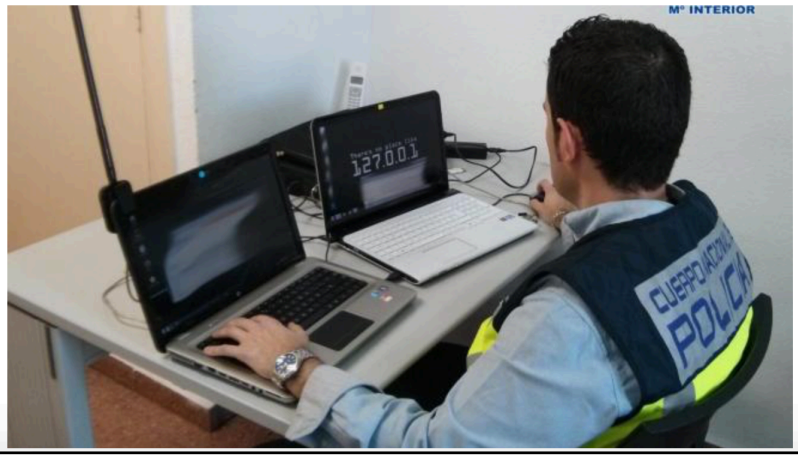
Actualidad Nacional Internacional Deportes Opinión Gente Más

El 'fraude del CEO': la nueva estafa con un correo que asegura ser tu "jefe" y que ha supuesto la detención de 11 personas

El Cuerpo Nacional de Policía detecta una alerta por 'phishing'.

EFE 11.05.2020 - 12:17H

- Es una modalidad de estafa diferente al 'phishing' y que busca víctimas con perfil concreto.
- Cuidado: Telefónica no está premiando a sus clientes, es una estafa.



BLOGS DE 20MINUTOS

DANDO LA NOTA
Mónica Naranjo estrena el videoclip de 'Hoy No', su nuevo temazo

¿QUÉ FUE DE?
Qué fue de... Stjepan Andrijasevic: talento croata en la Liga española

EN BUSCA DE UNA SEGUNDA OPORTUNIDAD
Los gatos, esos grandes desconocidos

Capítulo 4
Redes sociales

Las Redes Sociales son servicios utilizados por millones de personas. Además, las diferentes ramas de las redes sociales hacen que el numero total de usuarios se dispare.

Al hablar de redes sociales hablamos de servicios como Facebook, Twitter, Tumblir, Flickr, Instagram, LinkedIn, Badoo, Snapchat, Tinder, Grinder, Youtube y muchas más que ayudan a estar en contacto y a compartir información con otras personas que utilizan esos mismos servicios. En este libro también vamos a meter en el ámbito de las Redes Sociales a Skype y Whats App porque en el fondo lo son.

Tantos usuarios ha llevado a los ciberdelincuentes a utilizar estas redes sociales como objetivo y como ámbito de actuación donde realizar sus acciones. Es muy habitual que intenten hacerse con nuestros nombres de usuario y contraseñas para poder hackear nuestras cuentas o que intenten propagar malware y direccionarnos a páginas fraudulentas a través de ellas, entre otros menesteres.

Estas son algunas de las cosas a tener en cuenta a la hora de utilizar las redes sociales.

Links o enlaces y fotos

Al igual que hemos visto en capítulos anteriores, en las Redes Sociales también tenemos que andar con mucho cuidado a la hora de pinchar en los links, sobre todo en aquellos que mucha gente comparte y que nadie sabe de dónde han salido. Tenemos que ver la dirección de la página a la que nos lleva, si es real o es una página fraudulenta con apariencia real.

Otro intento de infección ha sido durante mucho tiempo y aún lo sigue siendo, que nos llegue un mensaje diciendo “apareces en un video en internet” acompañado de un enlace. Al pinchar en el enlace e intentar ver el video podemos descargar ficheros indeseados, o nos puede aparecer el mensaje de “actualice su reproductor para ver este video”, y al hacerlo es donde realmente estamos descargando malware.

Deberíamos pararnos a pensar durante un segundo si la necesidad que en poco tiempo nos ha surgido de compartir todo lo que nos llega es real, o es algo infundado que hacemos de forma automática. Muchas veces compartimos links fraudulentos o fotos con malware sin ser conscientes de lo que estamos haciendo y otros sufren las consecuencias.

Algunos ciberdelincuentes utilizan las redes sociales para crear páginas falsas donde poder engañar a los usuarios. Debemos tener cuidado con páginas de tiendas en las Redes Sociales.

Si vamos utilizar el servicio online de una tienda que no conocemos físicamente, debemos mirar si en su información aparecen más datos como números de teléfono o direcciones físicas que podamos corroborar, y si hacemos compras online siempre utilizaremos paypal o las pasarelas de pago seguro, nunca pagaremos haciendo transferencias bancarias.

Sexting

Aunque se dice por activa y por pasiva, parece que hay algo que no nos termina de entrar en la cabeza. Cuando mandamos fotos o videos, cuando que salen de nuestros dispositivos, perdemos su control.

La cultura del sexting, mandar mensajes de carácter erótico, se está extendiendo mucho, y también está dando muchos disgustos. Es algo que puede parecer divertido, pero no sabemos lo que pasa con esa foto o video que sale de nuestro teléfono una vez que lo mandamos, y esas fotos se utilizan mucho para hacer chantajes y extorsiones, para pequeñas "venganzas" cuando se terminan las relaciones o para humillar las personas que aparecen en las fotos o videos difundiéndolos en las Redes Sociales.

Es importante subrayar que cuando las fotos o videos contienen menores, es delito compartirlas y está tipificado en el código penal. También es importante subrayar la importancia de educar a los menores en el uso correcto de las redes sociales, en no hacerse fotos o videos que les puedan perjudicar y en no compartir aquellas cosas que les llegan que pueden parecer "graciosas" a priori pero que pueden causar mucho daño a las personas involucradas.

Siempre tenemos miedo de que nuestros menores sean víctimas de este tipo de humillaciones e intentamos protegerles, pero debemos ser conscientes de que pueden ser los "humilladores" y también debemos educarles en el respeto a los demás y el respeto a la privacidad de los demás.

¡A compartir todo lo que nos llega!

Es muy habitual el envío de imágenes "graciosas" por Whats App a muchos de nuestros contactos. Se ha creado una especia de ley no escrita en la que el tener Whats App parece que nos obliga a compartir todo lo que nos llega y a crear grupos para estar todo el día enganchados y compartiendo cosas, la mayoría de las veces superficiales e innecesarias. Hace unos meses se descubrió un malware para Android que podía propagarse a través de fotos y que bloqueaba las fotos, videos y documentos. Para desbloquearlos los ciberdelincuentes pedían un rescate (ransomware).

Páginas y cuentas falsas

Algunos delincuentes suplantan identidades de otras personas o servicios. Sin pertenecer a una empresa, crean un perfil donde todos los datos son ciertos excepto el link que nos redirige a una página fraudulenta.

Otros crean perfiles personales falsos para acechar y atacar a posibles víctimas, generalmente de forma sexual o pidiéndoles dinero. Tienen diferentes objetivos de forma simultánea, se ganan poco a poco su confianza y a los meses empiezan a pedirles fotos un poco picantes.

Mandan fotos que no son suyas para incentivar a las víctimas y cuando éstas responden les empiezan a extorsionar, amenazando con hacer públicas las fotos o videos si no hacen lo que les dicen.

Cuando el acoso es de un adulto a un menor, estas acciones se denominan Grooming.

Otras veces los delincuentes aparentan interesarse por las víctimas, y cuando las victimas se "enamoran" les empiezan a pedir dinero porque les ha surgido algún problema, o para pagar el transporte para ir a ver a las víctimas…

Detección de perfiles falsos

Para detectar perfiles falsos podemos hacer o fijarnos en diferentes cosas:

Hay aplicaciones como "Image Search" para smartphones y tablets, o servicios como Google Images que nos permiten **buscar imágenes en la red** y ver los resultados que dan. Si sospechamos de alguien en Internet podemos hacer una captura de una foto suya y buscarla a través de estos servicios. Si en lo resultados aparece que esa foto ha sido sacada de un banco de fotos, que es de un o una modelo o viene con el nombre de otra persona, ya sabemos que no es quien dice ser.

Publicaciones: Podemos ver cuándo han hecho sus publicaciones, si las han realizado todas el mismo días o en un periodo corto de tiempo podemos sospechar.

Perfil: Si su perfil no está completo, si no tiene imagen o si tiene 0 seguidores también podemos empezar a sospechar.

Si vemos que **lo único que hace esa cuenta es compartir cosas que otras personas han publicado y no interactúa con nadie**, también podemos empezar a sospechar de que puede ser una página falsa.

Ejemplos de sextorsión

La sextorsión es un tipo de extorsión en la que una persona o grupo amenaza a un tercero con publicar en las Redes Sociales sus fotos o videos de carácter sexual a cambio de dinero o de generar material pornográfico. Es muy habitual hoy en día pero se denuncia muy pocas veces debido a la vergüenza y humillación que genera.

Situación 1: María se ha puesto en contacto con Mario en las Redes Sociales, acaba de llegar a la ciudad, ha encontrado su perfil y le ha parecido atractivo. Mario, viendo que María es una chica de buen ver gracias a sus fotos en las Redes Sociales, empieza a chatear con ella y resulta que conectan de una manera muy especial: Tienen los mismos gustos, mismas aficiones… vamos que a Mario le empieza a gustar.

Después de varias sesiones de chats, María que es muy liberal le empieza a mandar fotos íntimas a Mario, y Mario le corresponde mandándole fotos suyas, ya que con su smartphone es muy fácil sacarse un selfie y mandarlo en 3 segundos. A María le sabe a poco y le propone quedar por videoconferencia para tener una sesión de cibersexo.

La sorpresa le llega a Mario varios días después, cuando Maria le dice que ha grabado la sesión de cibersexo que tuvieron y que si no quiere que la publique en las Redes Sociales o que se la mande a sus familiares y amigos tiene que pagarle 300€. Mario incrédulo descubre la cruda realidad: Un grupo de personas ha creado un perfil falso en una Red Social, con una foto de una modelo. Ha seleccionado un objetivo, en este caso a Mario. Después de estudiar las fotos que Mario tiene publicadas y todo lo que ha ido escribiendo, ya que Mario no usa los ajustes de privacidad y cualquiera puede ver todo lo que publica, cuando tienen suficiente información se ponen en contacto con él y casualmente “conectan de una forma muy especial”.

Le empiezan a enviar fotos de carácter sexual de a saber quién, y al tener cibersexo, María o como quiera que se llamara la chica, le grabó. Pensándolo bien la chica del cibersexo no se parecía mucho a la chica de la fotos, pero en ese momento tampoco es que importase demasiado. Y ahora, un grupo de desconocidos con quien ha chateado unas cuantas veces tiene un video "íntimo" suyo y amenaza con mostrárselo a familiares y amigos si no paga.

Situación 2: Maria tiene 14 años y Mario 15. A María le gusta mucho Mario y esté se ha empezado a acercar a ella. El problema es que Mario no está convencido de que Maria le quiera de verdad, por eso le pide una prueba de amor, que le mande imágenes de sí misma desnuda. A María al principio le da mucha vergüenza, pero como quiere de verdad a Mario se saca las fotos y se las manda. Mario, al tener las fotos se emociona y se las envía por Whats App a todos sus amigos o las publica en las Redes Sociales y María es humillada.

Situación 3: Mario y Maria tienen 26 años y llevan saliendo 5 años. Hace un tiempo descubrieron el "subidón" que les daba mandarse fotos sexuales y lo hacen de forma habitual. Pero un día todo se acaba y María rompe con Mario. Al poco tiempo alguien se pone en contacto con María diciéndole que ha visto fotos y videos sexuales suyos en una página de web de Internet. María se pone en contacto con Mario y éste le dice que todas las fotos y videos que tenia de ella están en una web pornográfica y que si le mosquea más se las mandará a sus familiares y amigos.

Situación 4: María está tranquilamente en su casa y un día recibe un mail con fotos suyas de carácter intimo. En el mail también amenazan con mandarlas a sus familiares y amigos si no paga una cantidad determinada de dinero. María no entiende cómo alguien puede tener fotos suyas ya que ella nunca se ha sacado fotos ni videos de ese tipo ni ha dejado que nadie le grabara o sacara fotos. Hablando con unos amigos informáticos, descubre que su ordenador estaba infectado con un tipo de software malicioso que permitía al ciberdelincuente usar la webcam del ordenador, incluso cuando la luz no estaba encendida, para sacar fotos y grabar a María sin que se diera cuenta. Este tipo de sucesos aumentan cada día.

Estas situaciones (en las que se pueden cambiar el sexo y la edad de los implicados) son muy habituales y las víctimas son hombres y mujeres de todas las edades, desde adolescentes a jubilados. Pero la vergüenza es tan grande que muchas personas pagan y no lo denuncian. La cantidad de dinero exigida varía en función del perfil de la víctima. A veces, los extorsionadores piden a las víctimas

que se conecten por videoconferencia para grabarles haciendo lo que les dicen y así generar material pornográfico.

La primera situación es muy habitual. Desconocidos estudian y se ponen en contacto con gente "inconsciente" o que se siente sola para intimar con ellos. A veces, cuando llevan un tiempo chateando con ellos, directamente les piden dinero para "coger un avión e ir a verles" o "porque su madre se ha puesto enferma y tiene que ir al hospital".

Otras veces y dependiendo del perfil de la víctima, empiezan a enviar fotos íntimas, de a saber quién, para que las víctimas les respondan. Si ven que lo pueden forzar, intentan llegar al cibersexo. Por si alguien se lo pregunta el cibersexo es algo así como masturbarse delante de la webcam mientras vemos a la otra persona haciendo lo mismo, o hacer strip-tease, tener conversaciones subidas de tono… A veces los extorsionadores utilizan grabaciones de otras personas y para engañar a las víctimas les muestran el video que ellos están reproduciendo en la pantalla en vez del video que está grabando la webcam. En esos videos grabados, el o la protagonista hace saber al "espectador" que no le puede oír para que no sea tan obvio que es un video grabado.

Respecto a los adolescentes, cada vez se está convirtiendo en más "natural" el sacarse fotos de carácter sexual y enviarlas a otras personas, seguramente debido a la gran influencia que el sexo está teniendo en la sociedad. El sexo y las imágenes con gran connotación sexual están muy presentes de una forma o de otra en gran parte de nuestro día a día, ya sea cuando vemos una serie, una película, anuncios en la tele, anuncios en la calle, revistas… es un bombardeo constante. No son imágenes de sexo explícito ni desnudos integrales, pero gran parte de la publicidad que vemos tiene una connotación sensual y sexual muy grande, los "ídolos musicales" y estrellas de cine cada vez son más explícitos y sugerentes en sus apariencias debido a la demanda social (cuanto más sugerente y explícito es algo, más visitas genera en youtube, más vende….) por lo que una vez más debemos pararnos a pensar antes de apoyar este tipo de material comprándolo, viéndolo o dándole difusión en las Redes Sociales. Todo lo que hacemos tiene un impacto.

Recomendaciones

* Nunca contestar o hablar con extraños en las Redes Sociales, y no aceptar a desconocido en las Redes Sociales. No sabemos quién está detrás de ese nombre y esa foto ni qué intenciones tiene.

* Revisar los ajustes de privacidad de las Redes Sociales para que solo nuestros contactos puedan ver las fotos y los comentarios que publicamos. Tampoco vamos a usar las Redes Sociales como un diario para que cualquiera nos pueda conocer mejor que nosotros mismos.

* Tener claro de que si alguien se saca fotos íntimas, una vez que salen de su smartphone, tablet u ordenador ha perdido el control total de ellas. Incluso si la persona a la que se las hemos enviado es nuestra pareja actual y confiamos plenamente en ella, ya no están bajo nuestro control y en el futuro nos podemos encontrar con sorpresas.

* No pagar y poner una denuncia. No hay ninguna garantía de que no vayan a publicarlo ni de que no nos vayan a pedir más dinero.

* Hablar con los adolescentes sobre el concepto del privacidad y los riesgos que conlleva mandar fotos sexuales. A veces los adolescentes se empiezan a mandar fotos sexuales de forma inconsciente porque quieren o les parece gracioso.

* Seguir las pautas de ciberseguridad habituales para no infectar el ordenador con software malicioso, tapar la webcam con un post-it o algo parecido y solo quitarlo cuando la vayamos a utilizar.

* Aprovechamos para recordar el peligro de las apps de ligoteo y de seguir las pautas de seguridad mientras las usamos: No ir a casa de desconocidos, quedar en lugares públicos de día, tener alguien cerca por si acaso. Ejemplos.

Páginas y comunidades dañinas

El que internet sea un lugar libre y todos podamos compartir información es algo muy positivo, pero esta situación también la aprovechan grupos extremistas para engañar y captar adeptos para sus respectivas causas.

Existen grupos violentos especializados en captar adolescentes, o páginas en las que se fomenta la violencia e incitan a los usuarios a realizar acciones, grabarlas y subirlas online. La necesidad de aceptación y la poca autoestima, hacen que algunos adolescentes y no tan adolescentes vayan cayendo poco a poco en las garras de este tipo de grupos.

También hay otras páginas especialmente dañinas que fomentan la anorexia y la bulimia (Ana y Mia) ofreciendo trucos para ocultar que no comen, perder peso, vomitar sin que se note... Artículo publicado.

Este tipo de páginas suelen estar prohibidas, pero sus creadores se las ingenian para camuflarlas y volver a crear otras parecidas cuando los responsables de las Redes Sociales cierran las originales. Por eso es muy importante denunciarlas siempre que las detectemos, para que entre todos hagamos de las Redes Sociales un lugar más seguro.

Desinformación, bulos y mentiras

Las redes sociales pueden ser un foco de desinformación sobre todos los temas imaginables: Desinformación sobre política, intentos de generar miedo y odio sobre grupos o temas determinados, desinformación peligrosa en el ámbito de la salud (lo hemos podido comprobar con el COVID-19 , solo en España se han detectado más de 500 desinformaciones y mentiras al respecto)... debemos tener cuidado con todo lo que leemos y solamente nutrirnos de fuentes fiables.

Siempre conviene verificar la información que leemos, sobre todo antes de compartirla.

Circulan bulos que indican que podemos saber cuantas personas visitan nuestro perfil de twitter o bulos relacionados con funciones adicionales de Whats App o de diferentes redes sociales que nos invitan a descargar herramientas que contienen malware para que infectemos nuestros dispositivos.

También abundan los bulos sobre política, economía, salud… ya ningún tema de conversación está libre en esta nueva realidad en la empieza ser habitual leer una noticia sobre cualquier cosa, y leer lo contrario 5 minutos después. No es fácil ser consciente de que más del 60% de lo que leemos, vemos o escuchamos en Internet es mentira: más del 60% de los mensajes que leemos en WhatsApp, más del 60% de las cosas que vemos en Facebook, Twitter e Instagram, más del 60% de lo que vemos en Youtube… más del 60% es mentira. Y algunas de estas mentiras y desinformaciones puede ser peligrosa para nuestra salud, e incluso pueden desencadenar verdaderos desastres como podemos ver en esta noticia.

Otras mentiras nos incitan al miedo y a realizar acciones rápidas y sin sentido como compartir cadenas de mensajes por miedo a que nos pase algo como que “tengamos que pagar el Whats App”.

Los ciberdelincuentes se aprovechan de que todo este mundo es muy nuevo para muchos y de nuestra ingenuidad. Debemos desarrollar un sentido común “cibernético”. Se aconseja no compartir las noticias que nos llegan antes de verificarlas, ya que algunos bulos se hacen virales, es muy difícil detener su propagación y colaboramos son saberlo con los ciberdelincuentes o compartimos desinformación.

¿Cómo puedo detectar la desinformación y las mentiras?

Para detectar desinformación podemos seguir las siguientes pautas:

- Si leemos algo en redes sociales o nos llega algo a través de apps de mensajería, lo que nos llegue tiene que tener un enlace a una página oficial, si no directamente no le haremos caso. Cualquiera puede escribir algo y difundirlo con diferentes intereses.

- Cuando leamos una noticia, por un lado nos aseguraremos de que el medio de información en el que estamos es legítimo y por otro lado leeremos toda la noticia, muchas veces los titulares son llamativos pero el resto de la noticia no tiene sentido o no tiene nada que ver con el titular.

- En esta época en la que afloran muchos medios de comunicación digitales nuevos, para saber si un medio es fiable podemos ver el tipo de noticias que publican. Si todas son sobre el mismo tema, tienen un tinte agresivo y titulares muy llamativos no es fiable. También podemos buscar el medio en un buscador para ver qué opiniones tiene.

- Cuidado con los estudios. Cuando leamos una noticia que haga referencia a un estudio, tiene que tener un enlace que nos lleve al mismo, si no lo tiene no haremos caso. Si tiene enlace, iremos al estudio y leeremos el resumen para ver si tiene relación con la noticia. Si no la tiene no haremos caso. Si la tiene, leeremos por encima el estudio para ver si tiene coherencia con la noticia. Si no tiene coherencia no haremos caso. Si la tiene debemos recordar que un estudio aislado nunca demuestra nada, para que un estudio tenga validez tiene que repetirse más veces y dar el mismo resultado.

- Siempre que leamos algo, podemos buscarlo en un buscador de Internet para comprobar si medios de comunicación fiables están informando sobre ello.

- Usar servicios online de “fact - checking”, comprobación de datos veraces. Un ejemplo español y otro internacional.

¿Sabes qué información estás dando?

Muchas veces compartimos cosas en las redes sociales sin ser conscientes de toda información que estamos ofreciendo:

Fotos

Al compartir fotos, todo el mundo que tenemos agregado en las redes sociales puede ver y descargar las fotos. Si no tenemos los ajustes de privacidad bien configurados, cualquier persona podría ver y descargar las fotos que compartimos.

A través de fotos podemos dar información sobre los lugares que frecuentamos y nuestras rutinas diarias. Si sacamos fotos en casa podemos mostrar si tenemos cosas de valor, dónde vivimos, nuestros sistemas de seguridad, cerraduras... También podemos tener carteles con información privada (en calendarios en las cocinas, notas en el frigorífico o en corchos de cuartos con números de teléfono, citas...). Se recomienda mirar lo que vamos a publicar antes de publicarlo, y si vemos que estamos dando mucha información publicar otra cosa.

Si en la foto aparece un niño el riesgo aumenta porque cualquiera puede saber dónde vive, qué parque frecuenta... No se recomienda subir fotos de niños a las redes sociales. Tenemos que aprender a respetar su privacidad, bueno, la suya, la nuestra y la de los demás.

Menos aún, se recomienda subir fotos de niños pequeños desnudos. Nos puede parecer que están muy salados en la piscinita, o en la playa, pero la verdad es que muchos enfermos utilizan todas las fotos que encuentran para hacer montajes bastantes desagradables, y esa foto que nos parecía tan bonita, deja de serlo si alguien la coge, recorta al niño y lo pone al lado de un hombre desnudo de 50 años.

Los padres son los mayores paparazzis que existen y según un estudio de The Parent Zone (UK), los padres habrán subido 1000 fotos de sus hijos a las redes sociales antes de cumplir 5 años. Muchos de ellos ignoraban que al subir una foto, también cedes a Facebook los derechos de esa foto para que haga con ella lo que quiera. Incluso hay quien sube fotos de las ecografías. Aún no ha nacido y ya está a la vista de todo el mundo. Artículo sobre “sharenting” en nuestro blog.

Estas precauciones también hay que tenerlas a la hora de realizar diferentes retos que hay en las redes sociales, ya que en el fondo estamos publicando fotos y videos y podemos dar mucha información.

Retos virales y apps

De vez en cuando se viralizan diferentes cosas en redes sociales, muchas de ellas relacionas con apps para smartphones. Por ejemplo, ya se han realizado varios retos relacionados con las app FaceApp, que a través de filtros de caras podemos ver cómo seríamos si fuésemos más mayores, o del sexo contrario.

Tenemos que tener cuidado con los permisos que damos a las apps, y conviene leer sus políticas de privacidad antes de usarlas. En concreto las apps que piden permiso a las galerías pueden ver las fotos que tenemos en ellas y muchas buscan fotos de documentos importantes como DNIs, pasaportes...

La app FaceApp, en su política de privacidad establece que les damos permiso para quedarse con todas las fotos que utilicemos, para que hagan lo que quieran con ellas, para venderlas y que incluso si FaceApp tuviese diferentes propietarios en el futuro, les cederíamos también los permisos.

También conviene leer la política de privacidad de las redes sociales, como por ejemplo la de TikTok, donde entre otras cosas recopilan el contenido del portapapeles de nuestros dispositivos, y utilizan la "precarga": todas las fotos y videos que saquemos con la cámara de TikTok, da lo mismo que los dejemos en borradores, los publiquemos o los borremos, van directamente a los servidores de TikTok, sin filtro. Hay una gran preocupación a nivel mundial por los problemas que TikTok supone para nuestra privacidad.

Apps de terceros

Hoy en día existen diferentes dispositivos que nos ayudan a monitorizar nuestra actividad física. Ya sean relojes, pulseras o diferentes aparatos, llevan un recuento de cuánto andamos, cuánto hemos corrido, nuestras pulsaciones... Muchos de estos aparatos vienen con apps específicas para nuestro smartphone o tablet, y a su vez tienen sus redes sociales en sus páginas web donde podemos ver los recorridos que otros hacen, sus tiempos...

Debemos tener cuidado porque por defecto, sin que hagamos nada, todo lo que hacemos es público hasta que no digamos lo contrario, por lo que cualquiera que esté dado de alta en esa página puede ver por dónde andamos y a qué horas, el ejercicio que hacemos... Conviene ir a esa web y establecer los ajustes de privacidad para que sólo quienes nosotros queramos puedan ver esa información.

Consejos para aumentar la seguridad

Verificación de dos pasos

La mayoría de redes sociales, servicios online y correos electrónicos disponen de un sistema adicional de seguridad llamado “verificación de dos pasos”. Esta verificación generalmente utiliza nuestro teléfono móvil mandándonos un mensaje de texto para asegurarse de que somos nosotros los que queremos entrar en nuestra cuenta. Es muy importante activar la verificación en dos pasos en todas las cuentas en las que se pueda.

Para activar esta función iremos a Configuración-> Seguridad.

Algunas también disponen de una función llamada “Inicios de sesión” que nos puede avisar si alguien intenta acceder a nuestras cuentas desde dispositivos o ubicaciones no habituales. Configuración->Seguridad.

Ajustes de privacidad

En las redes sociales conviene revisar los ajustes de privacidad para limitar quienes pueden ver nuestra información, las cosas y fotos que publicamos y también conviene hacer una limpieza de las personas que tenemos agregadas que no conocemos, ya que como no las conocemos no sabemos sus “intenciones”.

Imaginemos que las redes sociales son como nuestra casa. ¿Dejaríamos que cualquiera entrase y viese nuestras fotos, información personal y que se llevase lo que quisiera? ¿Y por qué en las Redes Sociales sí lo hacemos?

¿Cómo puedo comprobar si alguien ha entrado en mi cuenta?

En la mayoría de las redes sociales, en el apartado seguridad de la configuración también podemos ver un apartado que se llama “Inicios de sesión”.

A través de esta función veremos si hay alguien que está entrando a nuestra cuentas con otros dispositivos que no sean os nuestros.

Si vemos que hay alguien, justo al lado de esta opción en los tres puntitos podremos cerrar esas sesiones para forzarles a salir de las cuentas.

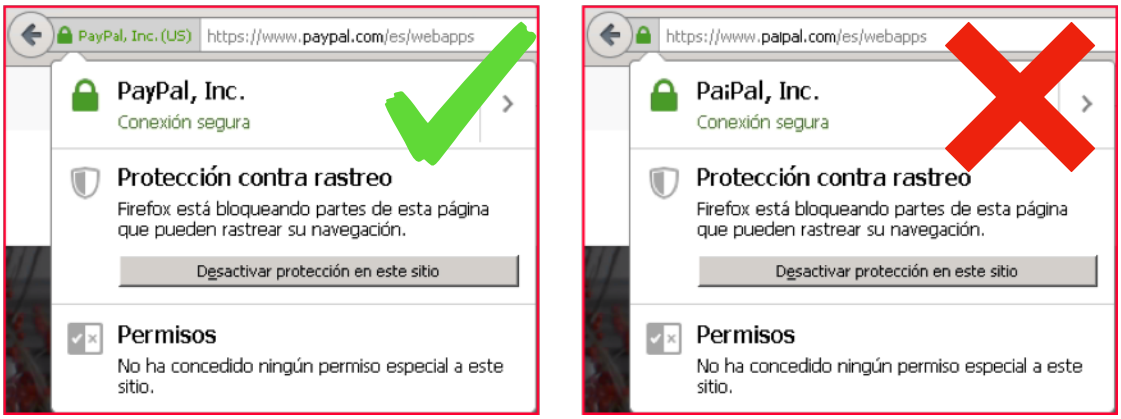
Justo después cambiaremos la contraseña y activaremos la verificación o autenticación en dos pasos.

Aquí os dejo un video de cómo se hace en Instagram, en el resto de las redes sociales los pasos son los mismo: Configuración -> Seguridad -> Inicios de sesión.

Podéis aprender a proteger más lugares desde la web de macsonrisas.

Consejos para realizar compras online

Se aconseja mirar siempre la dirección de la página en la que nos encontramos, la URL, hay muchas páginas falsas intentando suplantar tiendas y servicios online.



En tiendas que no conocemos, debemos verificar el número de teléfono y la dirección física, si disponen de ella o buscarla en los buscadores para ver las opiniones que hay de ella.

Conviene revisar la política de privacidad y de devoluciones. Parece obvio, pero tenemos que saber cuánto vamos a pagar y qué vamos a pagar. Esto quiere decir que miraremos si los precios que aparecen son con IVA o sin IVA y siempre tenemos que sumar los gastos de envío. También miraremos la letra pequeña de los productos para saber exactamente qué es lo que se vende.

Si compramos fuera de nuestro continente debemos mirar si al precio se le sumarán los gastos de aduanas o no, por eso también lo de leer la letra pequeña.

Si compramos algo, nunca vamos a pagar a través de transferencias ni vamos a enviar dinero en efectivo, ni vamos a mandar nuestra información financiera por mail. Siempre realizaremos los pagos a través de Paypal o a través de la pasarela de pago seguro de cada comercio online, fijándonos que en la barra de direcciones aparezca el candado blanco o verde o https://. Si alguna vez nos fijamos en que no esta ni https:// ni el candado, directamente saldremos de la página.

Siempre conviene ver las opiniones que otros usuarios tienen de ese producto. Si compramos en una tienda online que puede tener diferentes vendedores, debemos mirar quién es el vendedor de ese producto concreto y qué reputación y puntuación tiene.

También es importante realizar estas compras utilizando la tarifa de datos de nuestros dispositivos o conectándonos a redes wifi seguras, evitaremos las redes wifi públicas que no tienen contraseña, y aquellas de lugares donde se conecta mucha gente como restaurantes, bibliotecas, hoteles…

Capítulo 5
Contraseñas y seguridad

Las contraseñas son la única protección que tenemos en nuestros correos electrónicos y redes sociales. Por eso es muy importante tener contraseñas seguras y cambiarlas de forma habitual.

Recomendaciones para crear contraseñas

- Como mínimo deberán tener 8 caracteres, un número, una mayúscula y una minúscula. Cuanto más caracteres tenga, más segura será la contraseña.

- El uso de símbolos aumenta la seguridad: “$#/-…

- Evitaremos poner como contraseñas cosas relacionadas con nosotros tales como fechas de cumpleaños, fechas de aniversarios, nombres, apellidos, nombres de padres, hijos…

- En las preguntas de seguridad para la recuperación de contraseñas, también evitaremos introducir información personal como nombre de de los padres, mascotas…

- Cambiaremos las contraseñas de forma regular cada 6 - 8 meses.

- Las contraseñas son secretas, por lo que no debemos compartirlas con nadie, y menos a través de correos electrónicos, mensajes o diferentes formas de comunicación digital.

- Tendremos una contraseña diferente para cada servicio. Evitaremos tener las contraseñas apuntadas en cuadernos, folios, documentos de Word… Podemos usar gestores de contraseñas para acordarnos y tenerlas organizadas.

- Evitaremos patrones. Por ejemplo en Facebook Facebook123, en Paypal Paypal123…

- Hay quienes piensan en una frase y utilizan la primera letra de cada palabra como contraseña, o miran lo que tienen delante y los escriben incrustando en el medio un símbolo y algún número.

Gestores de contraseñas

Existen diferentes apps dedicadas a la gestión de contraseñas. Estas apps tienen una única contraseña de acceso que tenemos que recordar y al acceder podemos organizar todas nuestras contraseñas. Suelen ser multiplataforma, de forma que podemos sincronizar las contraseñas entre las aplicaciones de los diferentes dispositivos (smartphone, tablet, ordenador) y las podemos tener siempre disponibles. Eso sí, como se nos olvide la contraseña principal perderemos toda la información.

Las aplicaciones buenas siempre tienen un coste, no hay aplicaciones gratuitas buenas relacionadas con la seguridad. Podemos encontrar aplicaciones como 1Password, Keeper, Lastpass, Dashlane...

Tanto iOS como los últimos sistemas operativos de Android traen gestores de contraseñas integrados en sus sistemas.

Verificación en dos pasos

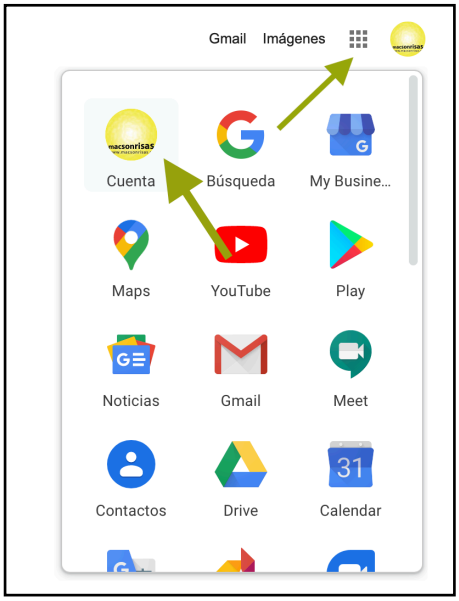
La verificación en dos pasos es un proceso de seguridad que se está instaurando en la mayoría de servicios online. Además de introducir un nombre de usuario y contraseña, nos mandan un código a través de un mensaje a nuestro teléfono móvil.

Esta verificación se utiliza también cuando intentamos acceder a nuestra cuentas desde dispositivos que habitualmente no utilizamos.

Para activar la verificación de dos pasos, iremos a la configuración del servicio en cuestión, al apartado de seguridad y allí la activaremos.

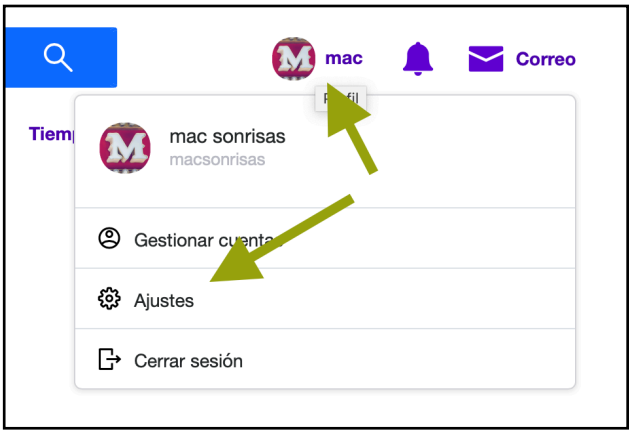
De la misma forma que en el capítulo anterior hemos visto cómo se activaban en Redes Sociales, la activaremos en correos electrónicos y demás servicios online.

Aquí os dejo unos ejemplos de cómo se activa la verificación en dos pasos en Google, en Yahoo y en Outlook.



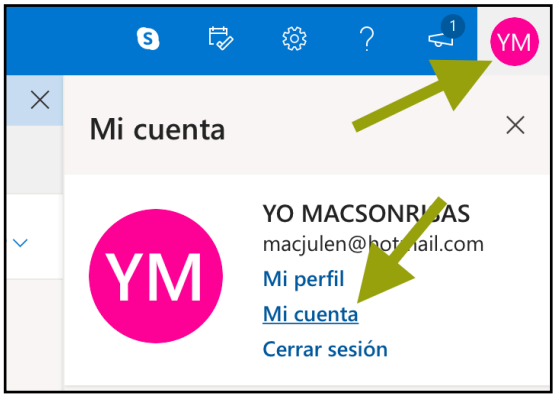
Verificación Google

Iniciando sesión vamos a nuestra cuenta y allí al apartado seguridad.



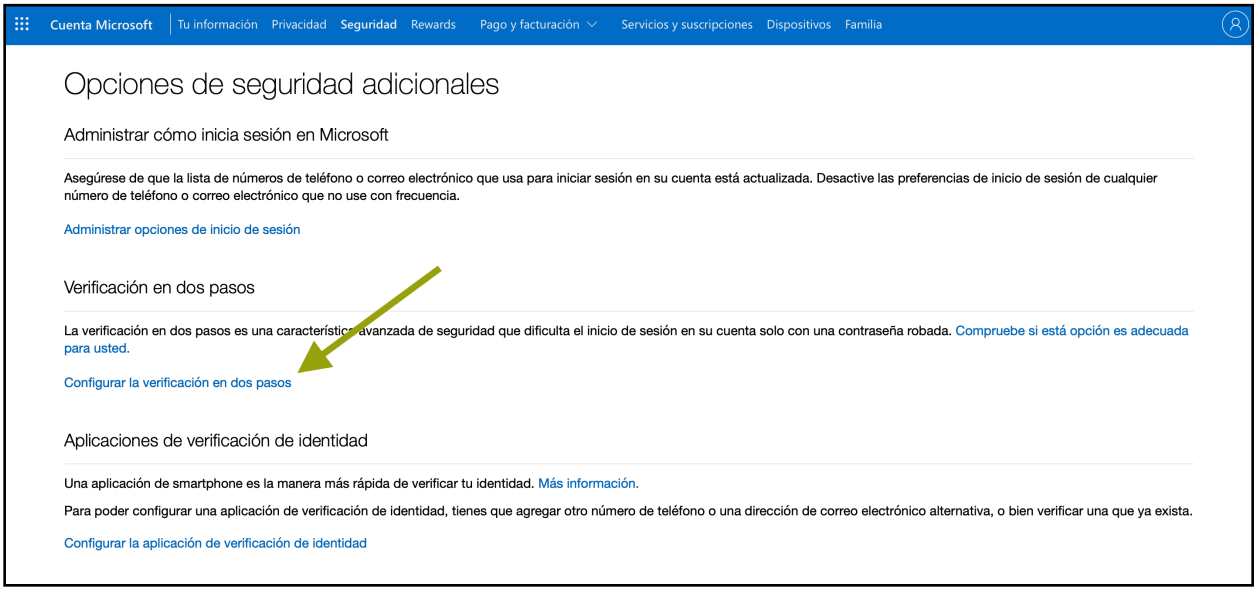
Verificación Yahoo

Iniciando sesión vamos a nuestra cuenta y allí al apartado seguridad.



Verificación Outlook

Iniciando sesión vamos a nuestra cuenta y allí al apartado seguridad.



Verificación Outlook II

Vamos a Más opciones de seguridad y configuramos la verificación en dos pasos.

Otras medidas de seguridad

Evitaremos introducir nuestros datos en formularios online o en formularios físicos. Es muy habitual que muchas empresas sorteen productos y nos pidan datos de contacto como nuestro correo electrónico.

Esa es una de las formas en las que nuestro correo electrónico puede acabar en manos de ciberdelincuentes. Esa empresa vende la información a otra empresa que la vende a otra empresa o esa empresa es atacada por ciberdelincuentes que se quedan con la información para sus actividades.

Tendremos mucho cuidado con los mails masivos, los que se mandan a mucha gente. Aunque hace mucho tiempo que se viene avisando, hay quien todavía envía emails a muchas personas a la vez sin usar el campo de “copia oculta” o CCO, de forma que todos las direcciones de correos quedan visibles. Si recibimos algún mail así, conviene avisar a la persona que lo ha mandado para que deje de hacerlo.

Hay que ser precavidos a la hora de utilizar servicios online para guardar información, las famosas “nubes”:

Las “nubes” son servidores que se encuentran en diferentes países. Hay que tener cuidado con la información que se pone porque depende del país, puede ser ilegal. Archivos con derechos de autor, Copyright…

Evitaremos poner información sensible y privada como números de DNI o copias, números de seguridad social, contraseñas…

Si tenemos información importante usaremos la nube para tener una “copia de seguridad”, no como ubicación principal.

Capítulo 6
Móviles seguros

En este capítulo, a modo de resumen, recordaremos todos los hábitos que conviene desarrollar para usar nuestros smartphones y tables de forma segura. También veremos consejos que no hemos comentado en anteriores capítulos.

Consejos

Activar el bloqueo de pantalla con código: Conviene proteger teléfono con el bloqueo de pantalla, de esta forma si alguien se hace con el dispositivo no podrá entrar en ese momento para ver su información.

Evitar rootear ni hacer jailbreak en los dispositivos móviles: Estas acciones eliminan la seguridad de los dispositivos. Si no sabes lo que es eso, mejor.

Se recomienda desactivar el wifi al salir de casa. Si vamos con el Wifi activado por la calle, cada vez que nuestros dispositivos detectan una red Wifi se produce una "conversación" entre el dispositivo y la red. La red le pregunta si quiere conectarse, y si el dispositivo no responde, se conecta o no se conecta, pero la red tiene la opción de preguntarle a qué otras redes se ha conectado, con lo que pueden realizar un seguimiento de los lugares en los que nos hemos conectado o el dispositivo haya detectado una red Wifi.

Se recomienda desconectar el bluetooth cuando no lo utilicemos. Es una forma de evitar que terceros intenten conectarse a nuestros dispositivos.

Cuidado con las redes Wifi públicas. Evitaremos el uso de las redes Wifi públicas, aquellas que no tienen contraseña, ya que cualquiera puede estar monitorizando la actividad en la red y recopilando datos que se envían y se reciben. También corremos el riesgo de que ciberdelincuentes entren en nuestros dispositivos, vean y recopilen información.

Cuidado con las redes Wifi no públicas de lugares públicos. Aunque la red Wifi esté protegida con contraseña, si es una red de un lugar con mucha afluencia de gente como pueden ser bibliotecas, restaurantes, hoteles... mucha gente puede estar conectada a la misma red y puede haber alguien viendo los datos que se envían y se reciben.

En cualquier caso, en ambas redes evitaremos loguearnos, es decir, evitaremos introducir nuestros nombres de usuarios y contraseñas en diferentes servicios online como bancos, tiendas, correos electrónicos o redes sociales.

Cuidado con los links y con las imágenes cuyo origen desconocemos.

Se recomienda no apuntar los nombres de usuarios y las contraseñas en las notas del teléfono. No es seguro, ya que si alguien coge el teléfono, todas las contraseñas se verán comprometidas. Para guardar y gestionar contraseñas existen diferentes aplicaciones específicas. Se llaman “gestores de contraseñas”. Únicamente tenemos que recordar una contraseña maestra para entrar en la aplicación, y una vez allí podremos apuntar, organizar y gestionar todas las contraseñas de todos los lugares que disponemos.

Descargaremos apps solamente desde tiendas oficiales, como Google Play o App Store y siempre actualizaremos las aplicaciones que tengamos instaladas, ya que muchas veces no se dice pero muchas actualizaciones traen mejoras de seguridad. A veces los desarrolladores de las aplicaciones detectan vulnerabilidades y las solucionan a través de las actualizaciones, pero si nos dijesen cada dos por tres que han detectado vulnerabilidades y que las están solucionando, seguramente dejaríamos de comprar o utilizar esas aplicaciones.

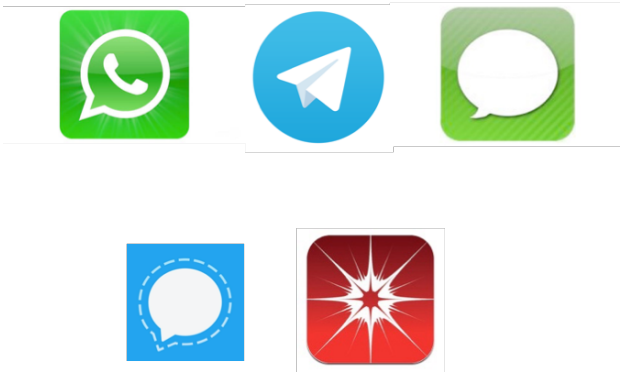
Conviene tener el sistema operativo siempre actualizado. Siempre que las características de los dispositivos nos lo permitan, debemos actualizarnos. Las actualizaciones de los sistemas operativos también traen mejoras de seguridad entre otras cosas.

Antivirus siempre, gratuito o de pago. En todos los smartphones menos en iOS (Apple) que aún no podemos instalarlos.

Se recomienda tapar las cámaras de los teléfono, por lo menos las delanteras, ya que hay malware que las activan sin nuestro permiso.

Apps de mensajería

En lo que a seguridad se refiere, cada app de mensajería tiene diferentes niveles de seguridad y de privacidad, con lo que cada uno tendrá que elegir una app de mensajería dependiendo de cual es su prioridad. Tendremos que preguntarnos qué tipo de información vamos a compartir y en función de eso sabremos que tipo de seguridad necesitamos.



WhatsApp: Si hablamos de las aplicaciones de mensajería más conocidas, Whats App es la más extendida. Últimamente han añadido la encriptación de punto a punto para hacer las conversaciones más seguras y para que no puedan ser intervenidas por terceros.

Telegram: Telegram es un poco más segura que Whats App, con un nivel de encriptación que nadie ha conseguido romper y con chats secretos, pero tampoco es del todo privada.

iMessage: De las apps de mensajería conocidas más seguras y privadas, las más conocidas es iMessage de Apple.

Signal: La app Signal nos ofrece la opción de mandar mensajes encriptados y realizar llamadas encriptadas, es una de las apps de mensajería más seguras y privadas que hay.

Wickr: Esta app utiliza una encriptación de nivel militar en el envío de mensajes de texto, fotos y videos, y además nos permite controlar durante cuánto tiempo pueden ver los destinatarios los mensajes antes de ser borrados. Esta última opción está muy bien, pero recordad que siempre se pueden hacer capturas de pantalla.

Apps cotillas

Cuando descargamos una app, debemos fijarnos siempre en la información que quiere usar de nuestro smartphone o tablet, y para qué. Algunas apps piden usar nuestra localización para mejorar su servicio, otras nuestro calendario, otras nuestros contactos... En algunos casos esa solicitud está justificada. Por ejemplo, las apps de mensajería nos piden acceder a nuestros contactos para mandar mensajes, o twitter nos pide acceso a la localización para geolocalizar los tweets si queremos. Hasta ahí bien.

Pero hay una serie de apps que sin ninguna justificación quieren acceder a toda la información posible de nuestros dispositivos. Tenemos que desconfiar de este tipo de apps ya que son un intento de robarnos información. Un ejemplo de este tipo de apps fue el popular juego “Angry birds”. Este juego tan extendido accedía a toda la información de la que disponíamos en nuestro dispositivos por defecto. De hecho, información revelada por Edward Snowden a principios de 2014 indicaba que agencias espías estadounidenses e inglesas podrían estar detrás de este tipo de aplicaciones para recolectar información de los usuarios sin su consentimiento.
Antes de descargar una app, en Google Play de Android podemos ver a qué información quiere acceder la aplicación fijándonos en los permisos. Si es una aplicación metereológica es normal que pida acceso a nuestra ubicación, pero si pide acceso a nuestros contactos, podemos empezar a sospechar.

Tanto en iOS como en Android, en los ajustes de privacidad podemos elegir a qué información vamos a dar acceso a cada aplicación. Si detectamos aplicaciones cotillas, conviene eliminarlas inmediatamente. Tenemos que ser cuidadosos a la hora de instalar apps en nuestros smartphones y tablets.

Apps de seguridad

Conviene usar las funciones o aplicaciones para buscar el teléfono en caso de pérdida o robo. En iOS viene de serie las aplicación “Buscar mi iPhone” y en Android viene “Buscar mi móvil”.

También hay diferentes tipos de apps que nos pueden ser útiles para mejorar nuestra seguridad

Buscar Mi iPhone

Características de Buscar mi iPhone (también es compatible con el iPad):

- Localiza tu iPhone, iPad, iPod touch o Mac en un mapa.
- Reproduce un sonido durante dos minutos a máximo volumen (incluso aunque el dispositivo esté en silencio).
- Bloquea tu dispositivo de forma remota con un código.
- Muestra un mensaje personalizado en la pantalla bloqueada.
- Consulta el historial de ubicaciones recientes de tu dispositivo en el modo Perdido (dispositivos con iOS).
- Obtén indicaciones hasta la ubicación del dispositivo.
- Borra de forma remota todos los contenidos y ajustes de tu dispositivo.
- Indicador de carga de la batería.

Para que esta app funcione iCloud tiene que estar activado, y dentro de iCloud tiene que estar activada la opción “Buscar mi iPhone”. Esta activación hace que ese iPhone, iPad o Mac se quede asociado a la iD de Apple con la que hemos activado iCloud.

Además, si alguien nos roba nuestro dispositivo, no podrá restaurarlo ni desactivarlo a menos que conozca nuestra ID de Apple y la contraseña. Esto junto con la pantalla de bloqueo, hace muy difícil que delincuentes puedan usar o vender nuestros dispositivos.

Prey Antirobo tiene diferentes funcionalidades para iOS y Android:

- SEGURIDAD MÓVIL: Alarma anti silencio, bloqueo remoto…
- REPORTES DE EVIDENCIA DE ROBO: Coordenadas GPS y Mapas, toma fotografías para intentan conocer la ubicación, mira redes wifi cercanas para intentar ubicarlo…
- SEGURIDAD DE DATOS: Borrado remoto, recuperación de datos y cifrado de datos hasta recuperar el dispositivo...

- Características de **Where's My Droid** (Android):
- Obtiene la locación GPS del teléfono.
- Alerta de ubicación al descargarse la batería.
- Activa el timbre/vibrador del teléfono.
- Activa cada característica vía texto.
- Utiliza nuestro sitio web Commander para activar cada característica.
- Protección con clave para evitar cambios no autorizados en la aplicación.
- Notificación en caso de cambios de tarjeta SIM o de número.
- Modo Oculto esconde los textos con mensajes de atención.
- Lista Blanca/Negra sobre quiénes pueden utilizar la aplicación vía texto.

- No gasta la batería.
- Características de Seguridad Avanzadas en la versión Pro.
- Saca fotos con la cámara del dispositivo.
- Bloquea el dispositivo de forma remota.
- Borra el dispositivo y la tarjeta SD de forma remota.
- Evita la desinstalación.
- Esconde el ícono de la aplicación.

Stash es un ejemplo de app que nos permite tener fotos, videos y archivos protegidos mediante contraseña en nuestros dispositivos Android.

File Locker es un ejemplo de app que nos permite tener fotos, videos y archivos protegidos mediante contraseña en nuestros dispositivos Android.

VPN (Virtual Private Network, Red Privada Virtual, en español), es el término que se usa para definir una red de comunicaciones que usa la infraestructura de Internet para conectarse de forma remota a diferentes redes.

Las VPNs requieren autorización, autenticación y usan criptografía. Los usuarios deben estar registrados y autorizados para acceder la red. Además toda la información que se transmite está codificada, lo que aumenta considerablemente el nivel de seguridad de la comunicación.

Por ejemplo, de esta forma podremos acceder a nuestro correo electrónico de trabajo si este no se puede configurar en dispositivos móviles por temas de seguridad.

Así también podremos navegar por internet de una forma más privada y segura con nuestros dispositivos móviles.

Existes diferentes aplicaciones de VPN para dispositivos móviles como **Proton VPN, HotsSpot Shield, Tunnelbear VPN o PureVPN**.

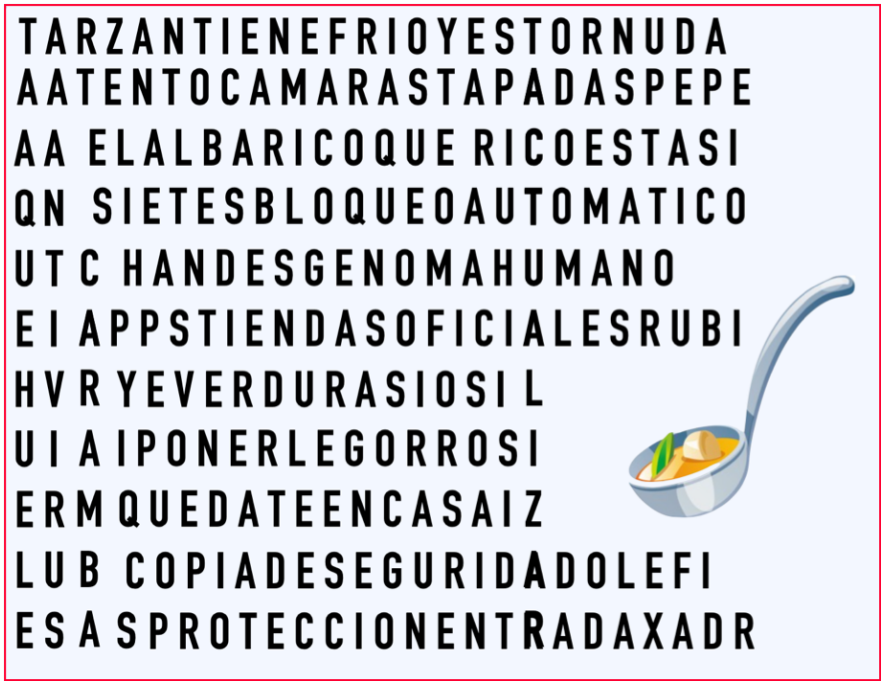
En capítulos anteriores ya hemos hablado sobre un software para Android llamado Conan Mobile que ha sido desarrollado por INCIBE (Instituto de Ciberseguridad) y que analiza nuestro dispositivo informándonos de si hay aplicaciones “maliciosas” y de posibles vulnerabilidades de seguridad que pueda tener.

Vuelvo a hacer hincapié en que si vamos a descargar cualquier programa, siempre lo haremos a través de tiendas oficiales o desde la página del desarrollador de cada programa.

Existen diferentes apps dedicadas a la gestión de contraseñas. Estas apps tienen una única contraseña de acceso que tenemos que recordar y al acceder podemos organizar todas nuestras contraseñas.

Algunas apps como 1Password además traen un navegador seguro incorporado para que podamos navegar por internet de forma segura si queremos.

En esta sopa de letras vienen 7 pautas para proteger ordenadores y smartphones, a ver si eres capaz de encontrarlas.



Capítulo 7
Ordenadores seguros

Es muy importante tener las pautas de seguridad interiorizadas para no lidiar con situaciones que nos generen dolores de cabeza. Muchas personas piensan que teniendo un antivirus tanto en ordenadores como en los móviles ya no hay de qué preocuparse, pero están muy equivocadas porque los antivirus detectan generalmente el 65% de los virus o malware. Las nuevas variantes de virus y malware pueden no ser detectadas hasta pasados unos días desde su creación, por eso es fundamental seguir las pautas de ciberseguridad.

Consejos

Podemos seguir estos consejos para aumentar la seguridad de nuestros ordenadores:

- Crearemos una cuenta de usuario de administrador que no utilizaremos, y trabajaremos en una cuenta de usuario estándar. Si algún tipo de malware se introduce en nuestro ordenador, no dispondrá de los permisos necesarios para propagarse o hacer lo que quiera.

- Se recomienda tener un Antivirus de pago siempre actualizado.

- Protegeremos el ordenador con contraseña, para que cualquiera no pueda entrar a fisgonear en cuanto nos descuidemos.

- Realizaremos copias de seguridad de forma habitual.

- Podemos crear una cuenta de usuario solamente para invitados, para que cuando alguien venga a casa pueda utilizar el ordenador sin que nos pueda ver archivos, cambiar preferencias, eliminar cosas…

- Si tenemos un ordenador de sobremesa, siempre es conveniente tenerlo enchufado a una regleta que proteja contra las subidas de tensión.

- Tendremos el Firewall siempre activado.

- Tendremos tanto los programas como el sistema operativo siempre actualizados.

- Se recomienda tapar las cámaras de los ordenadores.

- Evitaremos las descargas de música, películas y programas ilegales.

- Protegeremos los navegadores con las extensiones o complementos necesarios para hacer más segura la navegación por internet. Se recomienda instalar “Adblock” o similar para bloquear la publicidad, y “Trafic Light” para que nos indique qué páginas son seguras y cuales no.

- Tendremos cuidado con links y páginas fraudulentas.

- Andaremos con cuidado con USBs de origen desconocido, no sabemos si están infectados o no.

Buscadores privados

Aunque tiene que ver más con privacidad que con seguridad, últimamente el buscador DuckDuckGo ha ido ganando popularidad entre los usuarios de internet que están cansados de que Google y otros buscadores vayan recopilando toda la información que pueden sobre ellos.

DuckDuckGo es un buscador que protege nuestra privacidad al máximo. A diferencia de otros buscadores, no guarda ningún dato sobre nosotros ni sobre nuestra navegación.

Navegadores privados

Existen alternativas al navegador Chrome de Google. Chrome es un navegador muy cotilla que recopila todo lo que hacemos en internet. Podemos usar el navegador Focus de Firexos, Duck Duck Go también ha sacado su propio navegador u otros navegadores como Brave.

TOR es uno de los navegadores más privados que existen.

Consejos adicionales para puestos de trabajo

- No entraremos a las cuentas de correo personales ni a redes sociales personales desde el ordenador del trabajo.

- Evitaremos cargar los móviles en los ordenadores del trabajo.

- Avisaremos al responsable cuando detectemos que el ordenador hace cosas fuera de lo habitual: Apagarse solo, reiniciarse, parpadeos de pantalla…

- Si hay muchos usuarios usando un ordenador de trabajo, estableceremos los permisos necesarios para cada uno.

- Si vamos a comprar diferentes productos físicos de seguridad, nunca se lo compraremos todo al mismo proveedor, ya que si algún producto tiene una vulnerabilidad todas los productos también la tendrán.

- En materia de seguridad la confianza no existe. Antes de comprar un producto a una empresa, consultaremos a diferentes clientes que ya lo hayan comprado para saber si están contentos o no y realizaremos una pequeña investigación en internet para tener más referencias. Los comerciales nos informarán muy bien de las características porque hacen muy bien su trabajo, pero su trabajo es ese, venderlo.

Routers infectados

Los routers también pueden ser infectados, por lo que se recomienda tener siempre actualizado el firmware del router a la última versión. Si no sabemos hacerlo, conviene llamar a la compañía telefónica para que nos ayuden en el proceso. De vez en cuando, también conviene resetear su configuración.

Tanto en casa como en el centro de trabajo conviene cambiar el nombre y la contraseña de la red wifi que viene con el router.

Recordar que siempre que haya algo que no sepamos hacer tenemos un montón de videotutoriales en Youtube que nos ayudan a hacer todo lo que necesitemos.

Agradecimientos

Gracias

Gracias por comprar este libro interactivo. Si os interesa la ciberseguridad podéis seguirnos en Facebook (@macsonrisas) o Instagram (@macsonrisas2.0) además de visitar páginas interesantes como la Oficina de Seguridad del Internauta o el Instituto de Ciberseguridad, así como www.macsonrisas.es.

Algunas de las imágenes son cortesía de AKARAKINGDOMS, Salvatore Vuono, Stuart Miles, Boians Cho Joo Young, zdiviv, iosphere, twobee, lamnee, hyena reality y Mister GC a través de FreeDigitalPhotos.net y Tsahi Levent-Levi y jaymzg a través de Flickr. Muchas gracias por hacer este libro más bonito.

Recordad que también ofrecemos formaciones sobre educación digital a particulares, familias, empresas, asociaciones, centros educativos...

Más información en www.macsonrisas.es o en info@macsonrisas.es.