Manual de privacidad y seguridad en internet

Diego Chiquero Mena

29 abril 2025

Privacidad & **Seguridad** en internet

UN MANUAL DE LECTURA RECOMENDADO PARA CONOCER Y PROTEGERNOS DE LOS ***CIBERATAQUES***

Índice

Prólogo **8**

Sobre el autor **10**

1 Privacidad y Seguridad en Internet **11**

1.1 Introducción 11
1.2 Privacidad 12
1.3 Seguridad 12
1.4 RGPD (Reglamento general de protección de datos) 13
1.5 Aviso legal, política de privacidad y política de cookies . . . 13
1.6 Derechos ARCO 14
1.7 Derechos POL 15

2 Gestión de la privacidad **16**

2.1 Gestionar la privacidad 16
2.2 Datos personales sensibles 16
2.3 Oversharing o sobreexposición 17
2.4 Privacidad en tus cuentas 17
2.5 Navegación privada 18
2.6 VPN (Red privada virtual) 19
2.7 Cookies 20
2.8 Permisos cámara, micrófono y localización. 23
2.9 La nube 25
2.10 Correo electrónico y apps de mensajería 25
2.11 Cifrado o encriptado de datos 26
2.12 He decidido vender o donar mi dispositivo 27

3 Gestión de la seguridad en equipos físicos **28**

3.1 Gestionar la seguridad en los equipos 28

3.2 Cuenta de usuario en equipos locales y dispositivos móviles . 28

3.3 Router 30

3.4 Actualizaciones 31

3.5 Antivirus, antimalware, antispyware y firewall 31

3.6 Copias de seguridad 32

3.7 Cifrado o encriptado de unidades de almacenamiento 34

4 Gestión de la seguridad en la red **36**

4.1 Gestionar la seguridad en la red 36

4.2 Seguridad en las cuentas 36

4.3 Contraseñas 37

4.4 Protocolo https 40

4.5 Compras y transacciones 41

4.6 Wi-Fi 43

4.7 Plugins o extensiones 43

4.8 Descargas 44

4.9 Cierre de sesiones 45

4.10 2SV (Two Step Verification) o Verificación en Dos Pasos . . 45

4.11 MFA (Multi-Factor Authentication) o Autenticación de Factores Múltiples 46

4.12 AntiBotnet 48

4.13 Bluetooth 48

4.14 NFC (Near field communication) 49

5 Amenazas **50**

5.1 Principales amenazas 50

5.2 Virus 52

5.3 Gusanos informáticos 52

5.4 Troyanos 53

5.5 Ransomware o programa rescate 53

5.6 Spyware o software espía 55

5.7 Adware 56
5.8 Malvertising 56
5.9 Scareware o rogueware 57
5.10 Quishing 57
5.11 Phishing 58
5.12 Vishing 62
5.13 Smishing 63
5.14 Spam o correo malicioso 64
5.15 Toolbars 65
5.16 Usurpación o robo de identidad 66
5.17 Suplantación de identidad o Spoofing 67
5.18 Ciberestafas en compras online y otros engaños 68
5.19 Warshipping 71
5.20 Vulnerabilidades 71
5.21 Cryptojacking 72
5.22 Plugins maliciosos 73
5.23 SIM Swapping 74
5.24 Shoulder surfing o visual hackins 75
5.25 Ciberacoso 76
5.26 Ciberextorsión 76
5.27 Sextorsión 76
5.28 Doxing 77
5.29 Baiting 77
5.30 Clickjacking 77
5.31 Dumpster diving o scavening 78
5.32 Quid pro quo 78
5.33 Formjacking 79
5.34 Juice jacking 79
5.35 Voice hacking 80
5.36 Sustracción o perdida de tu dispositivo 80

6 Tu yo digital **82**

6.1 Toma consciencia de tu yo digital 82

6.2 Metadatos 82

6.3 Huella digital o reputación online 83

6.4 Sombra digital 85

6.5 Eliminar el historial de busquedas 86

6.6 Derecho al olvido 86

7 Contenido en la red **88**

7.1 El contenido digital 88

7.2 Contrastar la información 88

7.3 Fake news y Deepfake 89

7.4 Deep web 91

8 Otras particularidades importantes **93**

8.1 Otros conceptos relevantes 93

8.2 Desinfecta tu dispositivo 93

8.3 Analizadores de virus online 93

8.4 Menores en el uso de la red 94

8.5 Utilidades interesantes 97

8.6 Ataques en tiempo real 99

8.7 Eventos internacionales 99

8.8 Colabora 99

9 Formación y conocimientos **100**

9.1 Aprendizaje y reciclado continuo 100

9.2 Formación como medida preventiva 100

9.3 Desarrolla tu ciberinteligencia 101

9.4 Pon a prueba tus conocimientos 102

9.5 Canales de avisos y alertas 102

10 Entidades y plataformas de ayuda **103**

10.1 Ayuda y soporte desde instituciones 103

10.2 Instituto nacional de ciberseguridad 103

10.3 Oficina de seguridad del internauta 104

10.4 Agencia española de protección de datos 105

10.5 ObservaCIBER 105

10.6 Internet segura para niños 106

10.7 Pantallas amigas 107

10.8 Foro Info Spyware 107

10.9 Fuerzas y cuerpos de seguridad del estado 108

Prólogo

Este manual aglutina de manera filtrada y tamizada una amplia y detallada parte del conocimiento e información de relevancia que puedes encontrar en la web sobre privacidad y seguridad en internet, de forma ordenada y estructurada. Además, encontrarás en la bibliografía todas las fuentes que han hecho posible la elaboración y documentación de este manual, para que puedas contrastar por ti mismo dichas fuentes.

Entenderás las diferencias entre los conceptos de privacidad y seguridad en internet, para que de este modo puedas hacer una buena configuración y uso de éstas.

Aprenderás buenas prácticas en la gestión de la privacidad, así como la manera más adecuada de gestionar la seguridad tanto en los equipos (PC, tables, smartphones, etc.), como en la red de datos.

Conocerás las principales amenazas que existen en el uso de las tecnologías y el mundo digital.

Y por último, pero no por ello menos importante, se abordarán otros conceptos relacionados con los ciberdelitos, la huella digital, la importancia de ser selectivos con la información online y otros aspectos más.

Para concluir, también encontrarás a lo largo del manual multitud de enlaces que te llevarán a más información ampliada sobre las temáticas, así como una extensa lista de recursos y herramientas para que puedas llevar tu privacidad y seguridad en internet al siguiente nivel.

Si quieres contribuir y ayudar a nutrir de más contenido de valor este manual, por favor, no lo dudes y ponte en contacto conmigo, estaré encantado que colaboremos. Encontrarás mis datos de contacto en el siguiente apartado *sobre el autor*.

Este manual está disponible en el repositorio Github: diegochiquero/manual-de-privacidad-y-seguridad-en-internet. Y ha sido escrito en R-Markdown empleando el paquete `bookdown` cuya guia encontrarás en (Xie, 2021).

Imagen portada (Katemangostar - Freepik, 2021)


BY NC SA

Sobre el autor

Hola, mi nombre en Diego.

Y lo primero que me gustaría hacer, es agradecerte que hayas decidido leer este manual. Ya que éste hecho, hace que las horas de dedicación, esfuerzo, documentación, contrastación de fuentes y curación de contenidos hayan merecido la pena.

El propósito de este manual es hacerte consciente de los peligros de navegar por internet, de lo vulnerable y expuesto que puedes llegar a estar en el uso de las tecnologías y a su vez dotarte de conocimientos, consejos y herramientas para poder hacer una buena gestión de la web de manera segura y privada.

De formación académica Técnico superior en desarrollo de aplicaciones web. Para concluir y a modo de breve presentación, haré referencia a mi extracto de Linkedin:

> Apasionado de las tecnologías, el espíritu emprendedor y la comunicación.
>
> Plenamente convencido que el compromiso con los valores sociales puede marcar la diferencia, que el derecho nos asiste a todos y que un mundo mejor es posible.
>
> En continuo proceso de crecimiento personal y profesional.

Diego Chiquero Mena

Puedes contactar conmigo en chiquerodiego@yahoo.es

Más sobre mí Diego Chiquero Mena

Capítulo 1

Privacidad y Seguridad en Internet

1.1 Introducción

En estos últimos años hemos podido ver como la evolución de las IT (Tecnologías de la información) y el paso de la Web 1.0 a la Web 2.0, nos ha permitido a muchos de nosotros como usuarios interactuar los unos con los otros subiendo y compartiendo todo tipo de contenidos. La aparición de las Redes sociales ha traído con ellas, la posibilidad de publicar fotos, videos, información, comentarios, reseñas, etc. a través de cualquier dispositivo, ya sea un PC, tablet o smartphone. Y no solo eso, sino que además, también nos ha abierto un amplio abanico de posibilidades con las que podemos gestionar cuentas bancarias, hacer compras online, trámites telemáticos y un sinfín de gestiones que hasta hace tan solo unos años atrás eran difíciles de imaginar.

Además, a todo lo anterior se añade este nuevo escenario hacia la web 3.0 en el que ha aumentado la exposición a la superficie digital y donde el incremento exponencial de ciberdelincuencia parece no tener freno. Es por ello que bajo estas circunstancias es cuando más debemos aprender y mejorar las destrezas digitales y hacerlas compatibles con un uso responsable, respetuoso y crítico de la tecnología, desarrollando capacidades digitales en las que un entorno, seguro, privado y sostenibles que garantice el bienestar social sea posible.

Como consecuencia de ello, el enorme conglomerado de información sensible que se encuentra disponible en internet, hace que nosotros como usuarios estemos en el punto de mira de ciberdelincuentes y expuestos a todo tipo de ciberataques. En esta línea, este manual contribuye a enseñarte, aconsejarte y proveerte de herramientas necesarias para prevenir, evitar y paliar en la medida de lo posible todos los riesgos y peligros a los que estamos expuestos en nuestro uso diario de las tecnologías.

Por lo tanto, en lo sucesivo iras viendo el porqué de la importancia de velar de manera activa por tu privacidad y seguridad en internet haciendo una buena gestión de éstas. También te ayudará a conocer y reconocer la amplia

lista de ciberdelitos que actualmente están más extendidos.

En estas estadísticas publicadas por el Observatorio Español de Delitos informáticos (OEDI, 2021) puedes ver el porqué de cuidar tu privacidad y seguridad en internet. En ellas se expone una exhaustiva lista de ciberdelitos y sus recurrencias cronológicas.

1.2 Privacidad

La privacidad es aquello que se lleva a cabo en un ámbito reservado; en Internet podría entenderse como el control que ejercemos sobre nuestra información para limitar la cantidad de personas autorizadas a verla, así como la cantidad de contenido expuesto. Esto incluye datos personales, fotografías, documentos, etc.

Internet es una herramienta que nos permite la interacción entre dos o más personas. Siendo ejemplo de los anteriores sitios como Facebook y Twitter, Redes Sociales en donde las personas pueden compartir públicamente opiniones, noticias, sentimientos, ideas, fotografías, videos, etc. Por ello es necesario considerar que Internet es un espacio abierto al mundo, por lo tanto, cualquier acción que se haga va a tener un impacto global y permanente. Por ejemplo, imagina una publicación de la cual puedas arrepentirte (como una fotografía u opinión) no solo podrá ser vista por millones de usuarios, sino que también será prácticamente imposible de borrar completamente de la red .

También puede resultar peligroso publicar datos que puedan identificarte, como la dirección, teléfonos, lugar de estudio o trabajo, días de vacaciones, etc. Esto puede resultar todavía más complicado si posees una gran lista de amigos a los que no conoces personalmente.

Por todo lo que se ha mencionado en éstas últimas líneas, es de suma importancia que antes de publicar algo, pienses en las consecuencias que puede conllevar divulgar información sensible en sitios públicos y de los cuales no siempre se tiene un control directo (ESET, 2015).

1.3 Seguridad

La seguridad en internet son todas aquellas precauciones que son tomadas para proteger todos los dispositivos informáticos, así como la red de internet que pueden ser afectados por delincuentes cibernéticos. Además de ser una rama de la seguridad informática que se dedica a identificar y prevenir todas las amenazas que afectan a la red de redes, siendo una de las herramientas más conocidas los antivirus (GCFGlobal, 2021).

Entre los peligros más habituales de no hacer un buen uso de la seguridad en la red, nos encontramos, robo de datos bancarios o personales, virus informáticos, phishing, spam, etc. Pero estos no son los únicos riesgos que asechan en internet, como verás más adelante.

1.4 RGPD (Reglamento general de protección de datos)

El Reglamento General de Protección de Datos (RGPD) es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Entró en vigor el 25 de mayo de 2016 y fue de aplicación el 25 de mayo de 2018, dos años durante los cuales las empresas, las organizaciones, los organismos y las instituciones han debido ir adaptándose para su cumplimiento. Es una normativa a nivel de la Unión Europea, por lo que cualquier empresa de la unión, o aquellas empresas que tengan negocios en ésta y que manejen información personal de cualquier tipo deberán acogerse a la misma (Wikipedia, 2021k).

En el pasado, el uso de datos era obtenido por omisión, en estos momentos para estar seguros de cumplir con el RGPD se ha de obtener el consentimiento inequívoco o expreso por parte del usuario.

Paralela a la RGPD europea existe una a nivel de España llamada Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), recogida en el BOE Boletín Oficial del Estado y cuyo objeto es también garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas y en especial, su honor e integridad personal y familiar.

1.5 Aviso legal, política de privacidad y política de cookies

Si una web va a realizar transacciones comerciales de la naturaleza que sea, va a gestionar datos de usuarios o hacer uso de cookies, ha de tener a disposición del usuario las políticas que más abajo se detallan. Todas estas políticas están recogidas en el RGPD del apartado anterior. Sin embargo, para documentarlo con terminología más cotidiana, en este apartado nos hemos apoyado en la sección de derecho digital de la compañía IONOS by 1&1 en su división IONOS Guía Digital.

- Aviso Legal: Se trata de un documento donde se recogen tanto el cumplimiento por parte de la entidad o empresa, conforme a las leyes vigentes en el desarrollo de su actividad, así como los datos referentes a los administradores de la misma.

Todo proyecto de base digital u online con ánimo de lucro, ya sea a través de modelos de patrocinio, publicitarios o compra-venta de productos o servicios, requieren de un aviso legal visiblemente expuesto y a disposición de todos los usuarios. Este requerimiento está recogido en la legislación española en la Ley 34/2002 de Servicios de la Sociedad de la Información y el Comercio Electrónico (IONOS by 1and1, 2021a).

- Política de privacidad: El reglamento general de Protección de Datos de carácter personal, establece que cualquier página web que incluya un formulario de carácter personal que deban rellenar los usuarios, que incluya un correo de contacto o utilice las redes sociales desde las cuales se puede obtener información de los usuarios, está obligada a disponer de una política de privacidad (IONOS by 1and1, 2021c).

  La política de privacidad se creó con la finalidad de proteger y preservar los derechos del espacio privado de las personas.

- Política de cookies: Una cookie es una pequeña información enviada por un sitio web y almacenado en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador. Su propósito principal es identificar al usuario almacenando su historial de actividad en un sitio web específico, de manera que se le pueda ofrecer el contenido más apropiado según sus hábitos (IONOS by 1and1, 2021b).

  Toda web que haga uso de cookies está obligada ponerlo en conocimiento de los usuarios y a solicitar su aceptación.

  Con respecto a la legislación de la Unión Europea sobre el consentimiento de las cookies debes saber que dicha ley dicta que los usuarios de internet deben tener la opción de poder rechazarlas, sin que por ello éste se vea perjudicado en su navegación. Esto nos lleva a señalar que el problema está en que la mayoría de los sitios web no lo cumplen. Normalmente tú como usuario en una mayor parte de las veces solo te vas a encontrar con la opción de aceptar todas las cookies o rechazarlas, en otros casos con otra opción más confusa y compleja de manejar la configuración de estás. Y en la inmensa mayoría de las ocasiones no te vas a encontrar con esa alternativa que te brinda la ley de poder rechazarlas (Genbeta, 2021).

1.6 Derechos ARCO

Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), están regulados por la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).

- Derecho al acceso: Te da derecho a conocer el uso que la entidad o responsable de tus datos está haciendo de ellos.

- Derecho a la rectificación: Te da derecho a solicitar la rectificación de tus datos.
- Derecho a la cancelación: Te da derecho a solicitar la supresión de los datos que resulten inadecuados o excesivos.
- Derecho a la oposición: Te da derecho a oponerte al tratamiento de sus datos personales o el cese de éstos.

Para poder ejercer estos derechos solo basta con solicitarlo a la parte responsable de tus datos, aportando fotocopia del DNI o documento equivalente, la petición que se solicita, la dirección a efectos de notificaciones y los documentos que acreditan la petición que se formula (Grupo Ático, 2018a).

1.7 Derechos POL

Los derechos POL (Portabilidad, Olvido o supresión y limitación del tratamiento), están regulados por el Reglamento General de Protección de Datos (RGPD) (Grupo Ático, 2018b).

- Derecho a la portabilidad de los datos: Te da el derecho de solicitar al responsable de tus datos el traspaso de éstos a otra entidad o responsable. Un ejemplo claro es la conocida portabilidad en el mundo de la telefonía que hacen que tus datos puedas ser cedidos de una compañía a otra.
- Derecho al olvido o supresión: Se trata de un mecanismo jurídico que te da derecho a solicitar al responsable de tus datos la supresión o eliminación de estos, pero con un enfoque más estrecho con el ámbito digital. Desde el servicio ofrecido por AEPD puedes acceder a los enlaces donde solicitar el derecho al olvido en Google, Bing, Yahoo, aunque desde estos últimos enlaces ya puedes acceder directamente.
- Limitación del tratamiento: Permite que cualquier persona tenga derecho a exigir a la entidad responsable la limitación del tratamiento de sus datos personales.

Capítulo 2

Gestión de la privacidad

2.1 Gestionar la privacidad

La privacidad en Internet se refiere al control de la información personal que posee un determinado usuario que se conecta a Internet, interactuando por medio de diversos servicios en línea con los que intercambia datos durante la navegación. Por ello, en esta unidad vas a lograr aprender a gestionar la privacidad de manera inteligente, para así evitar males mayores que podrían hacer de tu vida privada un terreno en el que seguro, no te gustará estar (Wikipedia, 2020).

2.2 Datos personales sensibles

Cuando se habla de datos personales sensibles en la red, se refiere a aquellos datos que están revelando información privada, como por ejemplo, el domicilio o cualquier otra información de carácter privado, costumbres o hábitos. Así como acciones que ubican o determinan a una persona en posibles situaciones futuras que pudiesen abrir una brecha de vulnerabilidad en la vida privada de ésta. Un ejemplo sería subir a la red que te vas de vacaciones, de manera que estás diciendo a los ciberdelincuentes que tu casa estará vacía.

Entrando en un terreno más técnico los datos sensibles son aquellos que, de difundirse indebidamente podrían afectar la esfera más íntima del ser humano. Ejemplos de este tipo de datos son: el origen racial o étnico, el estado de salud, la información genética, las creencias religiosas, filosóficas y morales, la afiliación sindical, las opiniones políticas y las preferencias sexuales.

Por ello, aporta solo los datos necesarios y no te expongas.

2.3 Oversharing o sobreexposición

El Oversharing es la sobreexposición de información personal en internet y en su mayoría en los Medios Sociales a través de tus perfiles sociales. Este hecho se presenta continuamente en la actualidad, donde los jóvenes y no tan jóvenes, publican constantemente imágenes o información personal.

De esta manera, tu vida queda totalmente expuesta y aunque el propósito de ello sea totalmente lícito e incluso plausible, estos datos, imágenes o información pueden volverse en tu contra por un uso indebido o ilícito por parte de terceros.

Este exceso de información que se puede facilitar en internet, sumado al comportamiento malicioso de otros usuarios, supone un grave riesgo que se corre cada día al señalar tu ubicación, comentar información personal o privada, colgar una imagen o video comprometedores, etc.

Esto no supone un delito en cuestión, pero puede dar lugar al chantaje, ciberacoso o robo de información personal a través de algún tipo de técnica. Además, de exponerte al riesgo de un posible robo y/o suplantación de identidad (Agencia española protección de datos, 2021).

2.4 Privacidad en tus cuentas

Prácticamente todo el mundo en menor o mayor medida dispone de cuentas de usuarios en todas sus aplicaciones o servicios en la red. Una de las más conocidas es la cuenta de Google, así como también la de Microsoft entre otras. En ambos enlaces podrás ajustar la privacidad con la que más cómodo te sientas. Además, recuerda que no solo estos dos servicios disponen de estos ajustes, sino que también el resto de plataformas deben brindarte la posibilidad de que realices tu propia configuración.

En lo que respecta a las redes sociales como, Facebook, Twitter o Instagram, entre otras muchas más, no debes olvidar que también disponen opciones de privacidad y que en éste escenario está en juego tus datos más personales. Luego el mejor consejo es establecer una configuración privada en lugar de pública, ya que estas redes sociales no tienen por defecto, los niveles más elevados en cuanto a la protección y a la seguridad.

Con referencia a todo lo expuesto, puedes dejar la configuración de privacidad que la cuenta trae por defecto o acomodarla a tus necesidades o preferencias. Dentro de cada cuenta se encuentran todas las opciones de privacidad, como por ejemplo, historial de búsquedas, actividad de ubicación entre otras.

También está el control de las siguientes:

- Privacidad en las publicaciones: Facebook, Twitter o Instagram, entre otras muchas más, disponen opciones de privacidad y que en este escenario está en juego nuestros datos más personales, luego el mejor consejo es establecer una configuración privada en lugar de pública. (amigos, público o solo yo).
- Etiquetas y menciones: Establecer quién puede etiquetarte en publicaciones y quién puede ver las publicaciones en las que te han etiquetado.
- Interactuar en comentarios y envíos de mensajes: Controlar quién puede interactuar contigo.
- Bloquear usuarios: Bloquear a personas no deseadas para evitar que interactúen contigo en la plataforma.

Tienes más información en el siguiente enlace Configuración de privacidad en redes sociales

2.5 Navegación privada

La navegación privada es una función de privacidad que conocerás como modo incógnito o modo privado. Su principal característica es que permite a los navegadores web no almacenar información sobre la página en que navegamos.

La navegación privada te ofrece una sesión temporal que no comparte datos con el navegador, que no guarda información sobre páginas web, ni historial de navegación, caché web, contraseñas, información de formularios, cookies u otros datos de sitios web, borrando éstos y otros archivos temporales cuando finalices la sesión (Muy computer, 2018).

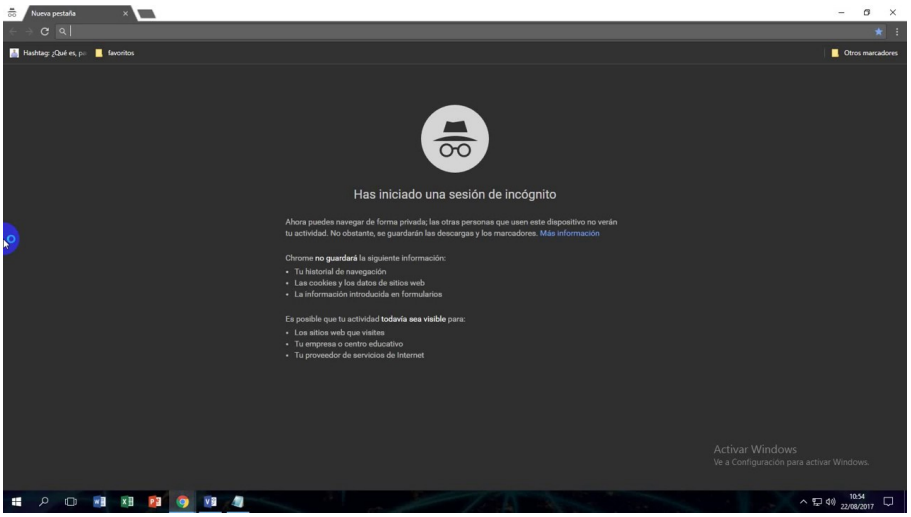

Figura 2.1: Navegación privada navegador Google Chrome.

Ten en cuenta que no es lo mismo navegar privadamente que navegar de forma anónima por Internet, lo que requiere de otras herramientas como TOR.

El uso de la navegación privada resulta conveniente en los siguientes supuestos:

- Transacciones económicas.
- Utilización de un ordenador de terceros.
- Obtención de resultados "puros" del motor de búsquedas.

También existen navegadores que protegen tu privacidad sin necesidad de activar la navegación privada, como por ejemplo, Epic, Brave e incluso buscadores como DuckDuckGo.

2.6 VPN (Red privada virtual)

Otra manera más de proteger tu privacidad, es hacer uso de una VPN (son las siglas de Virtual Private Network) (Avast, 2018).

Las VPN son una tecnología de red que permiten una extensión de tu conexión local o LAN, permitiendo conectar varios dispositivos como si se encontrasen físicamente en el mismo lugar. Entre sus ventajas está la de ofrecer una mayor privacidad al ocultar tu localización, pero también, y este el caso que nos compete, el que parezca que tu conexión esté realizándose en otro país concreto, con lo que uno se puede saltar censuras o acceder a contenidos de servicios locales.

Su principal particularidad es que se trata de una conexión segura y cifrada. Esto hace que no sea posible conocer la información que viaja en la petición que se realiza, así como tampoco la IP pública que identifica tu dispositivo, ya que la conexión se realiza a través de los muchos router VPN en diferentes ubicaciones.

Las VPN suelen ser aplicaciones o extensiones de terceros, aunque el navegador OPERA lo trae por defecto. Lo único que tendrás que hacer es activarla desde sus opciones, y se creará una conexión cifrada entre tu dispositivo y un servidor VPN para esconder tu ubicación real.

No obstante, no todas las VPN son igual de eficaces y en ocasiones algunas de ellas pueden no estar funcionando todo lo bien que cabría de esperar y durante tu sesión de navegación podrían verse expuestos algunos de tus datos. Por suerte, existen herramientas como What leaks? que te permite analizar la eficacia de tu VPN a la hora de proteger tu privacidad.

2.7 Cookies

Una cookie es un fichero que guarda nuestro navegador, donde se almacenan pequeñas cantidades de datos, de manera que el sitio web puede consultar la actividad previa del navegador.

Su propósito principal es identificar al usuario almacenando su historial de actividad de un sitio web específico, de manera que se le pueda ofrecer el contenido más apropiado según sus hábitos. Esto quiere decir que cada vez que visitas una página web por primera vez, se guarda una cookie en el navegador con un poco de información. Luego, cuando visitas nuevamente la misma página, el servidor pide la misma cookie para arreglar la configuración del sitio y hacer la visita del usuario tan personalizada como sea posible (Blogthinkbig by telefónica, 2014).

Existe la opción de navegar sin cookies gracias a las sesiones privadas que tienen los distintos navegadores, como has podido ver en el apartado anterior. De esta forma no se almacenará ningún tipo de información en tu ordenador cuando navegues en una web y del mismo modo tampoco recordará nada después al volver a navegar de nuevo.

Es importante que con frecuencia elimines las cookies, ahora que sabes que manejan información privada y además ocupan espacio en tu dispositivo. Existen dos formas manuales de hacerlo. La primera de ellas es desde el menú de opciones del propio navegador y la otra es con un software específico para tal cometido, como por ejemplo Ccleaner. Pero si quieres automatizar esta tarea, prácticamente todos los navegadores disponen de una configuración para que una vez cierres el navegador se realice una limpieza de manera automática. La siguiente imagen te muestra la opción que debes buscar en el navegador Google Chrome, para ello ve al Menu del navegador, entra en Configuracíón, luego Privacidad y seguridad, a continuación, Cookies y finalmente Borrar las cookies y los datos de sitios al salir de Chrome, pero debes tener en cuenta que las ubicaciones pueden variar con las actualizaciones. Si usas otro navegador puede ser que varíe la ruta de acceso, pero a grandes rasgos suelen ser muy parecidas y también se acceden a ellas a través del menú de opciones.

Por otro lado si quieres deshacerte de la incómoda notificación de cookies de las web, puedes instalar en el navegador el plugin I don't care about cookies o este otro Ninja cookie, elige el que más te guste.

Si quieres más información detallada sobre las cookies visita este enlace por qué borrar las cookies y este otro tipos de cookies, configuración y consejos de la Oficina de Seguridad del Internauta donde las analizan con más detalle.

Al hilo de las cookies debes saber que estas no son la única manera que existe de tracear nuestra actividad en internet y que hay técnicas más sofisiticadas.

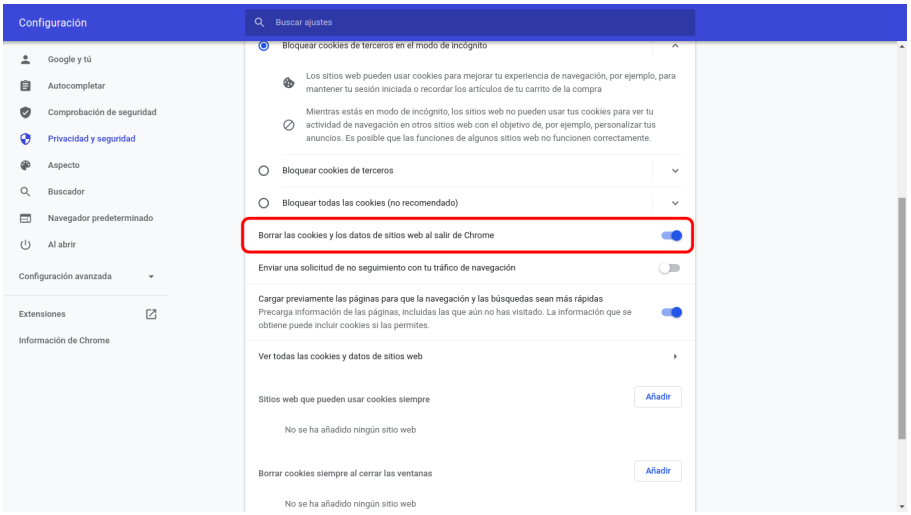

Figura 2.2: Eliminar cookies automáticamente al cerrar Google Chrome.

Estas técnicas son conocidas como Fingerprinting y hacen un rastreo de tu huella digital. Por lo tanto, el fingersprinting es una técnica que permite obtener información de una persona o empresa a través de los sistemas informáticos.

Si quieres profundizar más en este tema te recomiendo que visites el siguiente enlace ¿Qué es el fingerprinting?.

Para que te hagas una idea de lo que implica una política de cookies, a continuación tienes un ejemplo de los tipos de cookies y sus funciones.

Política de Cookies: El portal web “x” hace uso de cookies. Con su aceptación de la presente política concede su permiso para obtener datos estadísticos de su navegación en esta web, en cumplimiento del Real Decreto-ley 13/2012. Si continúa navegando consideramos que acepta el uso de cookies.

¿Qué son las cookies? Las cookies son archivos que las páginas web almacenan en el navegador del usuario que las visita, necesarias para aportar a la navegación web ventajas en la prestación de servicios interactivos.

Tipos posibles de cookies:

- Cookies de sesión: Son un tipo de cookies diseñadas para recabar y almacenar datos mientras el usuario accede a una página web, y no queda registrada en el disco del usuario.
- Cookies persistentes: Son un tipo de cookies en el que los datos siguen almacenados en el terminal y pueden ser accedidos y tratados durante un periodo definido por el responsable de la cookie, y que puede ir de unos minutos a varios años.
- Propias: son cookies generadas por la propia página web que se está visitando.

- De terceros: son cookies que se reciben al navegar por esa página web, pero que han sido generadas por un tercer servicio que se encuentra hospedado en ella.

Fines de las cookies:

- Fines técnicos: Son necesarias para el funcionamiento de la página web. Son las denominadas también estrictamente necesarias. Hacen posible el control de tráfico desde el servidor a múltiples usuarios a la vez, la identificación y el acceso como usuario del sistema, etc.
- Personalización: Hacen posible que cada usuario pueda configurar aspectos como el lenguaje en el que desea ver la página web o la configuración regional.
- Análisis o rendimiento: Permiten medir el número de visitas y criterios de navegación de diferentes áreas de la web de forma anónima.
- Publicidad: Permiten implementar parámetros de eficiencia en la publicidad ofrecida en las páginas web.
- Publicidad comportamental: Permiten implementar parámetros de eficiencia en la publicidad ofrecida en las páginas web, basados en información sobre el comportamiento de los usuarios.

Uso de Cookies:

La web "x" SOLO utiliza las siguientes COOKIES: Cookies de tipo comportamental para el almacenamiento de sesión y de caché para mejorar su experiencia.

- Cookies de análisis: Son aquéllas que permiten al responsable de las mismas, el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas. La información recogida mediante este tipo de cookies se utiliza en la medición de la actividad de los sitios web, aplicación o plataforma y para la elaboración de perfiles de navegación de los usuarios de dichos sitios, aplicaciones y plataformas, con el fin de introducir mejoras en función del análisis de los datos de uso que hacen los usuarios del servicio.
- Cookies publicitarias: Son aquéllas que permiten la gestión, de la forma más eficaz posible, de los espacios publicitarios que, en su caso, el editor haya incluido en una página web, aplicación o plataforma desde la que presta el servicio solicitado en base a criterios como el contenido editado o la frecuencia en la que se muestran los anuncios.
- Cookies de publicidad comportamental: Son aquéllas que permiten la gestión, de la forma más eficaz posible, de los espacios publicitarios

que, en su caso, el editor haya incluido en una página web, aplicación o plataforma desde la que presta el servicio solicitado. Estas cookies almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función del mismo.

- Estrictamente necesarias: Las Cookies estrictamente necesarias le permiten navegar por la página web y usar sus funciones esenciales.

2.8 Permisos cámara, micrófono y localización.

Una práctica muy saludable en el uso de la cámara o webCam e incluso el micrófono, es tenerla tapada cuando no la estés usando y si no fíjate en la foto que se muestra a continuación que le tomaron a Mark Zuckerberg.

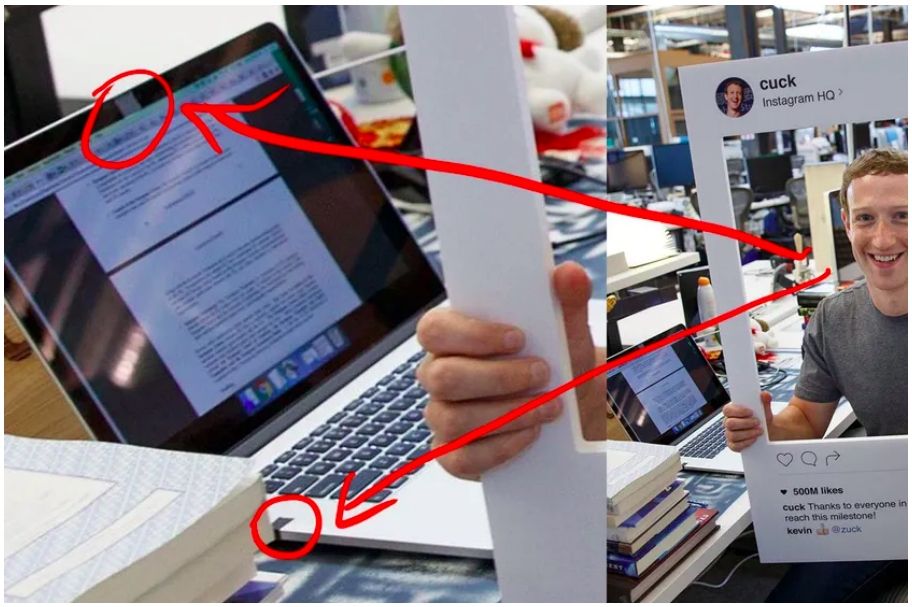

Figura 2.3: WebCam y micrófono del ordenador tapados.

Para tener el control total sobre las funcionalidades de cámara, micrófono y ubicación, debes establecer los permisos en la opción de Preguntar, lo verás más claramente en la imagen que se muestra más abajo. Para establecer estos parámetros existen dos maneras de hacerlo, uno de ellas es a través de las opciones que te da el menú de configuración del propio navegador, y para ello debes ir a Menú navegador, buscar Configuracíón, después Privacidad y seguridad, a continuación Configuración de sitios web y finalmente Permisos. Como ya se indicó en el caso de borrado de cookies automático, debes tener en cuenta que las ubicaciones pueden variar con las actualizaciones que reciba el navegador.

Aunque estos permisos son los más importantes cuando navegas por internet,

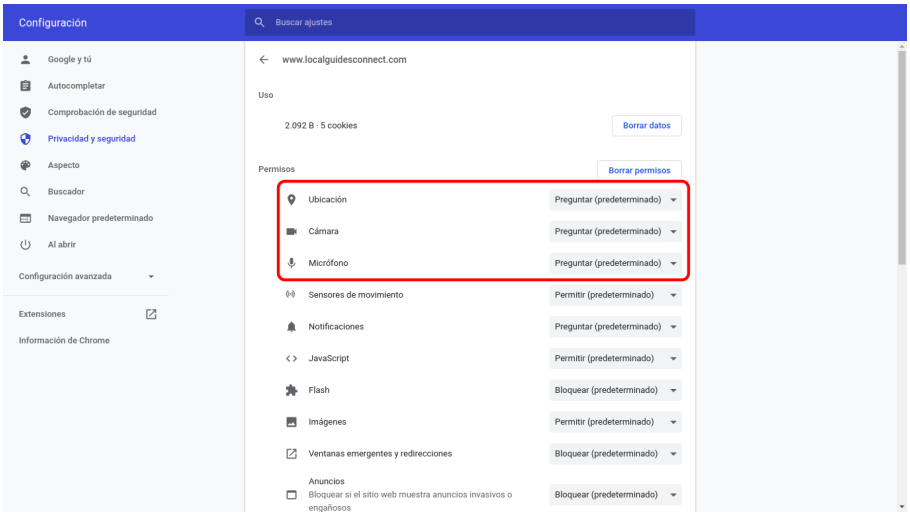

Figura 2.4: Ajustes permisos cámara, micrófono y ubicación desde el menú de opciones del navegador.

si te fijas en la figura 2.4 verás que no son los únicos y que entre éstos se encuentran los de notificaciones o los de ventanas emergentes entre otros.

La otra forma es más sencilla e incluso te permite cambiar los permisos directamente desde el navegador sin tener que ir al menú de opciones y esto lo tienes haciendo click en el candado de la barra de direcciones. Se trata del mismo candado que nos acredita que estamos ante una web segura. Puedes verlo en la siguiente imagen.

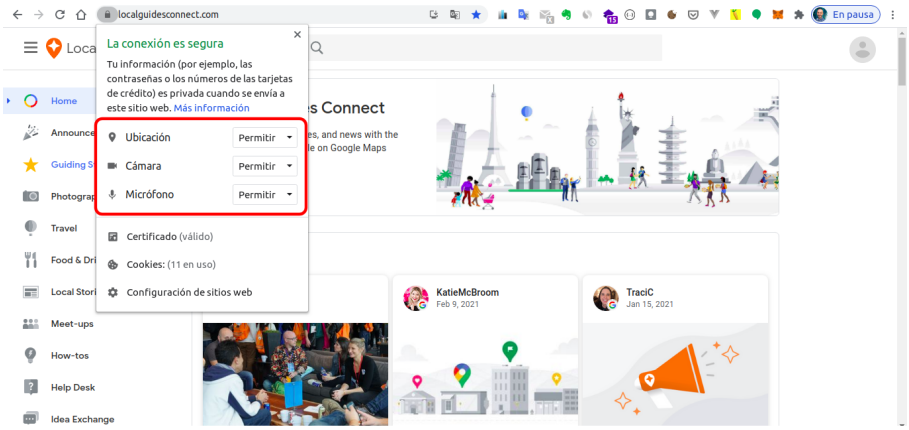

Figura 2.5: Ajustes permisos cámara, micrófono y ubicación desde el candado de la barra de direcciones.

Para concluir, no debes olvidar que con las aplicaciones móviles sucede lo mismo, y que puedes gestionarlos de igual manera desde ajustes del dispositivo. Visita los siguientes enlaces dependiendo de tu smartphone, cambiar los permisos de las aplicaciones en teléfonos Android o controlar el acceso a la información en las apps en el iPhone. En el siguiente enlace, permisos aplicaciones móviles encontrarás una tabla con los permisos y los riesgos que entrañan.

2.9 La nube

Como ya sabrás el almacenamiento en la nube, es el almacenamiento de datos en servidores por lo general aportados por terceros y que gracias a esto, puedes disponer de ellos desde cualquier lugar y dispositivo, con solo tener conexión a internet y conectarte al servicio donde están alojados tus datos. De esta manera ya no es necesario llevar contigo el dispositivo físico donde tienes almacenada tu información. Algunos de estos servicios más conocidos son Google drive, One drive o Dropbox entre otros.

Antes de decidirte por cuál de los proveedor de servicio en la nube debes decantarte, ten en cuenta los siguientes:

- Donde va a estar ubicada tu información. Esto te permitirá conocer la legislación y garantías de protección de tus datos en el país donde se encuentren.
- Saber si la plataforma comparte información con terceros o no.
- Si la web cuenta con certificado digital y es accesible mediante https.
- Mecanismos de cifrado, ya que éstos maximizan la seguridad de los datos.
- Políticas de privacidad.

De otro lado también puedes tomar tus propias medidas de seguridad cifrando tu datos antes de subirlos. Para ello puedes usar esta herramienta llamada cryptomator.

En este enlace encontrarás un estudio completo de los diferentes servicios de almacenamiento en la nube y sus características.

A la hora de compartir tus datos alojados en la nube debes tener en cuenta que solo es recomendable compartirlos con personas de confianza, ya que de lo contrario podrían hacer un mal uso de ello, o simplemente una mala gestión que provoque la pérdida de la información.

2.10 Correo electrónico y apps de mensajería

El correo electrónico es uno de los servicios web que más se suele utilizar. Por ello, debes saber que muchos de los gestores de emails que son utilizados a diario, no aplican estrictas políticas de privacidad, por lo que tus correos podrías ser leídos y rastreados no solo por terceros con intenciones poco saludables sino también por éstos mismos servicios de correo.

Esto no tiene por qué ser un inconveniente si no envías información sensible, pero si no es el caso quizá preferirías usar un gestor de correos que sí te

garantice una privacidad completa en tus envíos. De ser este tu caso puedes usar Protonmail, Tutanota o Fastmail que sí tienen en cuenta este aspecto, aunque no son los únicos. En el siguiente enlace tienes una lista de otras alternativas de emails privadas.

Si por el contrario prefieres ser tu quien gestiones esa capa de privacidad adicional, puedes optar por hacer uso de otras herramientas de encriptado que podrás ver en este artículo de cómo encriptar y proteger tu correo electrónico.

Otra alternativa de envío de correos cifrados, es el uso de la opción de correos confidenciales de Gmail. De esta manera el receptor necesitará un código para desbloquear el contenido del email que, recibirá a través de SMS en su smartphone. Más información en el siguiente enlace Enviar y abrir correos confidenciales.

Si además quieres saber si tu cuenta de correo o tu número de teléfono han sido comprometidos, puedes saberlo a través de la siguiente plataforma haveibeenpwned.

Con respecto a las aplicaciones de mensajería instantánea debes tener en cuenta que sucede lo mismo que con los correos electrónicos. A pesar que la mayoría de ellas, incluida la más popular de todas (whatsApp) disponen de capas de privacidad que la hacen confiable, a veces no podemos estar totalmente seguros de no estar sometidos a un seguimiento por parte de éstas. Es por ello, que las aplicaciones como telegram y signal nacen con el propósito de no inmiscuirse en el uso que haces de la aplicación.

2.11 Cifrado o encriptado de datos

Tener datos o información simplemente organizados en carpetas en tus dispositivos sin más no es una práctica muy recomendable y más si se trata de datos sensibles. Para evitar que alguien que se haga con tu dispositivo pueda acceder impunemente a cualquier información es necesario disponer de una buena capa de seguridad. Es aquí donde entra en juego la herramienta de encriptado Cryptomator.

Cryptomator es un software libre y por lo tanto gratuito, con el que puedes encriptar tanto archivos como carpeta que quieras mantener a buen recaudo. Además es compatible con Windows, macOS y Linux y también disponen de una app para Android y Iphone.

Con Cryptomator puedes crear diferentes bóvedas o cámaras cifradas. Cada bóveda está protegida por una contraseña y puede contener tantos archivos y carpetas como desees. En estas bóvedas estará tu información encriptada de manera que no podrá ser visible a menos que poseas la contraseña que los

desencripta. Con esta aplicación podrás estar tranquilo ya que nadie podrá acceder a tu información aun habiéndose hecho con tu dispositivo.

Otra interesante utilidad sería encriptar tus datos antes de subirlo a cualquier plataforma de almacenamiento en la nube con lo que te garantizas que no puedan ser leídos.

En la plataforma de Redes zone encontrarás más detalles de esta estupenda herramienta, así como una guía para su instalación.

2.12 He decidido vender o donar mi dispositivo

Si estás pensando en vender o quizá donar cualquiera de tus dispositivos, ya sea un disco duro externo, el ordenador o portátil, un USB o cualquier otro dispositivo que contenga almacenamiento, asegúrate primero de eliminar totalmente todo el contenido. Para ello utiliza software de borrado definitivo, ya que un simple formateado no borrará la información. El borrado solo se completa cuando se reescribe sobre la anterior información, es por esto que un formateo solo te hace constar que el espacio está disponible, pero el contenido, aunque oculto, sigue estando ahí. Esto quiere decir que con software avanzado y específico los ciberdelicuentes podrían recuperar todo el contenido (Xataka, 2019a).

Si quieres más recomendaciones sobre como actuar en este supuesto, te recomiendo que leas la siguiente entrada ¿Sabías que 2 de cada 5 dispositivos vendidos contienen información personal?.

Algunas herramientas de borrado definitivo son:

- Eraser
- Disk wipe

Capítulo 3

Gestión de la seguridad en equipos físicos

3.1 Gestionar la seguridad en los equipos

Para poder tener la tranquilidad de que tus equipos tales, como el ordenador, la tablet, el smartphone, el router, etc., estén a salvo de ataques o pérdidas de datos, entre otras, debes mantener una seguridad robusta y confiable en tus equipos.

A lo largo de esta unidad veras que debes hacer y las precauciones que debes tomar para que tus equipos e información estén seguros y a salvo de ciberataques.

3.2 Cuenta de usuario en equipos locales y dispositivos móviles

Una cuenta de usuario es el conjunto de información perteneciente a un usuario concreto. De esta forma indica al sistema operativo los archivos y carpetas a los que dicho usuario tiene acceso, así como la posibilidad de realizar cambios y configuraciones personales (OSI, 2021c).

Las pautas de seguridad que vas a ver a continuación te van a ser útil, tanto para ordenadores como cualquier tipo de dispositivo móvil, smartwatch y demás.

Todos los equipos informáticos funcionan con una cuenta de usuario, única y personal. Luego una vez, hayas creado la tuya, solo tú debes hacer uso y disfrute de ella. En los ordenadores personales existe la posibilidad de crear varias cuentas de usuarios. Una vez éstas están creadas solo son accesibles mediante contraseña y aunque solo sirva para no olvidarlo, recuerda que una contraseña nunca debe ser de compartida.

Desde aquí podrás acceder a cómo crear cuenta de usuario en Windows o crear cuenta de usuario en Mac.

Si tu equipo es compartido con varias personas, puede que te interese crear distintas cuentas de usuarios con distintos niveles de privilegios. Si no las gestionas adecuadamente, corres el riesgo de:

- Que terceros puedan acceder a tus archivos y eliminar/modificar información personal, como imágenes, música, documentos importantes, etc.
- Modificar configuraciones de seguridad o usabilidad de tu sistema, como, por ejemplo, desactivar el antivirus o firewall.
- Conectarse a determinados servicios con tus credenciales, como el correo electrónico o red social.

Además, puedes gestionar las opciones de inicio de sesión en Windows y las opciones de inicio de sesión en Mac lo que te permitirá tener un mayor control sobre tu inicio de sesión.

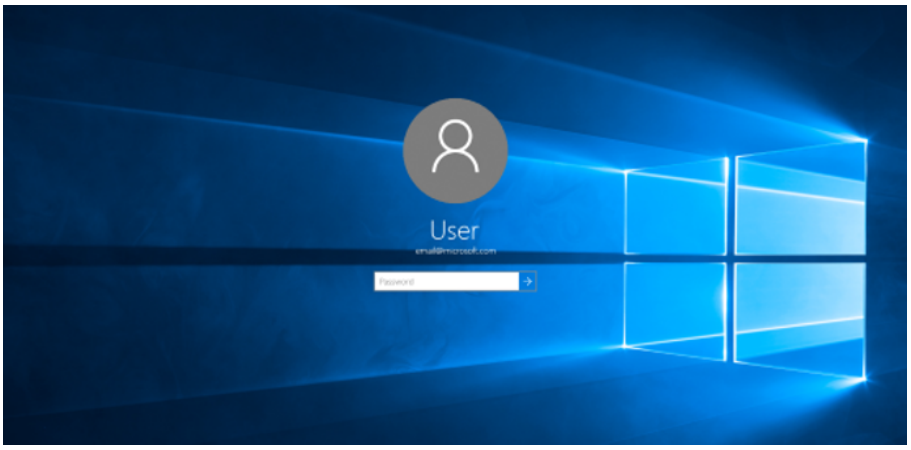

Figura 3.1: Cuenta de usuario Windows 10.

Existen tres tipos de cuentas distintas, cada tipo proporciona al usuario un nivel diferente de control sobre el equipo y son:

- Cuentas limitada o estándar: son aquellas que se deben utilizar para el trabajo diario con el equipo.
- Cuentas de administrador: proporcionan el máximo control sobre el equipo, por ejemplo para instalar un programa nuevo, y sólo se deberían usar cuando sea necesario.
- Cuentas de invitado: se usan principalmente por personas que necesitan usar temporalmente el equipo y no disponen de otra cuenta.

La utilización de cuentas limitadas diariamente, proporciona una mayor seguridad, puesto que impide la ejecución de diverso software malicioso (virus, gusanos, programas espía y troyanos) en algunos casos, como podría ser mientras navega por Internet o se conecta al equipo una memoria USB con ficheros infectados.

3.3 Router

Un router es un dispositivo que proporciona conectividad a nivel de red. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar. Además de ser el dispositivo que nos proporciona un punto de acceso Wi-Fi

Dispone de varios niveles de seguridad y estándares de cifrado, para que nadie pueda acceder a nuestra red y poder alcanzar cualquier dispositivo a través d la Wi-Fi.

Ordenados de menor a mayor grado de cifrado:

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2 (Wi-Fi Protected Access 2)
- WPA3 (Wi-Fi Protected Access 3)

Es importante que uses un nivel de seguridad WPA2 como mínimo, con el que vas a poder establecer una contraseña de hasta 63 caracteres en lugar de los máximos 29 de la WEP.

Para establecer una capa más de seguridad puedes realizar un filtrado MAC (Media Access Control). Un filtrado MAC consiste en la creación de una lista de dispositivos que tienen permiso para acceder al router, a pesar de que un tercero haya podido obtener la clave wifi.

Es igualmente importante que cambies la clave que el router trae por defecto. Este enlace te llevará a un generador de claves Wi-Fi donde podrás crear de forma automática una clave Wi-Fi segura y robusta.

De igual modo cambia la contraseña de acceso al router, para que solo tú puedas acceder a su configuración.

También es una buena práctica cambiar el nombre que la Wi-Fi trae por defecto, esto despistará a aquellos que puedan tener una lista de claves de acceso de las diferentes operadoras que existen en el mercado.

Otro aspecto a tener en cuenta es deshabilitar la opción WPS (Wifi Protected Setup) en el router. Esta función te permite conectar el ordenador o dispositivo a la Wi-Fi del router sin tener que escribir la contraseña cuando eliges tu red Wi-Fi desde el dispositivo. Se trata de un botón físico que traen algunos router y que al pulsarlo conecta el dispositivo de forma automática. Esta funcionalidad es muy práctica, pero conlleva el riesgo de que cuando pulsas este botón estás abriendo la Wi-Fi, lo que significa que inhabilitas todas las medidas de seguridad que tengas configuradas para la conexión. Si decides deshabilitarla puedes hacerlo desde la configuración

de tu router y normalmente vas a encontrarlo en los apartados Wireless o Network de la interfaz web (Xataka, 2020).

Para realizar cualquiera de las configuraciones propuestas en este apartado va a necesitar acceder a la interfaz de tu router y para ello, necesitarás saber la dirección IP de acceso. Esta te será facilitada por tu operador.

Visita el siguiente enlace para conocer las principales configuraciones del router.

3.4 Actualizaciones

Las actualizaciones de seguridad o parches son elaboradas por los desarrolladores y fabricantes de productos informáticos. Estos pueden tardar desde un día hasta meses para publicar un parche, en función del tipo de vulnerabilidad, dispositivos a los que afecte y otros criterios. Aunque también se realizan para mejoras de otras naturalezas, como, rendimiento, productividad, etc.

Tener actualizados los dispositivos es una medida más de seguridad. Para ello debes actualizarlos cada vez que el dispositivo lo solicita o en su defecto buscar una actualización disponible.

Las actualizaciones no solo corresponden al Hardware (ordenadores, smartphones, etc.), sino que también han de ser realizados en el software (programas), navegadores, antivirus, etc.

La principal función de las actualizaciones son las de mejorar tanto la funcionalidad como la seguridad de los dispositivos o software (OSI, 2021a).

3.5 Antivirus, antimalware, antispyware y firewall

Aunque a priori pudiese parecer lo mismo, los antivirus, antimalware, antispyware y firewall, cumple funciones diferentes, pero con un mismo fin, mantener la seguridad de tus equipos. La mayoría de estos tipos de software los puedes encontrar en dos modalidades: gratuita y de pago (Enetic, 2021).

- Antivirus: Es un programa que detecta la presencia de virus informáticos (software malicioso que altera el funcionamiento normal del ordenador sin que el usuario lo sepa o consienta) y los elimina o repara. Algunos ejemplos de antivirus son: Avira, Avast, AVG, Virus Total (online), entre muchos más.
- Firewall o cortafuegos: Es una parte de la red o el sistema que se realiza para bloquear accesos no autorizados y permitiendo los que sí lo están. Se pueden hacer por medio de software o hardware, y permiten una

mayor protección a las redes, especialmente importante en empresas que cuentan con datos que han de ser bien protegidos. El firewall más conocido es el Windows.

- Antispyware: Es un conjunto de herramientas que sirven para prevenir y eliminar Spywares (espías o programas que recopilan información del ordenador para transmitirla a otras personas sin el consentimiento ni conocimiento del propietario del ordenador). Algunos ejemplos de antispyware son: SpyBot, SuperAntiSpyware, SpywareBlaster.
- Antimalware: Es un software encargado de eliminar el software malicioso (malicious-software, malware) del ordenador tras un minucioso análisis del sistema. Algunos ejemplos de antimalware son: HiJackThis, Antimalware.

Dependiendo de las necesidades pueden ser usados uno o varios, ya que son complementarios entre sí.

Antes de decidir que herramientas de las anteriormente expuestas va a usar, puedes hacer una búsqueda e informarte sobre las opciones disponibles, ya que existen soluciones de todo tipo y para todos los gustos, gratuitas, de pago, para ordenadores, para smartphones. Desde la Oficina de Seguridad del Internauta ponen a tu disposición este listado de Antivirus gratuitos, para que puedas elegir el que mejor se adapte a tus necesidades. Pero no olvides nunca de asegurarte muy bien que estás ante un producto legítimo y descargarlo siempre de la web oficial.

Cabe destacar que Windows de un tiempo aquí ya trae de manera nativa su propio antivirus conocido como Windows Defender.

3.6 Copias de seguridad

Una copia de seguridad o backup en informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos, como por ejemplo, recuperar los sistemas informáticos o datos de una posible catástrofe informática, natural o intencionada, restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido o infectado por un virus informático u otras posibles causas (Wikipedia, 2021c).

Simplificando el sistema de copias de seguridad que en algunas ocasiones puede llegar a ser complejo, están los siguiente:

- Completas: Del sistema operativo completo, de esta forma al restaurar la copia, dispondremos de nuevo de toda la configuración a nivel de

S.O., software instalado, carpetas y archivos. Para este cometido vamos a necesitar de programas de terceros, algunos de ellos con versiones gratuitas y de pago, ejemplo de estos son: Acronis, AOMEI, EaseUS. Aunque más abajo verás que también pueden hacerse nativamente.

- Parciales: En este escenario lo que se hace es salvaguardar las carpetas y archivos personales. Como por ejemplo, carpetas con fotografías, documentos personales y demás. Esto lo puedes hacer de forma manual o con programas destinados a este propósito como por ejemplo lo es el FreeFileSync con el que puedes hacer copias manuales o automatizadas.

Y las copias pueden ser mantenidas:

- En almacenamientos externos: Tales como, discos duros externos, DVD, entre otros. De esta forma podemos custodiarlos a buen recaudo.
- En la nube: Estos son servicios de terceros accesibles online, ejemplo de ello son: BackBlaze, Carbonite, siendo estos especializados en backups. Pero si tus copias de seguridad se limitan a tus carpetas y archivos personales puedes usar un servicio en la nube, como Google Drive, Onedrive o Dropbox.

Las copias de seguridad debes realizarlas con la frecuencia que sea necesaria para garantizar tu nivel de seguridad (Media Cloud, 2021).

Puedes crear una copia de seguridad de tu sistema operativo fácilmente ya que tanto Windows como Mac traen esta opción de forma nativa, solo necesitaras disponer de un dispositivo externo de almacenamiento en el que puedas guardar la copia con espacio de almacenamiento suficiente. Para Windows tienes la guía en el siguiente enlace de como realizar y restaurar una copia de seguridad del PC, y para los dispositivos Apple la guía la encontrarás en cómo hacer copias de seguridad en Mac.

Una práctica muy recomendable a la hora de hacer copias de seguridad es seguir la estrategia 3-2-1 (INCIBE, 2018a) y que consiste en:

- Mantener 3 copias de seguridad: una principal con la que trabajar y dos de backups.
- Mantener la información en 2 tipos de almacenamiento distintos, por ejemplo, en un disco duro y en la nube.
- Mantener 1 copia de seguridad en un lugar diferente a los demás.

Las copias de seguridad no son solo exclusivas de los PCs o portátiles, sino que también debes contemplarlas en tus dispositivos móviles. Android pone a tu disposición el recurso de cómo crear copias de seguridad o restaurar datos

de un dispositivo Android y Apple el de cómo hacer una copia de seguridad del iPhone, iPad y iPod touch.

Es muy importante que dispongas de copias de seguridad, pero igualmente de importante es que conozcas la salud de los dispositivos de almacenamientos que usas. Para ello existe software específico que realiza diagnósticos e incluso algunos tienen sistemas de reparación. De esta forma podrás saber si debes cambiar el dispositivo o no, antes de quedar en la estacada.

Software de diagnóstico y/o reparación de unidades de almacenamiento:

- CrystalDisk: Diagnóstico de discos HDD.
- HdSentinel: Diagnóstico y reparación de discos HDD.
- HDDScan: Diagnóstico discos de HDD, SSD y memorias USB (pendrives).
- Check Flash: Diagnóstico de memorias USB (pendrives).

Por otro lado, si has borrado accidentalmente información y tu copia de seguridad no está totalmente actualizada, quizá te interese saber que también existe software de recuperación de datos eliminados, siempre y cuando no haya pasado el suficiente tiempo para que la información eliminada haya sido reescrita. Recuerda que la información eliminada solo se produce de forma definitiva cuando se reescribe dicha información.

Aunque este último apunte no está estrechamente relacionado con la seguridad en equipos físicos, que es el tema que se trata en esta unidad, nunca está de más saber que tienes esta opción, para poder recuperar datos perdidos.

Para recuperar tu información dispones de software como:

- Recuba: PC.
- Wise Cleaner: PC.
- Videos y audios Recovery: Smartphone.
- File Recovery: Smartphone.

3.7 Cifrado o encriptado de unidades de almacenamiento

Cifrar o encriptar tus discos duros ya sean externos o internos del ordenador o el encriptado de un simple Pendrive o USB es cada día más necesario para protegernos contra los amigos de lo ajeno, ya que aunque te sustrajesen el ordenador o cualquier otro dispositivo, no podrían acceder a la información

puesto que se encuentra bajo esta capa de seguridad robusta que es la encriptación.

El cifrado de dispositivos es una tecnología que cifra todos los datos almacenados en discos duros o cualquier otro dispositivo de almacenamiento externo, con sofisticadas funciones matemáticas recogidas en lo que se conoce como criptografía. De manera que para poder acceder a la información almacenada en el disco duro o pendrive en necesario tener la contraseña o clave de acceso (Blog de ayuda ley protección de datos - encriptación, 2020).

Existen varias herramientas en el mercado para este cometido como las detalladas a continuación:

- BitLocker. Software nativo del sistema operativo Windows.
- FileVault. Software nativo del sistema operativo de macOS.
- Veracrypt.
- Diskcryptor.
- Comodo Disk Encryption.

También tienes a tu disposición el siguiente enlace que te llevará a la revista digital Computerhoy donde te explican como encriptar tu ordenador Windows o Mac.

Capítulo 4

Gestión de la seguridad en la red

4.1 Gestionar la seguridad en la red

Como ya viste en la unidad de privacidad y seguridad, la seguridad en internet son todas aquellas precauciones que deben ser tomadas para proteger todos los dispositivos informáticos, así como la red de internet que pueden ser afectados por delincuentes cibernéticos.

Pero, ¿Qué es la red?. La red son un conjunto de servidores conectados entre sí y que son capaces, mediante un protocolo previamente establecido, de compartir datos y recursos. Por lo que, Internet, sería la interconexión de un conjunto de Redes entre sí a nivel mundial. No es una única Red, sino múltiples Redes conectadas entre sí, «hablándose» en todas ellas con el mismo «idioma» (protocolo).

Estas redes pueden ser:

- Públicas (accesibles a todo el mundo).
- Privadas (solo a los usuarios autorizados).

Más adelante verás de qué situaciones y amenazas te estás protegiendo si sigues todas estas recomendaciones.

4.2 Seguridad en las cuentas

Prácticamente todo el mundo en menor o mayor medida dispone de cuentas de usuarios en todas sus aplicaciones o servicios en la red. De entre las más conocidas están la cuenta de Google y la de Microsoft. En estos dos enlaces podrás ajustar la seguridad necesaria para poder hacer uso de ellas con más garantías. Además, recuerda que el resto de plataformas deben ofrecerte este servicio para que puedas configurar tu seguridad y dentro de lo posible estar más tranquilo.

4.3 Contraseñas

Una contraseña, clave o password es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso (Wikipedia, 2021b).

Su utilidad consiste en que a aquellos que desean acceder a la información se les solicita una clave o contraseña, si conocen dicha contraseña se les concede el acceso y si no la conocen, se les niega el acceso a la información.

Estas deben ser lo más seguras posibles y para ello debes crearlas bajo las siguientes:

- Debes incluir números.
- Utiliza una combinación de letras mayúsculas y minúsculas.
- Incluye caracteres especiales. Ejemplos: * ? ! @ # $ / () {} = . , ; :
- Una longitud mayor o igual a 8 caracteres.
- No debes incluir espacios en blanco.

Una modalidad de crear contraseñas robustas y fáciles de recordar es la siguiente (OSI, 2021b):

1. Elige una extensión de más de 8 caracteres. Ejemplo: Mi cuenta segura
2. Pon la primera mayúscula y elimina los espacios en blanco. Ejemplo: MiCuentaSegura
3. Cambia las letras por números. Ejemplo: M1Cu3nt4S3gur4
4. Añade caracteres especiales. Ejemplo: M1Cu3nt4S3gur4!
5. Personaliza la clave para cada servicio. Toma las dos primeras letras del servicio, para el caso de Facebook son la F y la A y colocalas una delante y otra detrás. Ejemplo: FM1Cu3nt4S3gur4!A

En la Oficina de Seguridad del Internauta tienes toda una suit de recursos para crearte la mejor de las contraseñas posible. Accede desde este enlace Contraseñas seguras.

También es recomendable que la cambies cada cierto tiempo, al menos aquellas que sean de mayor importancia. Algunas de las razones de por qué debes cambiar la contraseña cada cierto tiempo son:

- Puedes recibir un falso correo de sextorsión en el que simulan que tienen fotos o vídeos comprometidos, cuando en realidad no es así. Este escenario se vuelve más creíble cuando además va acompañado de una contraseña que llevas años sin cambiar.

- Puede que tus contraseñas estén disponibles junto con otras miles en forma de packs en la Deep web al alcance del mejor postor. Aquí tienes una entrada del periódico digital el mundo llamada Se filtran 8.400 millones de contraseñas, ¿qué debo hacer para saber que estoy a salvo? donde podrás obtener mayor información al respecto.

A su vez también han de ser fáciles de recordar, pero debes de huir de patrones poco seguros y fáciles de adivinar. A continuación, algunos ejemplos de contraseñas que nunca debes utilizar:

- Qwerty
- 1234
- Asdfg
- Password
- 11111
- Usar datos personales como la fecha de nacimiento, nombre mascota, etc.

En el siguiente enlace encontrarás una lista de las contraseñas más comunes que jamás deberías utilizar. Échale un vistazo por si alguna de esas se parece a la tuya.

Algunas reglas y ejemplos para que las contraseñas sean fáciles de recordar los encontrarás en estos enlaces:

- Trucos para crear contraseñas seguras
- Consejos para crear contraseñas seguras
- Cómo crear contraseñas con reglas mnemotécnicas

Otras recomendaciones que debes tener siempre presente son:

- No las compartas con nadie.
- No uses la misma contraseña en diferentes servicios.
- No las almacenes en el navegador.
- Evita usarlas en dispositivos públicos.
- Usa la verificación en dos pasos también conocida como autenticación doble.
- Usar Security keys o llave de seguridad. Verás que son más adelante en esta misma unidad en el apartado de MFA (Multi-Factor Authentication)

- Usa gestores de contraseñas, a continuación tienes algunos de estos servicios:
  - Bitwarden
  - LastPass
  - Google passwords
  - NordPass
  - Dropbox passwords

Si quieres una lista más exhaustiva de estas plataformas gestoras de contraseñas, visita el siguiente enlace de la Oficina de Seguridad del Internauta de gestores de contraseñas.

Para acabar con este apartado puedes comprobar la seguridad y robustez de tu contraseña, con los siguientes recursos online:

- How Secure Is My Password
- Password Check
- Test contraseñas
- ¿Cuánto tarda un hacker en forzar tu contraseña?

Por otro lado si eres de las personas que te gusta tener todo bajo control puedes usar este servicio de Google llamado Password Checkout o estos otros llamados Haveibeenpwned Passwords y ¿Ha sido mi contraseña robada? para averiguar si alguna de tus contraseñas ha sido comprometida.

Si quieres, también puedes usar un generador de contraseñas fuertes como el que te ofrece F-secure o Pinetools.

A modo de conclución, si tuviésemos que simplificar parte de lo anterior en tres puntos a tener siempre presente en la creación de contraseñas sería de la siguiente manera:

- Deben ser secretas: por lo que no deben compartirse absolutamente con nadie.
- Deben ser robustas: longitud mínima de ocho caracteres, que combine mayúsculas, minúsculas, números y símbolos.
- Deben ser únicas: se deben utilizar contraseñas distintas en diversos sitios, por ejemplo la contraseña de usuario debería ser distinta de la del correo electrónico.

Y por último, si quieres conocer los 5 métodos más usados por los ciberdelincuentes para el robo de contraseñas échale un ojo la al siguiente enlace Cómo hacen los hackers para robar la contraseña: los 5 métodos más usados

4.4 Protocolo https

El Protocolo seguro de transferencia de hipertexto (en inglés: Hypertext Transfer Protocol Secure o HTTPS), es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP (Wikipedia, 2021i).

El sistema HTTPS utiliza un cifrado basado en la seguridad de textos SSL (Secure Sockets Layer) o su versión actualizada TLS (Transport Layer Security) para crear un canal cifrado.

De este modo se consigue que la información sensible como el usuario y la contraseña, no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar.

Identificar si el protocolo https está activado en el navegador es muy sencillo, sólo debes fijarte en la parte superior izquierda de tu navegador. Si tu URL inicia con https: //, o bien, antes de la dirección se muestra un candado, estarás navegando con seguridad bajo el protocolo https.

Figura 4.1: Protocolo https vs http.

Si haces click en el candado, éste te mostrará que se trata de una conexión segura, así como el tipo de certificado de seguridad, cookies y la configuración del sitio web.

En el enlace del Incibe Qué hacer si el navegador nos dice que estamos intentando acceder a un sitio no seguro explican el aviso del navegador cuando nos advierte que se trata de un sitio no seguro, o lo que es lo mismo, que cuando el navegador se está refiriendo a que el sitio web tiene un protocolo “http: //” sin la “S” en lugar de “https: //” con la “S”.

IMPORTANTE: Tener el candado no garantiza que la web sea legítima. Ya que los certificados de cifrado seguro los emiten terceros y los ciberestafadores pueden hacerse igualmente con uno. Sobre todo si se trata del certificado de dominio, que el único requisito es que la persona figure como contacto de administrador de dominio en el registro WHOIS de un nombre de dominio. Se trata del nivel más bajo de autenticación utilizado para validar

certificados SSL. Si quieres más información sobre este primer nivel de certificado y los dos siguientes que ofrecen mayores garantías de legitimidad, visita el siguiente enlace ¿Cuáles son los tipos de certificados SSL? o este otro Diferencias y tipos de certificados de seguridad SSL.

4.5 Compras y transacciones

Para comprar por Internet debes tomar cuantas más precauciones mejor para evitar cualquier tipo de fraude. Los factores a tener en cuenta son los siguientes:

- Evita sitios webs que no te inspiren confianza: Por ello solo debes compras a través de webs y aplicaciones oficiales.
- Busca valoraciones y opiniones: Para ello dispones de las reseñas de Google maps, así como también de plataformas como Trust Pilot, Gowork, Esopiniones, Local guides connect o TripAdvisor.
- Utiliza plataformas que identifican webs fraudulentas como Fakeinet, Desenmascarame o Dnstwist que disponen de un listado de posibles tiendas falsas.
- Usa plataformas que verifican si la web ha sido hackeada, como Scamadviser o Urlscan.
- Usa solo plataformas con protocolo HTTPS: Visto en el apartado anterior. Y recuerda que tener el candado no garantiza que la web sea legítima. Ya que los certificados de cifrado seguro los emiten terceros y los ciberestafadores pueden hacerse igualmente con uno.
- Utiliza navegación privada: Así evitarás que se registre el historial de navegación.
- Trata de usar pasarelas de pago: Evita en lo posible el uso de tarjetas de crédito y opta por una pasarela de pago, como puede ser PayPal, te estarás garantizando la compra, además de disponer de protocolos de devolución del importe muy efectivos.
- En el caso de usar tarjeta de crédito usa siempre la misma o mejor aún utiliza tarjetas monedero o virtuales que facilitan los bancos con el fin de depositar solo en dinero con el que quieras hacer la compra.
- Haz comprobaciones adicionales:
  - Comprueba que la web está adherida a alguna plataforma de confianza online, como, por ejemplo, Confianza Online. Se trata del único sello de calidad que cuenta con los reconocimientos de la

Comisión Europea, el Instituto Nacional de Consumo o la Agencia Española de Protección de datos, además de estar respaldado por el Ministerio de Industria, Energía y Turismo. Y acredita que se cumple con los estándares de privacidad y protección de datos de los usuarios entre otros. También existe el Certificado de comercio electrónico expedido por Aenor.

- Verifica que reciben análisis de seguridad periódicos realizados por plataformas como McAfee Secure.
- Asegúrate que disponen de certificados de autenticidad de la web y seguridad de las transacciones como los que ofrece Norton secured o Comodo secure.
- También existen plugins como Historial de precios o Alitools shopping assistan que verifican si el precio del producto o servicio que deseas adquirir ha sido inflando por algún tipo de campaña publicitaria, como es el caso del Black Friday en los que suelen subir los precios para justificar su descuento.
- En primera instancia desconfía de los productos o servicios a precios muy inferiores al real o con suculentos descuentos.
- Verifica que las reseñas sean legítimas con plataformas como Review Meta y Fake Spot. Si quieres saber más sobre las campañas de reseñas fraudulentas lee esta entrada sobre reseñas falsas.
- Los sellos y certificados los encontrarás normalmente en la parte inferior de la web en forma de logos y debes hacer click en ellos para obtener más información sobre la entidad que los expide y la vigencia de éstos, ya que muchas webs fraudulentas utilizan sellos falsos.

Figura 4.2: Sellos y certificados de comercio online.

Tienes disponible más información sobre compras online en Compra segura en internet (Guía práctica) y también dispones de esta entrada de cómo detectar fraudes y análisis de una web falsa.

4.6 Wi-Fi

Con respecto a la Wi-Fi nos encontramos ante dos escenarios: Wi-Fi propia y Wi-Fi ajena.

Uno de los peligros a los que más expuesto estás, es en el uso que haces de los puntos Wi-Fi ajenos. Ya que por lo general suelen ser puntos de accesos a la red gratuitos. En este escenario, existe el riesgo que aun tratándose de una red confiable puede haber sido hackeada por un tercero o que en primera instancia no provenga ni si quiera de una red de confianza. En cualquiera de los dos supuestos, tus dispositivos quedan expuestos y con ello, toda tu información sensible, a merced de ser espiado, robado o extorsionado.

Es por ello que debes tener la precaución de no hacer transacciones de ningún tipo, ni enviar datos sensibles. Es decir, usarla solo en caso de no te quede otra opción o en caso de tener que hacer cualquier búsqueda de carácter trivial.

Aun así, si usas una Wi-Fi pública estás expuesto entre otros ataques al conocido como Man-in-the-middle (Ataque de Intermediario en español), o el Packet sniffing. Si quieres más información al respecto visita el siguiente enlace Tipos de pirateo que puedes sufrir en un Wifi público

Es de suponer que si estas en casa con Wi-Fi propia, estas recomendaciones no son tan necesarias. Pero sí, que sería muy recomendable por tu parte, que tuvieses muy en cuenta las recomendaciones que tienes a tu disposición en el apartado de Router en este manual. Además, es conveniente que si no has establecido las capas de seguridad que se recomiendan en ese apartado, hagas una revisión de tu conexión Wi-Fi, por si tienes algún intruso y de ser así poder eliminarlo. Para ello tienes a tu disposición en el blog de la Oficina de Seguridad de Internauta un recurso llamado descubre y elimina a los intrusos de tu red wifi.

Lo más recomendable es que siempre que puedas navegues con cable en lugar de Wi-Fi.

4.7 Plugins o extensiones

En informática, un complemento o plugin es una aplicación (o programa informático) que se relaciona con otra para agregarle una función nueva y generalmente muy específica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de la interfaz de programación de aplicaciones. Complemento y plug-in se diferencian en que los complementos son desarrollados por empresas reconocidas y tienen certificado de seguridad y los plug-in pueden ser desarrollados por cualquiera (IONOS by 1and1, 2020b).

Existen una infinidad de plug-in de diferente naturaleza y para multitud de propósitos. En esta ocasión nos vamos a centrar en los usados por los navegadores, un ejemplo de estos es el archiconocido adBlock, cuya función es la eliminar esos molestos anuncios de algunos portales webs.

Estos pueden estar desarrollados por terceros con intenciones de controlar la información que manejamos en nuestro dispositivo. De ahí que deban proceder de fuentes fiables y que estén configurados para actualizaciones automáticas.

Cada navegador dispone de repositorio de plug-ins o extensiones, que pueden ser consultados y desde donde los puedes instalar y comprobar su fiabilidad, así como consultar las valoraciones.

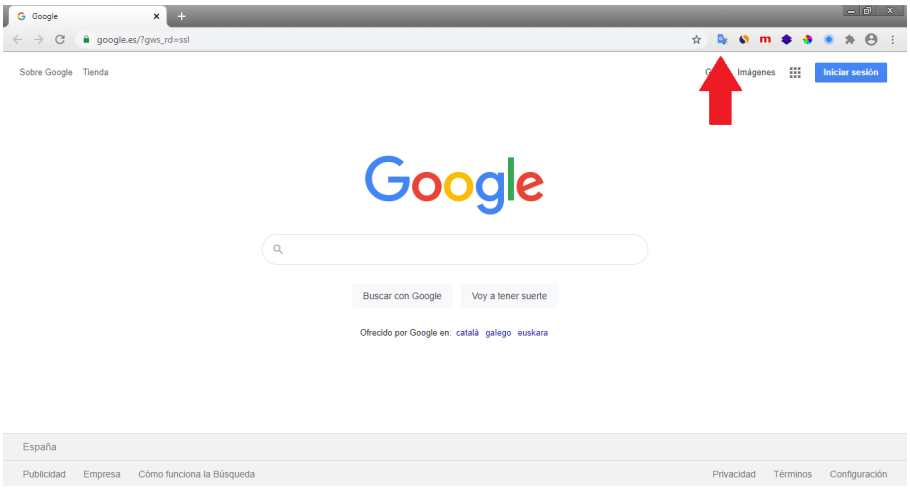

Figura 4.3: Plugin traductor de Google seguido de otros plugin con diferentes funcionalidades.

Si quieres ampliar tu conocimiento y saber más de plugins y extensiones pásate por el blog de la Oficina de Seguridad de Internauta y lee esta entrada sobre extensiones: Superpoderes para los navegadores.

4.8 Descargas

Debes de tener muy en cuenta que las aplicaciones o programas deben ser descargadas desde sus sitios oficiales, y no desde otros. Es importante tener siempre presente que, incluso en ocasiones ni si quiera los antivirus reconocen algunas aplicaciones o programas que pudieran contener alguna vulnerabilidad, algún virus o gusano que afecte tu ordenador.

Existen también multitud de webs que en apariencia, ofrecen programas muy mediáticos o de mucha popularidad y que pueden haber sido previamente infectados con algún tipo de código malicioso mediante la modificación o alteración del mismo. Por ello, lo más aconsejable es que descargues las aplicaciones desde las webs oficiales (Google books, 2021).

Dentro de todos los tipos de archivos que pueden contener malware, uno de los más comunes es el .EXE. Incluso a la hora de descargar archivos de este tipo nuestro antivirus puede saltar, aunque no se trate de una amenaza e incluso cuando quieras mandar un EXE por e-mail tampoco está permitido, por cuestiones de seguridad. Es todo un clásico, ya que se trata de un archivo ejecutable que podría instalar software malicioso en nuestro sistema. Hay que tener mucho ojo siempre que gestiones un archivo de este tipo (Redeszone, 2020).

Es una buena práctica huir de portales de terceros, ya que con los instaladores muchos de ellos descargan malware y molestas toolbars.

4.9 Cierre de sesiones

Cuando hagas uso de algún servicio en internet, como por ejemplo, Facebook, Gmail o cualquier otro, lo primero que tienes que hacer es iniciar sesión con tus credenciales.

Si estas en tu dispositivo no pasaría nada si una vez abierta la sesión no la cierras después de haber usado el servicio, pero si por el contrario estas usando un dispositivo ajeno, el servicio quedaría abierto y tus datos expuestos.

Por la razón antes expuesta, es importante que no dejes ninguna sesión abierta.

4.10 2SV (Two Step Verification) o Verificación en Dos Pasos

La mayoría de cuentas a día de hoy están configuradas para soportar lo que se conoce como SFA (Single Factor Authetication) o Factor de autenticación Simple. Se trata del acceso a cuentas o servicios con el solo uso del usuario y una contraseña, algo que todo el mundo viene haciendo desde hace tiempo. Esto se ha vuelto en gran medida un gran riesgo, ya que si un tercero consigue hacerse con tu contraseña no tendrá ninguna dificultad para tomar el control.

Es por este motivo que cada vez más servicios están implementando lo que se conoce como 2SV (Two Step Verification) o Verificación en Dos Pasos. Este sistema funciona de la siguiente manera, justo después de introducir tu contraseña, se te envía una notificación de forma segura al dispositivo en el que hayas iniciado sesión, de manera que solo tienes que aprobar la notificación para realizar el inicio sesión. Algunos servicios como la verificación en dos pasos de Google viene de manera nativa y tan solo tienes que activarla.

Como puedes ver, los dos pasos son:

1. Usuario y contraseña: Que solo tú conoces.
2. Notificación: Recibes un aviso en tu dispositivo.

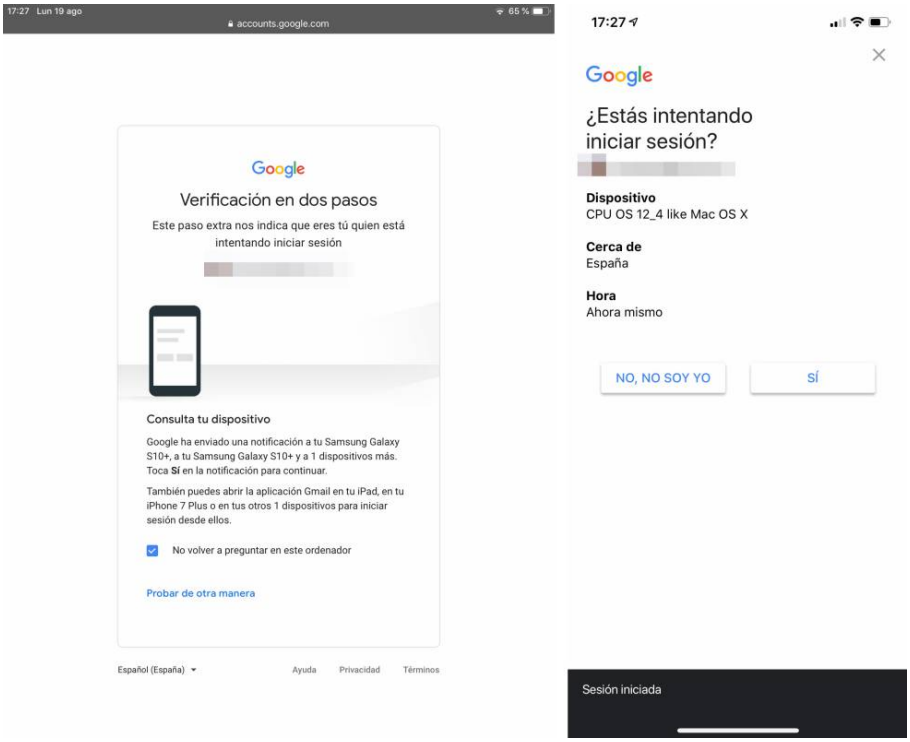

Figura 4.4: Verificación en dos pasos.

Según la fuente que uses para informarte puede ser que termines sin comprenderlo del todo, ya que algunos medios también entienden la verificación en dos pasos (2SV) como un 2FA (segundo factor de autenticación). La diferencia es tan sutil que a veces es difícil de discernir, pero podría entenderse si ves el 2SV como una notificación que recibes y que apruebas sin más y la 2FA como un código que has de introducir. No obstante si quieres más información, en este enlace sobre verificación en dos pasos encontrarás más detalles, además de enlaces hacia las distintas plataformas y redes sociales más populares para que puedas implementarlo.

Es extremadamente recomendable que uses este sistema de verificación en la medida que puedas. Recuerda que de un modo u otro la mayoría de servicios y plataformas disponen de esta capa de seguridad. Normalmente las encontrarás en Ajustes y Seguridad.

4.11 MFA (Multi-Factor Authentication) o Autenticación de Factores Múltiples

La autenticación de factor múltiple es una forma eficaz de aumentar la protección de las cuentas de usuario contra las amenazas más comunes, como los ataques de phishing, apropiación de cuentas, etc. Y se trata un

método de control de acceso informático, en el que a un usuario, se le concede acceso al sistema solo después de que presente dos o más pruebas o factores diferentes de que es quien dice ser. Estas pruebas pueden ser diversas, como una contraseña, clave secundaria rotativa, un certificado digital instalado en el equipo, un token físico, etc. entre otros y son éstos lo que se conocen como factores de autenticación (Wikipedia, 2018).

Son tres los tipos de factores de autenticación:

- Algo que sabes: Factor de conocimiento (contraseña, respuesta a una pregunta, un PIN).
- Algo que tienes: Factor de posesión (tarjeta, smartphone, token hardware como las Security keys).
- Algo que eres: Factor biométrico (huellas dactilares, escaneos de retina, reconocimiento facial, reconocimiento de voz o el comportamiento de un usuario).

Uno de los ejemplos de autenticación en dos factores más común es la acción que realizas cuando vas a sacar dinero de un cajero. Por un lado, metes la tarjeta (algo que tienes) y luego pones el PIN (algo que sabes). Esto es lo que se conoce como la autenticación en dos pasos o 2FA (segundo factor de autenticación) y que a veces tiende a confundirse con la verificación en dos pasos 2SV (Two Step Verification) que puedes verla en esta misma unidad.

Otro ejemplo son los inicios de sesión en los que se necesita un código adicional que es gestionado a través de correo electrónico, SMS o llamadas telefónicas, como es el caso de algunas entidades bancarias, esto es lo que se conoce como OTP por sus siglas en inglés “One-Time Password” y en castellano “contraseña de uso único”. Y en otros supuestos, aunque la plataforma disponga de dicho servicio necesitarás una aplicación externa como Google Authenticator o Microsoft authenticator entre otras y que se trata de una App de autenticación en dos pasos, que te genera el código adicional, que ha de ser utilizado inmediatamente ya que éste expira con el tiemplo.

También puedes hacer uso de autenticación de factores múltiples con lo que se conoce como Security Key o llave de seguridad. Se trata de un dispositivo hardware generalmente con conexión USB y necesitarás usar como segundo factor de autenticación una vez hayas introducido tu usuario y contraseña. En la publicación las mejores llaves de seguridad usb encontrarás algunos de los más utilizados y recuerda siempre comprar en las plataformas oficiales o de confianza.

En la mayoría de los casos solo se combinan dos de estos tres factores, aunque existe la posibilidad de implementar los tres si se viene necesario.

Figura 4.5: Autenticación de factores múltiples.

Más información en Banco Santander stories y Autenticación en dos factores vs autenticación en dos pasos.

4.12 AntiBotnet

Un Botnet es el nombre genérico para denominar a cualquier grupo de PCs infectados y controlados por un ciberdelincuente de forma remota. Generalmente se trata de un hacker o un grupo de ellos los que crean el botnet a través de un malware que infecta a una gran cantidad de equipos. Este grupo de equipos u ordenadores son los que forman parte del botnet, o también llamados "bots" o "zombies". No existe un número mínimo de equipos para crear un botnet. Los botnets pequeños pueden incluir cientos de PCs infectados, mientras que los mayores utilizan millones de equipos (INCIBE, 2021d).

Para saber si estás siendo víctima de este tipo de ataque, existen servicios antibotnet que identifican si desde tu conexión a internet se ha detectado algún incidente de seguridad relacionado u otras amenazas. Además en el siguiente enlace obtendrás una suite de rastreo y eliminación de Botnet Servicio Antibotnet: Cleaners.

4.13 Bluetooth

El Bluetooth es otro punto vulnerable en tu seguridad en la red. El Bluetooth, viene incorporado en multitud de dispositivos y permite conectarnos con otro dispositivo para compartir archivos o emparejar determinados dispositivos, como auriculares inalámbricos, etc. (IONOS by 1and1, 2020a).

Y sus principales amenazas son:

- Bluejacking: envían spam a la víctima mediante notas, contactos,

imágenes, etc. Puede resultar peligroso y convertirse en una denegación de servicio dirigida a un objetivo o espacio (por ejemplo, un bar).

- Bluesnarfing: se beneficia de las vulnerabilidades más comunes para obtener datos confidenciales del dispositivo atacado.
- Bluebugging: aprovecha bugs (fallos de programación) para ejecutar comandos en el terminal y controlarlo.

El riesgo que corres cuando tienes este servicio activado es que el dispositivo de un tercero acabe sincronizándose con el tuyo, con los riesgos expuestos. Para evitarlo, una vez hayas terminado, mantenlo desactivado.

Si quieres más información visita el siguiente enlace Diferencias entre los principales ataques por bluetooth: Bluesnarfing, Bluejacking y Bluebugging.

4.14 NFC (Near field communication)

El NFC, es una tecnología inalámbrica de corto alcance que permite conectar dos dispositivos entre sí para intercambiar información o realizar pagos (IONOS by 1and1, 2019).

Sus principales amenazas son:

- Ejecución de programas maliciosos: ejecuta código en terminales Android simplemente acercando una etiqueta NFC al dispositivo.
- Pagos sin autorización: realiza compras por proximidad sin consentimiento (limitadas a un máximo de 20€).
- Transmisión de datos sin cifrar: lee datos como el nombre, apellidos, el número de la tarjeta y, en algunos casos, las transacciones realizadas.
- Copia de datos bancarios: con el empleo de Lectores con comunicación inalámbrica NFC.

El riesgo al que te expones si tienes este servicio activado es que el dispositivo de un tercero acabe sincronizándose con el tuyo, con los riesgos expuestos. Para evitarlo, una vez hayas terminado de usarlo, desactívalo. Otra opción es llevar un protector antirobo de tarjetas.

Capítulo 5

Amenazas

5.1 Principales amenazas

En lo referente a la seguridad de tus dispositivos debes tener en cuenta la diversidad de amenazas que existen, tales como virus, spywares, troyanos, gusanos y que pueden comprometer tus dispositivos y toda la información que en ellos contengas.

La mayoría de éstos están catalogado como Malware. Un Malware es un tipo de software malicioso con un primer objetivo inicial de infiltrarse en un equipo o sistema informático sin el consentimiento del usuario, para posteriormente actuar sobre él (Wikipedia, 2021g).

En este punto es importante que sepas cuáles son todas y cada una de las amenazas a las que estas expuesto, si no tienes las herramientas y no adoptas una actitud prudente en el uso de los dispositivos y la red.

En unidades anteriores viste que precauciones y herramientas debes adoptar para no correr riesgos. En esta unidad verás cuáles son estas amenazas y como llegan a tus dispositivos.

Las amenazas vienen de la mano de perfiles a los que conoces como hacker, ciberdelicuente, pirata informático, etc. Pero cabe destacar que estos conceptos no son lo mismo (OSPI, 2018). Por lo tanto:

- Ciberdelincuentes: Sus ataques se dirigen a objetivos concretos como escuelas, hospitales, instituciones, grandes empresas o bancos, entre muchos otros.
- Ciberterroristas y ciberyihadistas: Organizaciones terroristas que han desarrollado sus propias divisiones informáticas, aunque todavía no parecen ser capaces de desarrollar ciberataques sofisticados.
- Hackivistas: Grupos reivindicativos que actúan por razones ideológicas.
- Cibervándalos: Simplemente responden al deseo de armar revuelo y suelen ser ciberdelincuentes amateurs y poco cualificados.

Dispones de más información en hacker vs ciberdelincuente y ¿Quiénes son los ciberdelincuentes y qué buscan?.

¿Cómo detectar si estás infectado?

- Cambios en el navegador, página de inicio distinta, nuevos favoritos o barras de herramientas.
- Ordenador ralentizado.
- Ventanas emergentes inesperadas.
- Perdida de espacio en la memoria ram o disco duro.
- Apagón del equipo de manera inesperada.
- Mensajes anormales a la hora de encender el equipo.
- Mensajes de alertas inesperados.
- Ficheros cambiados de nombre o desaparecidos.

Una buena práctica para minimizar los riesgos es disponer de una suite de seguridad que estaría básicamente formada por:

- Antivirus.
- Anti-Spyware.
- Firewall o corta fuegos.
- Copia de seguridad.
- Discos de arranque.
- Anti-phishing. El phishing lo verás en esta misma unidad más adelante.

Si hay menores en casa:

- Control parental.
- Filtro web que restringe el acceso a contenidos no apto para menores.

Los tres ciberataques que encabezan el ranking son:

1. Fraude de ventas.
2. Vulnerabilidad de los equipos.
3. Infecciones por malware que pretenden borrar datos, alterar las funciones básicas del equipo, espiar y/o robar datos.

5.2 Virus

Un virus es un programa informático diseñado para infectar archivos u ocasionar efectos molestos, destructivos e incluso irreparables en tu ordenador, dañando hardware, software y archivos (Panda Security, 2021c).

Los virus tienen diferentes vías de entrada a tus equipos, como por ejemplo:

- Utilización de una memoria USB previamente infectada.
- Descarga de contenidos mediante redes de compartición P2P, u otras fuentes poco fiables.
- Apertura de algún fichero adjunto en un correo electrónico.
- Visitar una web maliciosa o pulsar sobre alguna dirección acortada que se publican en redes sociales u otros medidos y que en realidad no sabes a qué páginas web te puede llevar.

5.3 Gusanos informáticos

Los gusanos son en realidad una subclase de virus, por lo que comparten características similares (Panda Security, 2021a).

El principal objetivo de los gusanos es propagarse y afectar al mayor número de dispositivos posible, colapsar los ordenadores y las redes informáticas e impidiendo así el trabajo a los usuarios.

A diferencia de un virus, un gusano no necesita realizar cambios en los archivos de programas, sino que se aloja en diferentes ubicaciones del ordenador, principalmente la memoria RAM, para seguidamente clonarse a sí mismo y usar tus contactos y otros recursos del dispositivo para auto enviarse, a través del correo electrónico o programas P2P entre otros. Por lo que tienen la capacidad de propagarse sin la ayuda de una persona.

Los gusanos tienen diferentes vías de entrada a los equipos, como, por ejemplo:

- Utilización de una memoria USB previamente infectada.
- Descarga de contenidos mediante redes de compartición P2P u otras fuentes poco fiables.
- Apertura de algún fichero adjunto en un correo electrónico.
- Visitar una web maliciosa o pulsar sobre alguna dirección acortada que se publican en redes sociales u otros medidos y que en realidad no sabes a qué páginas web te puede llevar.

5.4 Troyanos

Un Troyano o también llamado Caballo de Troya es una clase de malware que normalmente se camufla como software legítimo. Los ciberladrones utilizan este software malicioso para acceder en tus equipos y una vez dentro campar a sus anchas (Kaspersky, 2021c).

Uno de los más peligrosos son los keylogger es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que realizas a través de tu teclado. Posteriormente son guardadas en un fichero y remitido a través de la red a los ciberdelincuentes.

Pudiendo llegar también como virus o gusanos, una vez activados, los troyanos pueden permitir a los cibercriminales espiarte, robar tus datos confidenciales y obtener acceso por una puerta trasera a tu sistema.

Los métodos más comunes de infección de un troyano suelen ser:

- La descarga de programas piratas o crackeados.
- Descarga de programas gratuitos desconocidos (juegos, salvapantallas y aplicaciones sencillas relacionadas con el entretenimiento).
- Abrir archivos adjuntos infectados.
- Abrir una imagen o cualquier otro tipo de archivo que sea en realidad un ejecutable con extensión modificada.
- Visitar sitios web trampa, es decir, sitios en los que para poder ver los vídeos sea necesario descargar un códec que en realidad es el troyano.
- Visitar una web maliciosa o pulsar sobre alguna dirección acortada que se publican en redes sociales u otros medidos y que en realidad no sabes a qué páginas web te puede llevar.
- Descarga de contenidos mediante redes de compartición P2P u otras fuentes poco fiables.

Algunos de los troyanos con más incidencias son el Dropper o los que usan archivos PDF para propagarse, pero recuerda que no son los únicos y que siempre están en constante evolución.

Existen herramientas que analizan y limpian los troyanos que se esconden en tu dispositivo y a su vez previene futuros ataques troyanos. Una de estas herramientas es el Trojan remover.

5.5 Ransomware o programa rescate

El Programa rescate o ransomware, está dentro del conjunto de software malicioso que también se conoce como malware y que impiden utilizar el

equipo mientras el usuario no pague una cierta cantidad de dinero. El virus bloquea o cifra la información o datos del equipo (Wikipedia, 2021j).

Para intimidar y engañar a las víctimas les hacen creer que han incurrido en algún tipo de actividad delictiva, como incitación al odio, terrorismo o pederastia, entre otros.

En la actualidad estos son unos de los ataques más virulentos. Según un estudio realizado por la compañía Panda Security en el 2019 este delitito tuvo un incremento con respecto al año 2018 del 500%. Y según un estudio del Observatorio del Sector Público de Inetum solo en 2018, el número de afectados por estos ataques fue de más de 1.000 millones en todo el planeta.

Figura 5.1: Ransomware (Malware).

Las diferentes vías de entrada de ransomware a tu equipo son:

- Utilización de una memoria USB previamente infectada.
- Descarga de contenidos mediante redes de compartición P2P, u otras fuentes poco fiables.
- Apertura de algún fichero adjunto en un correo electrónico.
- Visitar una web maliciosa o pulsar sobre alguna dirección acortada que se publican en redes sociales u otros medidos y que en realidad no sabes a qué páginas web te puede llevar.

En este punto cabe destacar que hay firmas de antivirus como AVG que pone a disposición del usuario una suite de herramientas gratuitas para

deshacer el cifrado del ransomware, de igual modo tienes a tu disposición los Descifradores de Ransomware Gratuitos de Kaspersky y la oficina de seguridad del internauta también pone a disposición otros recursos para combatir el ransomware en el siguiente artículo ¡No pagues ningún rescate si un ransomware ha cifrado tu información!.

Además, en el caso del sistema operativo de Windows 10 en su última versión dispone de una protección de forma nativa contra ransomware, aunque esto no te garantiza estar inmunizado.

Algunos de los ransomware más mediáticos son CryptoLocker, CryptoWall y WannaCry, pero no son los únicos, además de estar siempre en constante evolución y lo que es peor aún, éstos últimos irán dejando paso a otros mucho más nuevos y peligrosos.

5.6 Spyware o software espía

El spyware es otro tipo de malware que se mantiene oculto mientras recopila información en secreto, que después transmite a una entidad externa, sin el conocimiento o el consentimiento del propietario del dispositivo (Avast, 2020).

Puede supervisar y copiar todo lo que escribes, cargas, descargas y almacenas. Algunas cepas de spyware también son capaces de activar cámaras y micrófonos sin que te des cuenta.

Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet e incluso algunos muestran anuncios no deseados.

Sin embargo, a diferencia de los virus, no se intenta replicar en otros ordenadores, por lo que funciona como un parásito.

El spyware tiene diferentes vías de entrada a los equipos, muy parecidas a los virus y gusanos:

- Descarga de contenidos mediante redes de compartición P2P u otras fuentes poco fiables.
- Apertura de algún fichero adjunto en un correo electrónico.
- Visitar una web maliciosa o pulsar sobre alguna dirección acortada que se publican en redes sociales u otros medidos y que en realidad no sabes a qué páginas web te puede llevar.

5.7 Adware

El Adware también un tipo de software malicioso que te muestra publicidad constante y molesta, bien instalando otro programa o con ventanas emergentes (Avast, 2021).

Las vías de entrada a son las mismas prácticamente que cualquier otro tipo de malware:

- Descarga de contenidos mediante redes de compartición P2P u otras fuentes poco fiables.
- Apertura de algún fichero adjunto en un correo electrónico.
- Visitar una web maliciosa o pulsar sobre alguna dirección acortada que se publican en redes sociales u otros medidos y que en realidad no sabes a qué páginas web te puede llevar.

Aunque parte de toda la molesta publicidad que recibes es legítima, existe una plataforma que se llama Lista Robinson a la que puedes inscribirte e indicar cuales son las empresas publicitarias de las que no quieres recibir publicidad y por qué medios no quieres recibir dicha publicidad: teléfono, correo postal, correo electrónico o SMS/MMS. Además, se trata de un servicio gratuito.

Otro software muy útil contra la lucha de la publicidad no deseada es Ghostery que se encarga de bloquear anuncios, detener rastreadores y acelerar sitios web. Ghostery descubre los rastreadores que hay tras cada sitio web y te permite controlar lo que no deseas para que tu experiencia de navegación sea más limpia, rápida y segura.

También es importante saber que prácticamente todos los medios sociales, como Facebook, Instagram, Google y demás disponen en sus menús de configuración de opciones para gestionar la publicidad que llega a tus dispositivos.

5.8 Malvertising

Malvertising es el acrónimo de las palabras Malicious y Advertising, que en español sería Publicidad Maliciosa. Esta amenaza lo que hace es esconder malware para infectar los dispositivos en los espacios de publicidad de otras páginas webs, como son los banners de publicidad en las cabeceras o laterales tanto izquierdos como derecho de muchas de la web que a diario te encuentras en internet.

La diferencia principal con el adware es que este primero necesita que el malware se instale en el dispositivo y en el caso del malvertising no es

necesaria ninguna instalación por parte del usuario para resultar infectado (OSI, 2015).

La vía de contagio por la que podemos caer víctimas de este ciberdelito, es como habrás podido ver, haciendo click en los anuncios en páginas webs.

5.9 Scareware o rogueware

Esta variante de malware conocido como Scareware o Rogueware es otro software malicioso más que trata de engañar a los usuarios para que visiten sitios infestados de malware. Normalmente suele darse en forma de ventanas emergentes, que además, aparecen como advertencias legítimas de compañías de software en su mayoría de antivirus y que afirman que el sistema operativo ha sido vulnerado o que los archivos del PC han sido infectado (Kaspersky, 2021b).

Las vías de contagio son las mismas que has visto en malwares anteriores:

- Descarga de contenidos mediante redes de compartición P2P u otras fuentes poco fiables.
- Apertura de algún fichero adjunto en un correo electrónico.
- Visitar una web maliciosa o pulsar sobre alguna dirección acortada que se publican en redes sociales u otros medidos y que en realidad no sabes a qué páginas web te puede llevar.

5.10 Quishing

Los Quick Response (QR) son códigos de barra de dos dimensiones diseñados para ser leídos e interpretados rápidamente. Actualmente y sumado a la gran proliferación de smartphones en el mercado, son muy utilizados en publicidad y campañas de marketing. Esto es debido a su gran facilidad de manejo, ya que solo basta con apuntar con la cámara y el smartphone se encarga del resto.

Lamentablemente los códigos QR también pueden ser utilizados con fines maliciosos, de manera que, un ciberdelicuente podría usar el código QR para direccionar a los usuarios a páginas web phishing, descarga de malware o cualquier otra amenaza (ESET, 2012). Esta amenaza además de ser conocida como Quishing, también se le conoce como Malware QR.

La vía de contagio como te habrás podido dar cuenta queda implícita.

5.11 Phishing

El término Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima (Infospyware, 2021).

El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en lo que se conoce como suplantación de identidad o spoofing (término que verás más adelante en esta misma unidad) a través de una aparente comunicación oficial, por lo general un correo electrónico, redes sociales, SMS, etc., a raíz de un malware o incluso utilizando también llamadas telefónicas.

Según el propio INCIBE, El phishing es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico.

También existe una modalidad de phishing más específica llamada Spear phishing.Los ataques de Spear phishing (literalmente “pesca con arpón”), al igual que los de phishing en general, son estafas en las que se intenta engañar al destinatario para que revele al atacante información confidencial, tales como credenciales de sus cuentas. También se pueden utilizar vínculos y archivos adjuntos para que el destinatario descargue de forma involuntaria malware que puede darle al atacante acceso al ordenador del usuario y a otra información delicada. El spear phishing se diferencia del phishing más genérico en que es de naturaleza dirigida a un objetivo determinado.

Por lo general, los mensajes de spear phishing se personalizan según la información pública que el atacante haya encontrado acerca del destinatario. Eso puede incluir desde temas relacionados con el campo de especialización, la función en la organización, los intereses, la información residencial pública y también fiscal del destinatario, así como toda información que los atacantes recopilen en las redes sociales. Esos detalles específicos logran que el mensaje parezca ser más legítimo y aumentan la probabilidad de que el destinatario haga clic en algún vínculo o que descargue los archivos adjuntos.(Proofpoint, 2022)

Los medios de phishing más usados por lo ciberdelincuentes:

- Correos electrónicos de carácter corporativo.
- Mensajería instantánea.

- Redes sociales.
- Webs corporativas (Bancos, pasarelas de pago, tiendas online, etc.)
- SMS.

Para poder detectar si estas siendo víctima de uno de estos fraudes debes estar atento a lo siguiente:

- La dirección web o URL: Fíjate muy bien en la URL a la que te remite el enlace que te envían. Insistir en que hay que fijarse muy bien porque en algunas ocasiones las diferencias son inapreciables y se centran incluso en caracteres que se copian o se alteran (una l minúscula por una i mayúscula; un punto situado en un lugar poco visible y otras estrategias).
- Ortografía: Forma en la que está redactado el mensaje. Los ciberatacantes en algunos casos no tienen tu misma nacionalidad ni hablan tu misma lengua y, en muchas ocasiones traducen los textos automáticamente y contienen faltas de ortografía, errores gramaticales o un tratamiento o forma de dirigirse a ti que ninguna comunicación oficial de tu banco, organismos o empresas contendría.
- Cuidado con el remitente: Correo electrónico de tu banco, de la Agencia Tributaria, de Amazon u otra empresa. Lo primero que debes mirar es el remitente y comprobar que esa dirección es la que está vinculada a esos servicios. De la misma manera, si el correo te ha llegado a la carpeta de spam ya es un signo inequívoco de que el remitente es sospechoso. Lee la siguiente entrada pare saber donde buscar el remitente Cómo saber quién te envía un correo electrónico para comprobar que es quien dice ser. Esta parte es muy importante para saber si se trata de un phishing.
- Cuidado con lo que solicitan:¿Qué te piden en el correo? Ten muy presente que los bancos y las empresas u organismos no reclaman jamás que introduzcas tus datos personales o que los reingreses en una web para reactivar tu cuenta. No lo reclaman jamás.
- Desconfía de los cupones promocionales y las encuestas: Esta modalidad de phishing ha sido una de las que más éxito ha tenido en los últimos años y ha afectado a todas las grandes marcas. Existen ejemplos de phishing a Mercadona, Ikea, a El Corte Inglés, a Zara, a Lidl… Y todo a través de cupones promocionales en los que te prometen una compra o un vale descuento a cambio de que accedas a un enlace y rellenes tus datos personales.
- Descarga archivos adjuntos: Salvo que hayas comprobado todos los pasos anteriores y estés completamente seguro de la identidad del remitente,

así como del objeto del mensaje, no descargues documentos adjuntos sin antes pasarlos por un buen antivirus.

- Usa el sentido común y desconfía siempre: Este consejo es válido para detectar el phishing o cualquier otra amenaza en Internet. ¿Quién va a regalar gafas Ray-Ban o a venderlas un 75% por debajo de su precio?.

Figura 5.2: Phishing banco Santander.

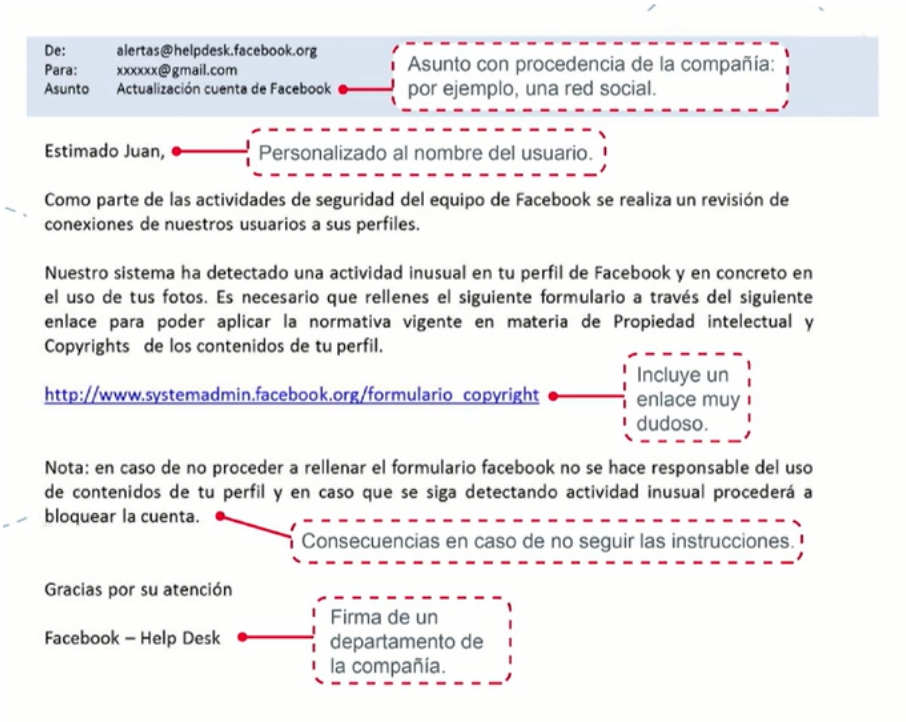

Figura 5.3: Spear phishing Facebook.

En relación a la protección contra el phishing existen diferentes herramientas y servicios que puedes implementar en tu uso diario de las tecnologías. Algunos de estos son:

- Software anti-phishing: Software específico para la detección de phishing.

  - Sophos home.
  - Phishing protection

- Proveedores de email: Estos ofrecen protección contra el phishing a través de filtros y configuraciones con el objetivo detectar y frenar este tipo de fraude llevado a cabo por medio del correo electrónico. Para ello analizan de forma automatizada todos los emails, con el fin detectar links fraudulentos o dominios falsificados que tienen la intención de robar tus datos, protegiendo así a los usuarios de estos tipos de fraudes o estafas online. Esta protección puedes encontrarla prácticamente implementada en la mayoría de gestores de correos actuales.
- Nativo del sistema operativo Windows: Anti-phishing defender.
- Antivirus: Algunos antivirus traen implementado estándares contra el phishing como el ESET anti-phising.
- Plugins: Extensiones para el navegador como lo son ZoneAlarm Web Secure Free y Metacertprotocol.
- Código anti-phishing: Existen plataformas webs que ofrecen este servicio. Consiste en un código o palabra clave que tú facilitas la primera vez a la web y que esta incluye en sus futuros email, verificando así la legitimidad del mismo. Un ejemplo de ello lo encontrarás en la plataforma de intercambio de criptomonedas Binance código anti-phishing.
- Navegadores:
  - Firefox es uno de los navegadores que implementan grandes capas de seguridad siendo una de ellas la protección anti-phishing y que además, cuenta con Mozilla support y Cómo protegerse del Phishing y del Malware con esta herramienta de Firefox.
  - Google Chrome a su vez cuenta con los recursos ofrecidos por Google safe browsing.

Si quieres saber más sobre los diferentes formatos de phishing, visita el siguiente enlace de la plataforma INCIBE, Principales formas de estafa a través del email: phishing más comunes. Y además, si también quieres ver otros ejemplos de phishing de bancos como CaixaBank, Santander o BBVA, pásate por la siguiente publicación titulada Detectadas campañas de phishing y smishing suplantando a diversas entidades bancarias de la Oficina de Seguridad del Internauta, donde te encontrarás capturas de pantallas, detalles y soluciones que te ayudarán a salir airoso de este peligroso ciberdelito.

Otra técnica muy parecida al Phishing e igualmente peligrosa es el Pharming y que consiste en la explotación de una vulnerabilidad en el software de los

servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio (Kaspersky, 2021a).

También existe otra amenaza silimiar estas, conocida como Typosquatting, URL hijacking o fake URL. Está basada en los errores tipográficos cometidos por usuarios de internet cuando introducen la dirección de un sitio web en un navegador. Cuando esto sucede la dirección puede llevarlos a un sitio alternativo propiedad de un cybersquatter (Wikipedia, 2021m).

- Ejemplo: https://wikiepdia.org

Una técnica más reciente de phishing es el "Browser-in-the-browser" en la cual un ciberdelincuente o phisher simula una página de un servicio online para así introducir en esta una ventana emergente de inicio de sesión única, haciendo que el usuario crea que es una ventana de inicio de sesión legítima, como las que ya estamos acostumbrados a ver en muchas webs legítimas, e introduzca así sus credenciales. Más información en el siguiente enlace Browser-in-the-Browser: una nueva técnica de phishing casi indetectable.

Otros tipos de fraudes que pueden llegar a través de técnicas de phishing o smishing son las conocidas como el fraude de las suscripciones a servicios premium o de tarificación especial. Este fraude consiste en conseguir que los usuarios faciliten el número de teléfono o contesten a algún mensaje para que, sin dar consentimiento explícito o ser conscientes de ello, nos suscriban a servicios de tarificación especial. Puedes leerlo en el siguiente artículo ¿Suscripciones premium por SMS? No, gracias. El otro tipo es el ciberataque "Pass-the-Cookie" que consiste el robo de cookies de sesión con el que luego pueden acceder al servicio al que pertenece la cookie, puedes saber más en la siguiente entrada Así es el nuevo ciberataque 'Pass-the-Cookie': qué es y cómo evitarlo

Para que puedas hacerte una idea de la magnitud de esta técnica de ingeniería social, en la siguiente entrada del blog oficial de Google llamado Cocreación para una web más segura: Google y Euroconsumers lanzan Space Shelter en vísperas del Mes Europeo de la Ciberseguridad, podrás encontrar que con sus algoritmos de detección Google bloquea más de 100 millones diarios de intentos de phishing.

5.12 Vishing

El Vishing es una estafa que consiste en una llamada de teléfono en la que ciberdelicuente suplanta la identidad de una persona, empresa o institución

para conseguir que le proporciones información privada y sensible. Esta información normalmente va a ser datos personales, contraseñas o peor aún los datos bancarios. Se trata de técnicas de ingeniería social con la que el estafador se va ganando la confianza de la víctima de manera que ésta termina proporcionándole cualquier tipo de datos. Si quieres saber más sobre ingeniería social visita este enlace ¿Sabías que los ataques de ingeniería social suponen el 93% de las brechas de seguridad?.

En esta línea puedes encontrarte con lo que se conoce como pretexting o pretexto. Se trata en un ataque más de ingeniería social y que consiste en elaborar un escenario o historia ficticia, donde el atacante tratará que la víctima comparta información que, en circunstancias normales, no revelaría. Habrás podido notar que a su vez también es la base del Phishing y del Smishing, que verás más adelante (Redeszone, 2021).

En el siguiente enlace La Guardia Civil actúa por un nuevo caso de 'spoofing', la estafa telefónica en auge te encontrarás que aun cuando el estafador te pide que introduzcas la contraseña por pulsación de teclado, como cuando hablas con un operador de telefonía y te dicen para información marca 1, para contratar marca 2, para hablar con un gestor marca 3..., es otra forma más de obtener tu contraseña.

Por lo tanto, debes tener muy en cuenta, que cualquier petición de tus contraseñas o información financiera es una estafa, ya que las instituciones legítimas nunca te pedirían este tipo de datos tan sensibles a través del teléfono.

La vía de contagio como se ha señalado al principio es a través de una llamada de teléfono.

5.13 Smishing

El Smishing es un acrónimo formado por las palabras SMS y phishing, debido a su parecido con este ataque tan popular. La diferencia entre el Smishing y el Phishing, es que mientras este último lleva a cabo la estafa utilizando el correo electrónico como medio, en el Smishing se utilizan mensajes de texto enviados a través de SMS al smartphone o a través de las distintas aplicaciones de mensajería instantánea. Al igual que el phishing y el vishing, también se trata de una técnica de ingeniería social.

El modus operandi sigue siendo muy similar a otros ataques donde el ciberdelincuente suplanta la identidad de alguna persona o entidad de confianza de la víctima, con el objetivo de engañarla y conseguir que comparta información personal, realice un pago, haga clic en un enlace malicioso o se descargue un archivo adjunto entre otras.

El mayor riesgo de este tipo de ciberataque es el desconocimiento de los usuarios, ya que no esperan ser engañados a través de un mensaje de texto (INCIBE, 2021b).

Si quieres más información visita el siguiente enlace Campañas de smishing suplantando a múltiples entidades bancarias.

Como se ha destacado en líneas anteriores la vía de entrada de esta amenaza a través de SMS.

Figura 5.4: BBVA smishing.

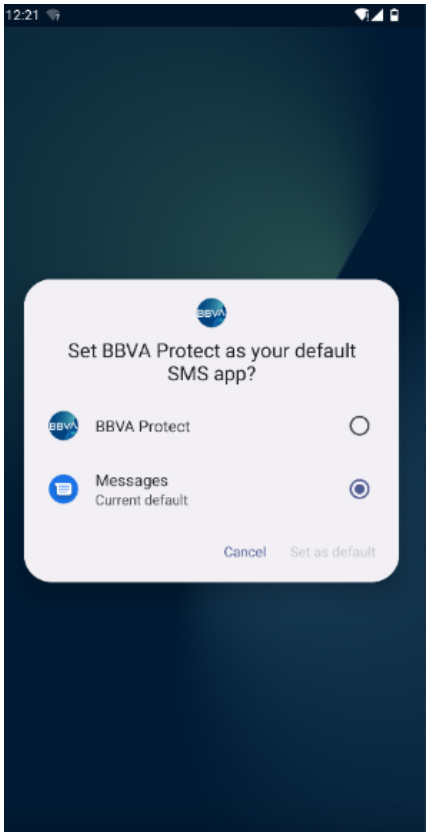

Figura 5.5: Reemplazo app de mensajería.

5.14 Spam o correo malicioso

Los términos spam o correo malicioso hacen referencia a los mensajes no solicitados, no deseados o con remitente no conocido (correo anónimo),

habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor (Wikipedia, 2021l).

Su finalidad suele ser con motivos comerciales, pero también pueden contener enlaces peligros como el Phishing, solicitar datos sensibles o contener descargas que sean un riesgo para tu privacidad y seguridad:

- E-Mails Spam con fines comerciales
- Envíos masivos / Avisos de virus
- E-Mails con ofertas o regalos
- Correos Phishing

Si recibes un email de carácter sospechoso, no lo abras y márcalo directamente como spam, para que así tu gestor de correos lo identifique para los sucesivos.

En este caso no hace falta destacar que este molesto malware llega por medio de gestores de correos.

En torno a este concepto también aparece el SPIM (SPam over Instant Messaging), en castellano viniendo a ser como spam a través de mensajería instantánea, puedes leer más en el siguiente artículo Hablemos de ciberseguridad – III – Spam, SPIM y SPIT.

5.15 Toolbars

Las Toolbars son barras de herramientas que aparecen en la parte superior de los navegadores. Generalmente sirven para tener enlaces más rápidos a servicios, por ejemplo, Windows Live Toolbars da acceso al correo y búsqueda entre otras funcionalidades. Regularmente los navegadores tienen las suyas propias.

Pero puede ocurrir que, a través de una instalación de software, normalmente gratuito puedan ser instaladas. Debes tener en cuenta que algunas de estas son muy molestas y en algunos casos pueden llegar a bombardearte con publicidad no deseada y que además en ocasiones llegan a ser muy difíciles de eliminar. Aunque cada vez son menos frecuentes.

Normalmente, se instalan como un añadido al instalar aplicaciones gratuitas en el ordenador. Si no tienes cuidado durante el proceso de instalación y pulsamos siempre “Siguiente-Siguiente-Siguiente” las toolbars acaban en tu navegador. Para evitarlo no debes instalar una aplicación dando a “Siguiente-Siguiente-Siguiente” sin leer lo que nos están indicando. Para evitar este

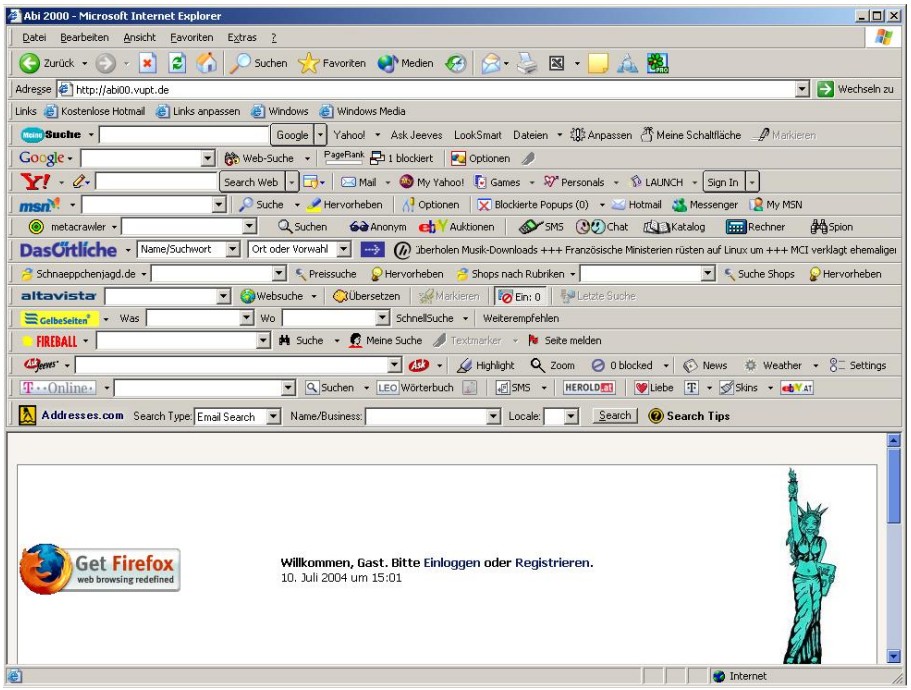

Figura 5.6: Toolbar.

supuesto, recuerda que lo mejor es descargar programas solo de las webs oficiales.

En el caso de haber instalado alguna toolbars por descuido existen algunas herramientas para desinstalarlas fácilmente, entre ellas esta Malwarebytes.

Como se ha señalada más arriba la vía de contagio suele ser la instalación de software normalmente gratuito.

5.16 Usurpación o robo de identidad

El robo de identidad, usurpación de identidad es la apropiación de la identidad de una persona: hacerse pasar por esa persona, asumir su identidad ante otras personas en público o en privado, en general para acceder a ciertos recursos o la obtención de créditos y otros beneficios en nombre de esa persona. Esto que sucede en el mundo analógico también ocurre en el mundo digital (Wikipedia, 2021n).

La manera que tienen los ciberdelincuentes de usurpar la identidad suele ser a través de los siguientes:

- Robo masivo de cuentas de email por medio de métodos de hacking.
- Por medio de Phishing, Smishing o Vishing.
- Dejando tú cuenta abierta en sitios públicos.
- Usando Wi-Fi de terceros creadas para ese fin.

- Software espía o troyanos.

La usurpación de identidad permite a los delincuentes hacerse con información personal de sus víctimas, para luego con ella interceptar aún más datos de otros perfiles, a quienes engañan con el fin de extorsionar u obtener lucro económico e incluso a veces realizar actividades delictivas. En caso de ser víctima de esta amenaza debes tener en cuenta lo siguiente:

- Guarda los mensajes de texto e emails que recibas.
- Haz capturas de pantalla.
- Revisa todas tus redes sociales.
- Avisa a tus contactos sobre el perfil falso.
- Infórmalo dentro de la aplicación. Todas las plataformas y redes sociales disponen de un apartado de Suplantación de identidad en las cuentas.
- Si es de carácter grave denúncialo a las autoridades.
- Si es posible cancela cuenta.

En la Oficina de seguridad del internauta tienes una publicación que se llama ¡Me han secuestrado mi cuenta! de una historia real donde puedes ver cómo gestionar este tipo de ataques.

Algunas de las formas en que lo ciberdelicuentes se hacen con nuestras cuentas:

- Cómo evitar ser víctima del fraude del sí y la suscripción a servicios premium
- Robo de cuenta de Whatsapp

5.17 Suplantación de identidad o Spoofing

Normalmente cuando un ciberdelincuente usurpa o roba una cuenta, ya sea particular o corporativa, la principal intención es hacer uso del spoofing o también conocido como suplantación de identidad. Estos términos pueden confundirse con el Phishing, pero no son lo mismo. Podría decirse que el Phishing es el término o palabra que se utiliza para describir la manera con la que los estafadores se hacen con tus datos y el spoofing son las herramientas, procedimientos o técnicas con los que lo lleva a cabo. Ejemplo: Un ciberestafador suplanta la web o el correo que recibes de tu entidad bancaria para que facilites tus datos, esta es la herramienta o herramientas y el término o nombre que recibe este acto es el Phishing. No obstante, en el

siguiente enlace puedes obtener más información sobre las diferencias entre Phishing y Spoofing.

La suplantación de identidad no solo se lleva a cabo después de haberte robado o usurpado tu identidad, sino que también, puede llevarse a cabo cuando un tercero crea un perfil falso desde cero con tus datos y tus fotografías para que la gente piense que de verdad se trata legítimamente de ti.

A tener en cuenta también el hecho, que el uso de una acreditación física que no pertenece a su legítimo dueño, también está considerado una estafa. Un claro ejemplo es el uso que hace un tercero de una tarjeta de identificación robada, para obtener el acceso a un determinado departamento físico de una compañía o empresa. Esto es lo que se conoce como Masquerating o suplantación de identidad física.

Existe otra suplantación de identidad llamada email spoofing y que resulta de recibir un correo electrónico al parecer enviado por una dirección de correo conocida, ya sea de un familiar, amigo, conocido, compañero de trabajo, etc. Tienes toda la información en el siguiente enlace del Incibe Email spoofing: cuando el correo parece haber sido enviado por mí o alguien conocido.

Otra actividad relacionada con la usurpación de identidad es el Brushing. Este delito es el que realizan algunos vendedores de Internet, que envían paquetes con objetos muy pequeños a diferentes usuarios para hacerse pasar por ellos y después poder valorar sus propios productos. Aunque en cierto modo esto no te pone en un serio riesgo, conviene conocerlo por si te sucede saber que se trata de una suplantación de la identidad y que es aconsejable interponer una denuncia (Computer Hoy, 2021).

5.18 Ciberestafas en compras online y otros engaños

Llegados hasta aquí, recordarte que todas las precauciones que se detallan en este manual en el apartado de Compras y transacciones de la unidad de Gestión de la seguridad en la red, son altamente recomendables en este punto. Además de ser fuertemente aconsejable seguir todas esas indicaciones, también se trata de tener en cuenta el conjunto de requisitos que veras a continuación, ya que cada uno de ellos por independiente te va a garantizar una capa más de seguridad y te irán indicando si puede o no puede ser una estafa.

Según una publicación de Newtral (plataforma web de periodismo digital) las estafas por internet representan más del 80% de los ciberdelitos. Más concretamente la fuente es arrojada por el Sistema Estadístico de Criminalidad (SEC), gestionado desde el Ministerio del Interior, y que

declara que el total de ciberdelitos denunciados en 2019 un 88% corresponden a fraudes online. Léela pinchando en el enlace.

Decálogo de requisitos a comprobar a la hora de comprar en una tienda online:

- Formato seguro de URL: Https con su correspondiente candado. Aunque como has podido ver en el apartado de Protocolo https, los ciberdelincuentes también tienen acceso a este protocolo, por lo que no es seguro al 100%.
- El diseño de la tienda: Aunque muchas de las tiendas fraudulentas están muy bien confeccionadas, si tienes la más mínima sospecha no corras riesgos. Además, fíjate si tienes imágenes de mala calidad, mal enfocadas, textos incongruentes o faltas de ortografía.
- El precio que suele ser muy por debajo o simplemente con un descuento muy suculento.
- Opiniones de usuarios: Por supuesto no buscarla dentro la propia web, ya que serán del todo falsas.
- Tipos de pagos permitidos: A pesar de contar en principio con un amplio abanico de opciones de pago, Paypal, transferencia bancaria, contra reembolso, pero curiosamente solo funciona el pago con tarjeta.
- Conocer la empresa detrás de esa web, su información legal, ubicación, política de envío y de devolución, etc.
- Certificado de seguridad: Certifica que no ha sido vulnerada ni hackeada.
- Sello de confianza y autenticidad: Verifican que se trata de una web legítima y confiable.

Además, puedes visitar la siguiente entrada donde aprenderás cómo detectar fraudes y análisis de una web falsa.

Las estafas online no solo te las vas a encontrar en la compra de productos o servicios, sino que también en diferentes escenarios como los que verás a continuación. Pudiendo encontrarlos a través de correos electrónicos, webs de venta de segunda mano, en webs maliciosas, etc.

Algunos ejemplos de estafas son:

- Timo Nigeriano: Lotería, viuda, enfermo terminal, herencias, etc (Wikipedia, 2023).
- Falsas ofertas de empleo: Ofertas de empleo bajo pago previo en concepto de gastos de gestión o materiales de estudio. O llamadas a teléfonos de tarificación especial que comienzan por un 803 u 806 (INCIBE, 2023b).

- Falsos prestamistas de dinero: Que después de pagar los costes luego no recibes (INCIBE, 2023d).
- Falsas ofertas de alquiler de pisos: Que te hacen pagar la fianza y luego desaparecen (INCIBE, 2023c).
- Novias o novios de orígenes exóticos: Embaucan para posteriormente pedir dinero (INCIBE, 2018b) o el también conocido Catfishing: la estafa del amor.
- Falsos correos de sextorsión: Simulan que tienen fotos o vídeos comprometidos, cuando no es así (INCIBE, 2021a).
- Propuesta de compra del producto que tienes en venta: Solicitando que hagas el pago del envío por adelantado.
- Pedir que hagas el pago o contactar contigo fuera de la plataforma de venta.
- Sorteos ganados bajo cualquier pretexto: Eres el visitante número 1.000 por ello te has ganado un premio (INCIBE, 2020)].
- Tu hijo tiene un accidente y te pide pagar por Bizum la grua (INCIBE, 2023a).
- Un familiar o amigo que está en el extranjero y necesita dinero para pagar los costes de aduana de sus maletas retenidas en el extranjero (INCIBE, 2022).
- Un hijo que ha cambiado el número por haber tenido algún percance con el anterior y necesita dinero bajo cualquier excusa.
- Un número desconocido que afirma equivocación al haber contactado o pregunta por otra persona e intenta entablar conversación para, generalmente, inducir a invertir en criptomonedas.
- Un familiar o amigo que se encuentra en algún apuro y solicita ayuda.
- Solicitud de dinero por Bizum enmascarada como pago de un producto que estás vendiendo. Al finalizar la operación se está haciendo un pago en lugar de un cobro. Léelo aquí Estafa Bizum.
- Pago pendiente de tasas de matrícula de la universidad. Léelo aquí Estafa matrícula
- Otras muchas y nuevas que van ingeniando.

Las vías de entrada de las ciberestafas suelen llegar por medio:

- Correos electrónicos o mensajería instantánea.
- Plataformas de venta de segunda mano.

- Web de venta fraudulentas.
- Redes sociales.

En esta Guía de fraudes online tienes un amplio catálogo de recursos para detectar si estas siendo víctima de una estafa o fraude online.

Por último, pero no por ello menos importante, si en algún momento te encontrases ante una posible estafa debes reportarlo a través desde este enlace para reportar webs fraudulentas en el Incibe.

5.19 Warshipping

El warshipping es un tipo de ataque que los ciberdelicuentes llevan a cabo mediante el envío de paquetería, y en cuyo interior se encuentra un dispositivo electrónico, pudiendo ser de diferente naturaleza. Estos pueden contener cámara, micrófono o simplemente ser un dispositivo, que al ser conectado instale un software fraudulento de manera que permita a los ciberdelicuentes remotamente vulnerar la privacidad y la seguridad de la víctima. Aun que suele estar destinados a empresas que continuamente reciben paquetería, usuarios de compras online también pueden ser blanco de este ciberdelito (INCIBE, 2021c).

5.20 Vulnerabilidades

Una vulnerabilidad en términos de informática es una debilidad o fallo en un sistema de información, que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma. Estas vulnerabilidades pueden tener distintos orígenes como por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos (INCIBE, 2017).

Los fallos de vulnerabilidad les corresponde corregirlos a las terceras partes implicadas, lo a veces con lleva la dificultad de que escapan a nuestro control. Pero para protegernos de tales, debes tener actualizados todos tus sistemas y software.

Un ejemplo de vulnerabilidad muy conocido fuero el Meltdown y Spectre, relacionadas con los procesadores informáticos, que existen desde mediados de los noventa, pero que han sido descubiertas ahora.

Las vulnerabilidades son también una puerta de entrada para lo que se conocen como ataques de click cero. Un pirateo de clic cero explota los fallos de tu dispositivo y utiliza una deficiencia en la verificación de datos para acceder a tu sistema. Y no necesita la intervención de la propia víctima.

También pueden ser explotadas por lo que se conoce como "exploit". Un exploit es un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico.

Amplía la información en el artículo del centro de recursos de los servicios de antivirus Kaspersky ¿Qué es el malware de clic cero y cómo funcionan los ataques de clic cero?.

5.21 Cryptojacking

El cryptojacking, también llamado minería de criptomonedas malicioso, consiste en un tipo de software fraudulento que se oculta en un ordenador o en un dispositivo móvil, y utiliza los recursos de estos para extraer diversas formas de monedas digitales conocidas como criptomonedas. Hay que aclarar que no está tan focalizado en el robo directo de estas, sino, que se centra en el robo o secuestro de dispositivos de terceros con el fin de utilizarlos para minar estas criptomonedas, y a los que se le conocen también como dispositivos zombies (Innovation and Entrepreneurship Business School, 2021).

Se trata de una amenaza reciente que se hace con el control del navegador web, y de este modo, comprometen todo tipo de dispositivos, desde ordenadores de escritorio y portátiles hasta teléfonos inteligentes e incluso servidores de red.

Existen recursos y herramientas para saber si estamos siendo víctimas de cryptojacking (Genbeta, 2018):

- Te puede pasar que el ordenador se recaliente, que empiecen a sonar los ventiladores de pronto y se mantengan encendidos por más tiempo de lo que consideras normal.
- El sistema operativo se pondrá lento, incluso se puede llegar a colgar el navegador o todo el sistema constantemente.
- Comprueba el administrador de tareas en Windows, o el Monitor de actividad en MacOS. Fíjate en los procesos que estén ocupando el mayor porcentaje de CPU. En circunstancias normales un solo proceso no debe pasar de 10%, rara vez sobrepasan el 20% al menos que se trate de software muy complejo como el de edición de vídeo, juegos, o el mismo sistema actualizando. Pero que te aparezca el navegador en números absurdos como 70-90 y hasta 100% es una alarma clara.

Las vías de contagios son las mismas que la mayoría de malware tales como los virus, gusanos, troyanos, spyware y demás. Por lo que puedes

verlo en dichos apartados de esta misma unidad. Además, existen webs y plugin que comprueban si estas siendo víctima de este ciberdelito e incluso alguna de estas herramientas previenen y bloquean estos ataques. A continuación, tienes una lista para que puedas elegir la que mejor se adapte a tus necesidades:

- CoinEater
- Minerblock
- Not mining
- NoCoin
- NoMiner
- Adblock nocoin list

Señalar que Microsoft Defender, que como ya sabréis es el antivirus que Windows trae por defecto ya incluye protección contra el cryptojacking, aunque de momento solo está presente en la versión empresarial, es de suponer que con el paso del tiempo lo terminen incluyendo en las versiones de Windows Home.

Por otro lado, ya son algunos navegadores los que implementan herramientas nativas para paliar el cryptocjacking como es el caso del navegador Firefox. Puedes obtener más información en este enlace Firefox añadirá protección contra el minado de criptomonedas y el fingerprinting.

5.22 Plugins maliciosos

En primer lugar, es importante tener claro qué es un plugin. Así pues, se trata de un software o aplicación que actúa como complemento para ampliar las funcionalidades del programa principal al que complementa. Dicho esto, algunos ciberdelicuentes usan esta funcionalidad para sus actividades delictivas, como espiar o recopilar datos sensibles e incluso el robo de criptomonedas. (IONOS by 1and1, 2020b).

Instalar un plugin suele ser una acción muy sencilla, y te puede servir para finalidades muy diversas, un claro ejemplo ello, es el plugin de Google drive o Adblock para el bloqueo de publicidad, etc. Es por esto que debes tener siempre algunas consideraciones, como verás a continuación.

Sin embargo, a pesar de ser programas muy útiles que la inmensa mayoría utiliza, no todos son conscientes del riesgo que conlleva el simple hecho de instalar un plugin. El problema suele venir por no tener actualizado un buen sistema de seguridad.

A veces, el simple hecho de que el plugin esté disponible no significa garantía ninguna. Tanto es así que aquí podemos ver uno de los que recientemente ha sido retirado de WordPress hasta en cuatro ocasiones. Un programa capaz de recopilar datos de los navegantes con el correspondiente riesgo a nivel de Reglamento General de Protección de Datos que esto conlleva, así como de publicar entradas no deseadas y prácticas de spam. De otro lado, Google está continuamente retirando plugins maliciosos de su plataforma.

El contagio de estos plugins maliciosos normalmente es a través de las Webs Store de las diferentes plataformas. Por lo que los puntos más importantes a tener en cuenta a la hora de protegernos son:

- Infórmate del desarrollo del plugin así como posibles variaciones.
- No descargues plugins sospechosos.
- Utiliza preferiblemente aquellos plugins de referencia, con fama y garantía reconocidas.

5.23 SIM Swapping

El SIM Swapping, es la técnica que usan últimamente los ladrones digitales que se basa en duplicar la tarjeta SIM del móvil de sus víctimas. Así, pueden acceder a toda su información personal y, sobre todo, pueden usarlas en la verificación a través de un SMS por medio del móvil que suelen pedir los bancos cuando se opera a través de Internet y algunas otras plataformas online.

Por ello, aunque la mayoría de las apps de los bancos son muy seguras, con protocolos complejos para las claves de acceso, cifrado de las comunicaciones y teclados virtuales, los timadores digitales son capaces de saltarse la seguridad por medio de una técnica llamada ingeniería social, que consiste en el engaño a través de técnicas de persuasión y manipulación psicológica. Sin embargo, en lugar de timar directamente a las víctimas, el SIM swapping se consigue por medio de un engaño a los dependientes de las tiendas de telefonía.

Por lo tanto, una vez que el ciberdelicuente se hace con tus credenciales del tipo que sea, tales como contraseñas bancarias o de perfiles sociales, como Facebook, Instagram, etc. o cualquier otra credencial privada, no va a tener problemas para obtener el SMS de verificación.

Cabe destacar que cuando se es víctima de este asalto digital, al obtener la duplicación de la SIM por parte del atacante, tu tarjeta queda sin uso, por lo tanto pierdes la cobertura de llamadas y la conexión de internet (Panda Security, 2021b).

Por lo tanto, es importante que sigas estas recomendaciones para no ser víctimas del SIM Swapping:

- Utiliza una contraseña adicional o doble autentificación: reconocimiento facial, por voz, PIN adicional, Google authenticator, etc.
- No compartas demasiada información en Internet. Cuantos más datos haya sobre ti en la web, más fácil será para los malos chantajearte, timarte o conseguir otras cosas tuyas, como contraseñas, cuentas bancarias, etc.
- No almacenes todo en tu móvil, no es una caja fuerte. Es un dispositivo electrónico que no es 100% seguro.
- Exige a tu operador móvil que refuerce sus sistemas de seguridad cuando se trate de operaciones en tu nombre.
- Los mensajes a través de aplicaciones de mensajería tipo WhatsApp, Telegram, Line, etc. son más seguros que los SMS, ya que están encriptados y éstos últimos no, haciéndolos más susceptibles.
- No vincules tus cuentas bancarias a tu cuenta o teléfono.
- No le des nunca a nadie tu código PIN. ¡Nunca!.
- Instala un antivirus o solución de seguridad para evitar que puedan robar o acceder a tus datos personales.

Desde el Instituto nacional de Ciberseguridad y a través de este video podrás obtener más información sobre que es el SIM Swaping.

5.24 Shoulder surfing o visual hackins

El shoulder surfing o también conocido como visual hackins es una técnica en apariencia muy sencilla empleada por los ciberatacantes con el objetivo de conseguir información de un usuario en concreto. Esta técnica consiste en mirar literalmente por encima del hombro y que suele llevarse a cabo mientras viajamos en metro, en autobús o en cualquier sitio público donde los cibervándalos puedan estar atento al uso que haces de tu dispositivo sin que puedas percatarte de ello (OSI, 2020d).

Como has podido leer, evitar el uso de datos sensibles en espacios públicos es la mejor fórmula para evitar caer en este tipo de amenazas.

5.25 Ciberacoso

El ciberacoso es una forma de acoso o intimidación por medio de las tecnologías digitales. Su modus operandi se realiza en las redes sociales, las plataformas de mensajería, las plataformas de juegos, smartphones y cualquier otro dispositivo, plataforma o medio que disponga de conexión a internet. Es un comportamiento que se repite y que busca atemorizar, enfadar, humillar o maltratar a otras personas.

Ejemplos de ciberacoso son:

- Difundir mentiras o publicar fotografías vergonzosas de alguien en las redes sociales.
- Enviar mensajes hirientes o amenazas a través de las plataformas de mensajería.
- Hacerse pasar por otra persona y enviar mensajes agresivos en nombre de dicha persona.

El acoso cara a cara y el ciberacoso ocurren juntos a menudo. Pero el ciberacoso deja una huella digital, lo cual quiere decir, que queda un registro que puede servir de prueba para ayudar a detener el abuso (Unicef, 2021).

5.26 Ciberextorsión

La ciberextorsión es una forma de chantaje que sufre la víctima a través de los medios digitales, mediante el cual se le fuerza u obliga a pagar o a realizar algún acto o actividad delictiva o no lícita, para evitar los términos del chantaje. Un caso muy común es el del malware Ransomware que te obliga a pagar una cantidad de dinero si quieres recuperar tus archivos.

La plataforma de antivirus Panda Security pone a tu disposición una Guía de ciberextorsión para que puedas documentarte con más amplitud.

Dentro de la ciberextorsión se encuentra lo que se conoce como sextorsión. Este ciberdelito es también una forma de extorsión en el plano digital, pero en este caso con contenido sexual. En la sextorsión la víctima es amenazada con la supuesta publicación y difusión de contenido sexual.

5.27 Sextorsión

La sextorsión, o extorsión sexual, consiste en la amenaza de revelar información íntima sobre una víctima a no ser que esta pague al extorsionista. En esta era digital conectada, dicha información podría incluir mensajes

de texto sexuales (en inglés conocidos como sexts), fotos íntimas e, incluso, vídeos. Los delincuentes suelen pedir dinero, pero a veces buscan material más comprometedor (envía más o divulgaremos tus secretos)(Kaspersky, 2023b).

Si quieres leer un correo real de sextorsión echa un vistazo al siguiente enlace Ciberdelincuentes están creando falsas imágenes y videos sexuales mediante IA para sextorsión se trata de una publicación del antivirus ESET.

5.28 Doxing

El término "doxing" es la abreviación de "exponer dox", siendo "dox" un término coloquial para referirse a los documentos. Por lo general, el doxing es una acción maliciosa que un hacker realiza contra personas con las que está en desacuerdo o que considera desagradables.

El doxing (a veces escrito como doxxing) consiste en revelar información identificadora de una persona en línea, como su nombre real, dirección particular, lugar de trabajo, teléfono, datos financieros y otra información personal. Luego, esta información se divulga al público sin el permiso de la víctima (Kaspersky, 2023a).

5.29 Baiting

Para llevar a cabo el baiting los ciberdelincuentes suelen utilizar dispositivos de almacenamiento extraíbles, normalmente memorias USB o incluso CDs y DVDs infectados con un software malicioso para posteriormente dejarlos en un lugar en el cual sea fácil de encontrar por la víctima como por ejemplo, baños públicos, ascensores, aceras, etc. Cuando la víctima encuentre dicho dispositivo y lo introduzca en su ordenador, el software malicioso se ejecutará de manera inadvertida y posibilitará que el hacker pueda acceder a los datos del usuario o usuaria (Moodle-Universidad de Alicante, 2021).

La vía de contagio como te habrás podido dar cuenta queda implícita.

Si quieres saber cómo minimizar el riesgo por contagio a través de USBs lee el siguiente artículo Cómo conectar con seguridad un pendrive que puede tener virus.

5.30 Clickjacking

El clickjacking busca usuarios desprevenidos que hagan clic en algún botón, pestaña o accedan a un enlace mientras navegan por internet, haciéndoles

creer que están ante algo legítimo y positivo para ellos. Suelen ser ganchos tales como, una oferta muy ventajosa o algo que provoque en la víctima la necesidad de entrar e informarse y de esta modo quedar infectado (Wikipedia, 2021a).

5.31 Dumpster diving o scavening

Este ciberdelito se conoce como el proceso de buscar en tu basura para obtener información útil sobre ti o tu empresa que luego pueda ser utilizada en tu contra. Aunque este tipo de ataques está más bien dirigido a empresas, debes tener cuidado con la información que desechas por el método de tirarlo a la basura. Nunca se sabe lo que los cibercacos están dispuestos a hacer (Wikipedia, 2021e).

Cuando te deshagas del algún dispositivo físico de almacenamiento, ya sea un disco duro externo, un PC, un USB o cualquier otro dispositivo, asegúrate primero de eliminar totalmente todo el contenido. Para ello utiliza software de borrado definitivo, ya que un simple formateado no eliminará la información. El borrado solo se completa cuando se reescribe sobre la anterior información, es por esto que un formateo solo te hace constar que el espacio está disponible, pero el contenido sigue estando ahí, aunque oculto. Esto quiere decir que con software avanzado y específico los ciberdelincuentes podrían recuperar todo el contenido (Xataka, 2019a).

Algunas herramientas de borrado definitivo son:

- Eraser.
- Disk wipe.

Para evitar este tipo de amenaza ya sabes, ten cuidado con lo que tiras a la basura.

5.32 Quid pro quo

Según el diccionario de la lengua española el término “quid pro quo” es una locución latina que significa, cosa que sustituye a algo equivalente o que se recibe como compensación por ello. Sabiendo esto, el ciberdelincuente que emplea esta técnica, promete a su víctima un beneficio a cambio de información personal. Este beneficio suele ser compensaciones en formato regalo, como pueda ser merchandising, dinero, acceso gratuito a programas de pago, ayuda en servicio técnico, etc. Normalmente este ciberdelito te llegará a través de llamadas telefónicas o mensajes de supuestos expertos que ofrecen este tipo de compensaciones sin coste alguno (Mailfence, 2020).

Las vías de contagio se han señalado más arriba y son las llamadas de teléfono o los mensajes con independencia de la naturaleza de estos.

5.33 Formjacking

El formjacking es la técnica que utilizan los ciberdelincuentes para interceptar la información que pones al comprar por Internet. Cuando entras en una página y realizas un pago, tienes que introducir los datos de tu tarjeta bancaria y esa es la información que busca el ciberestafador.

Esto lo llevan a cabo secuestrando los sitios webs donde habitualmente compran los usuarios. De esta forma la información que se introduce va a parar a un servidor controlado por ciberdelicuentes a través de lo que se conoce como la técnica de inyección de código malicioso, también conocido como e-skimming, pudiendo así, robar información de pagos, número de la tarjeta o cualquier otro tipo de datos sensibles.

Es por ello que es muy recomendable evitar las páginas que puedan ser vistas como vulnerables, ya que éstas van a ser la vía de contagio. Aunque esto pueda parecer difícil de detectar, si ves una web con una estética un tanto antigua es posible que el resto de la web también este algo obsoleta y sea el objetivo de este ciberdelito (Redeszone, 2019).

5.34 Juice jacking

Prácticamente todo el mundo en algún momento se ha quedado sin carga en algunos de sus dispositivos, pero gracias a que existen multitud de cargadores de USB públicos, esto ya no es un problema. Pero detrás de los beneficios que esta práctica nos aporta, se esconde una amenaza que va proliferando cada vez más llamada juice jacking. El juice jacking consiste en alterar con fines maliciosos la fuente de carga de los USBs por parte de los diberdelincuentes y que a través de esta técnica pueden aprovecharse tanto para el robo datos como para la inyección de archivos (ESET, 2021).

En la siguiente entrada del Incibe te cuentan cómo un puerto de carga público puede ser un vector de contagio de malware ¡SOS, batería baja! Cuidado con dónde cargas tu dispositivo.

Para evitar ser víctima de este ciberataque puedes:

- Llevar batería portátil.
- Existe un dispositivo llamado juice jack defender actúa como escudo bloqueando la transmisión de datos.

Además los cargadores públicos pueden estar en mal estado con voltajes no adecuados por el mal uso de los usuarios y provocar avería de forma física el dispositivo.

De verte en la necesidad de hacer uso de ellos:

- No hagas uso del dispositivo mientras realiza la carga.
- Mantén la pantalla bloqueada para minimizar la transmisión de datos.
- No aceptar peticiones de conexión con el dispositivo.

La vía de contagio de esta ciberamenaza queda evidente en lo anteriormente expuesto, por lo que intenta evitar en la medida de lo posible usar cargadores públicos.

5.35 Voice hacking

El voice hacking hace referencia a las técnicas utilizadas para manipular la voz de las personas mediante tecnologías avanzadas. Esto incluye la clonación de voz, que emplea inteligencia artificial para imitar la voz de una persona específica y generar grabaciones que parecen reales. También se denomina deepfake de voz o deep voice, ya que produce mensajes falsos que aparentan provenir de alguien auténtico.

Los estafadores pueden captar la voz de una persona sin su permiso y emplear ese audio para crear mensajes falsos que resulten convincentes. Este tipo de ataque puede poner en riesgo la seguridad de dispositivos como asistentes virtuales (Alexa, Siri, Google Home) y otros aparatos IoT.

Puedes leer el artículo completo en ¿Qué es el voice hacking?.

5.36 Sustracción o perdida de tu dispositivo

Otra contingencia con la que te puedes encontrar es el robo o perdida de tu dispositivo. Si te encontrases ante esta posibilidad, a continuación, tienes esta lista de todo lo que debes hacer para minimizar males mayores.

Qué hacer en caso de que hayas extraviado o te hayan robado tu dispositivo móvil:

- Pide a tu operadora que bloquee el IMEI de tu teléfono.
- Búscalo con el localizador para Android o para Apple.
- Anula la SIM y pide duplicado de la misma.

- Cambia todas tus contraseñas. ¡Todas!.
- Denúncialo a la Policía.
- Denúncialo a tu operadora
- Avisa a tus contactos. Sí, a todos.
- Bloquea el dispositivo y borra el contenido que puedas de forma remota.
- Comprueba tu cuenta bancaria y ponte en contacto con tu banco.

Lo mismo ocurre para el caso de ordenadores portátiles ya que Microsoft también dispone de servicio de Encontrar y bloquear un dispositivo Windows perdido. Del igual modo también en el caso de portátiles de Apple en Localizar un dispositivo en Buscar en el Mac

Capítulo 6

Tu yo digital

6.1 Toma consciencia de tu yo digital

En esta sociedad actual, tecnológica y digitalizada, de la que todos en mayor o menor medida formamos parte, debemos tener siempre presente que la forma en que desarrollamos nuestra personalidad, creamos nuestras relaciones sociales o gestionamos nuestra economía, nos lleva a definir nuestra imagen de marca y reputación digital.

En la esfera digital todas y cada una de nuestras acciones tendrá una repercusión directa en lo que el resto va a percibir sobre nosotros y por ende a definir quiénes somos, tanto desde una perspectiva personal, profesional como social creando constantemente y a veces casi de manera imperceptible nuestra identidad digital. Es por ello que no debes perder el foco y entender que esto va a contribuir y afectar a todas las capas de tu yo analógico.

Por lo tanto, en este nuevo escenario hacia la web 3.0 en la que ha aumentado la exposición a la superficie digital, y en el que el incremento exponencial de la ciberdelincuencia parece no tener freno, debes aprender y mejorar la experiencia digital y hacerla compatible con un uso responsable, respetuoso, crítico y creativo de la tecnología. Y a su vez desarrollar capacidades digitales que propicien un progreso inclusivo, seguro, privado y sostenibles que garantice el bienestar social.

6.2 Metadatos

Los metadatos pueden ser descritos de varias formas posibles, pero de forma resumida son un conjunto de datos que proporciona información de un recurso. Datos como pueden ser un archivo de imagen o un documento de texto, siendo algunos de estos metadatos la fecha de creación, la de última modificación o la resolución en el caso de una imagen (Wikipedia, 2021h).

La función principal de los metadatos es la de ampliar con información adicional la contenida en el recurso del que forman parte con el fin de mejorar la calidad y efectividad de las búsquedas realizadas, no solo a la hora de realizar una búsqueda de un archivo perdido en nuestro sistema operativo, sino que esto afecta incluso al posicionamiento web.

En ciertas ocasiones estos datos pueden provocar problemas, algunos de ellos de seguridad y privacidad como puede ocurrir por ejemplo por alguno de los dos motivos siguientes:

- Suele ocurrir que algunas cámaras fotográficas incluyan las coordenadas geográficas desde las que se realiza la fotografía entre los metadatos en los archivos de imágenes, pudiéndose localizar la posición en la que la imagen fue tomada. Esto es lo que se conoce como Geoetiquetado.
- Puede determinarse la versión del software con la que fue guardado un archivo, por lo que si trabajas en una empresa y no tienes la licencia de dicho programa, los metadatos pueden generarte problemas.
- La longitud de los mensajes, el autor, la localización, las fechas, la hora, etc. identifican patrones de comportamientos, hábitos, relaciones y detalles personales. Todos estos datos son denominados el petróleo del siglo XXI (OSI, 2020c).

Para que puedas hacer una valoración de por que a todos los datos personales se les denominan el petróleo del siglo XXI, visita la siguiente infografía de cuál es el valor de tus datos en la red.

6.3 Huella digital o reputación online

Eres lo que publicas, lo que compartes, con quién te relacionas e incluso lo que visitas desde tus dispositivos y todo este rastro es lo que compone la huella digital.

En otras palabras, la huella digital o reputación online es la fama o prestigio que una persona o una empresa tiene en el mundo digital. Realmente la reputación digital no difiere mucho de la reputación tradicional, ya que en cierto modo ambas están conectadas, por lo que deben ser coherente la una con la otra.

También se puede denominar la identidad digitad como el conjunto formado por:

- Información que nosotros mismos publicamos.
- Información que compartimos de otros usuarios.

- Aquella información que existe en Internet sobre nosotros.

Cabe destacar que la variante digital ha tomado gran importancia, ya que cuando una persona o compañía quiere saber de ti, uno de los mecanismos que va a utilizar es buscarte en internet, y es, en este punto donde radica la importancia de contar con una buena reputación online (Cícero Comunicación, 2021).

En este sentido es importante en un primer momento, conocer si tu huella digital goza de una buena salud y para ello lo más recomendable es que hagas un ejercicio de búsqueda, para ver si los resultados que obtienes son buenos. Puedes usar algunas de las siguientes herramientas para este propósito:

- Buscar directamente en Google o otros buscadores. Puedes apoyarte en las búsquedas avanzadas de Google. Esto es lo que se conoce como Egosurfing.
- También tienes plataformas que te ayudan a descubrir dónde están tus datos personales y poder gestionar tu huella digital. En los siguientes enlaces puedes encontrar dos de ellas Say mine y Jumbo privacy.
- Crear alertas de Google alert. Este recurso también te servira para estar al día de lo que se publica sobre ti.
- Hootsuite. Esta herramienta te buscará entre las principales redes sociales, como Facebook, Twitter, etc. es usada en su mayoría en el mundo corporativo.
- Haz una búsqueda de imágenes inversa. Con esta búsqueda puedes ver si una imagen tuya, está siendo utilizada en otros sitios web y con qué fin. En el siguiente enlace, tienes la información para llevarla a cabo. Cómo hacer una búsqueda de imágenes inversa.

Si los resultados obtenidos no son de tu agrado, algunas plataformas te permiten solicita la eliminación de dicho contenido o simplemente puedes gestionar tú, esa información desde la propia plataforma. En el caso de Google puedes hacerlo a través de Mi Actividad.

Crear una buena huella digital requiere de tiempo y debes ser cuidadoso con la manera en que interactúas en la red. Existen decálogos que te guían para crear una excelente reputación online, así como videos tutoriales y herramientas para llevarlo a cabo. Nos obstante aquí tienes las mejores recomendaciones para cuando quieras compartir, comentar, valorar o opinar en cualquiera de los medios sociales como Facebook, Instagram o cualquier otra, hacer una reseña en Google o participar en algún foro (Valencia Plaza, 2014).

- Presencia y actualización sistemática.

- Cuidar la imagen mostrando transparencia.
- Aportar contenido de calidad.
- Respetar siempre la opinión ajena.
- Identificar los canales apropiados con los que interactuar.
- Tener en cuenta las reglas de urbanidad digital, esto consiste en una redacción cuidada y usos de negritas o enlaces de interés.
- Diferenciar entre lo público y lo privado.

Estas últimas puedes tenerlas en cuenta si quieres llevar tu huella digital a un nivel más profesional.

- Disponer de un blog personal.
- Mantener una actitud en la red activa.
- Permanecer atento a las nuevas redes y formas de difusión.

6.4 Sombra digital

Cada foto que subes a Facebook, Instagram, cada mail que mandas, cada comentario o reseña que vas dejando en la web está generando lo ya conoces como huella digital. Hasta aquí todo bien, pero además de este rastro que es más o menos voluntario, también vas dejando otro rastro del que quizá no seas tan consciente, y a este rastro es al que se le conoce como sombra digital.

Ya en 2008 existían métricas que aseguran que la cantidad de información que se tiene de un individuo era mayor a la información creada por el mismo.

Partiendo de estos preceptos, la sombra digital es la información que queda de nosotros en los diferentes sistemas ya sean públicos o privados. Estos datos nos identifican y saben de nuestros gustos y preferencias. En la mayoría de los casos sin que nosotros mismos seamos conscientes de ello.

En este punto es cuando te estas preguntando como se crea la sombra digital. Pues bien, la sombra digital se va creando con el uso que haces de tus dispositivos, de la cámara en lugares públicos o privados, con el uso de la domótica como en el caso de las bombillas inteligentes y de otras múltiples maneras cuando interactúas con la tecnología. Los fabricantes introducen cookies y software específico para este fin dentro de los sistemas operativos, para saber cuándo los usas, el tiempo que empleas, si usas hardware externo del tipo que sea e incluso para hacer un mapa de tu casa mientras usas tu aspiradora inteligente. Como verás la sombra digital se va construyendo por si sola.

Este concepto podría considerarse como una vulnerabilidad más de tu privacidad, pero también puede ser de mucha utilidad, como por ejemplo, cuando Google maps analiza tu movilidad para gestionar mejor tu trayecto, mostrarte cuánto vas a tardar, que ruta puedes tomar y todo en tiempo real, algo que no sería posible sin la gestión de la sombra digital (Xataka, 2019b).

Si quieres ser más consciente de todo lo que Google recopila del uso que haces de sus servicios, lee la siguiente entrada donde podrás ver toda la traza de tu actividad digital He mirado todos los datos que Google tiene sobre mí, y confirmo que es el Gran Hermano definitivo. Además tienes el servicio de takeout.google.com desde podrás descargar todo lo que la Compañía de Mountain View tiene de ti.

6.5 Eliminar el historial de busquedas

Cualquier navegador, salvo que usemos una navegación privada, almacena un registro de las páginas que hemos visitado, una información que podemos borrar si queremos o conservar en el caso de querer localizar más tarde alguna página que no recordemos. Es muy útil en este segundo caso, pero puede llegar a ser embarazoso si no queremos que nadie pueda ver las webs que hemos visitado.

Cada navegador ofrece la posibilidad de borrar toda esta información y para ello puedes acceder desde los menús del propio navegador. Cada navegador tiene una forma diferente de realizar este borrado, aunque normalmente suele estar en la opción/pestaña herramientas. No obstante, el siguiente enlace te llevará a la web del antivirus AVG, desde donde te enlazará a los diferentes tutoriales de cómo borrar el historial de navegación y de búsquedas de los navegadores más populares, como Google Chrome, Firefox o Microsoft Edge entre otros.

6.6 Derecho al olvido

El Reglamento General de Protección de Datos recoge una norma que permite a los usuarios poder ejercer su derecho al olvido. Esto quiere decir que todas las personas tienen el derecho de solicitar a los buscadores, webs o plataformas que eliminen todos sus datos personales que aparecen en los resultados de búsqueda al introducir un nombre o cualquier otro dato personal. Dicho de otro modo, el derecho al olvido es aquel que tienen todos los ciudadanos a impedir la difusión de información personal a través de Internet.

Cabe aclarar que la eliminación de un enlace de un buscador no implica la desaparición de toda la información de carácter personal publicada en Internet. Este borrado sólo afecta a los motores de búsqueda que enlazan a dicho contenido (OSI, 2020b).

Los siguientes enlaces te llevarán a los formularios de las plataformas detalladas donde podrás solicitar tu derecho al olvido:

-Solicitud de derecho al olvido de Google

-Solicitud de derecho al olvido de Bing

-Solicitud de derecho al olvido de Yahoo

-Solicitud de derecho al olvido de Facebook

Como podrás imaginar estas son las plataformas más relevantes, no obstante, todas las demás deben de tener esta opción. Si la plataforma a la que quieres solicitar tu derecho al olvido no está entre éstas, solicítalo por el canal de comunicación que tengan establecido.

Este derecho se puede gestionar al amparo de la agencia española de protección de datos y en caso de fallar esta primera vía administrativa siempre nos quedaría la vía judicial.

Esto es parte de lo que se conoce como derecho al olvido. Si quieres más información visita el enlace ¿Sabes cómo ejercer el derecho al olvido?.

Capítulo 7

Contenido en la red

7.1 El contenido digital

Cada vez más el contenido digital es mayor, a su vez va creciendo de manera exponencial y además está disponible en multitud de formatos, como textos, imágenes, audio, vídeos. Llega a todos los públicos por diferentes canales y an tratándose del mismo contenido, la manera en que este es mapeado o modelado, también es otra variante más de como la información llega al receptor final. Un ejemplo de como mapear o modelar una misma información en un mismo formato sería el uso de la representación visual o también conocido como Visual Thinking y una infografía, ambos dos están representados en formato imagen.

La lectura que debes hacer en este punto, es que no toda la información vale y no todo el contenido es de calidad, por ello, tener claro los siguientes puntos pueden ser de mucha ayuda.

7.2 Contrastar la información

Según el diccionario de la Real Academia Española, la palabra contrastar en una de sus acepciones consiste en comprobar la exactitud o autenticidad de algo. Hoy en día la información en más rápida de encontrar y abundante en lo que se conoce como infoxicación. La infoxicación no es más que la sobrecarga de información a la que las personas se ven sometidas en su día a día, por lo que es importante saberla escoger, y saber que en muchos casos se trata de información irrelevante que algunas personas comparten simplemente por falta de conocimiento o criterio y en el peor de los casos para confundir.

Al contrastar información debes hacer un análisis de todas aquellas fuentes que encuentras, ya que el resultado de una búsqueda en los navegadores es muy abundante y la información a veces es efímera y puede llegar a no estar totalmente actualizada, con lo que eso conlleva.

No debes conformarte con dar por buena la primera versión de una información en Internet, empobrece tu experiencia como usuario y te perjudica como lector. Por ello debes tener presente el compromiso ético, por mucho que las prisas sean las que mandes en algunas ocasiones, siempre debes cuidar tu ética al trabajar y contrastar muy bien toda información y fuente (Fuentes de información, 2016).

7.3 Fake news y Deepfake

Las fake news o también llamados bulos o hoax son noticias sobre temas de interés social o de actualidad para crear una alarma o atraer la atención del mayor número de usuarios posibles y su objetivo principal es la desinformación. Suelen compartirse por redes sociales, correo electrónico o aplicaciones de mensajería instantánea como WhatsApp que aun contando con una función antibulos no queda exenta (OSI, 2020a).

Se diseñan y emiten con la intención deliberada de engañar, inducir a error, manipular decisiones personales, desprestigiar o enaltecer a una institución, entidad o persona u obtener ganancias económicas o rédito político, aunque en algunas ocasiones también incluyen promociones, ofertas y descuentos, especialmente en época de rebajas o compras navideñas (Wikipedia, 2021f).

De otro lado el deepfake es una técnica de inteligencia artificial que permite editar vídeos falsos de personas que aparentemente son reales, dando como resultado final un vídeo muy realista, aunque ficticio (Wikipedia, 2021d).

Amplia la información sobre deepfake en este artículo ¿Qué es y en qué consiste Deepfake? de la revista digital Computer Hoy. En este otro artículo llamado así es posible saber si un vídeo es un deepfake con sólo un abrir y cerrar de ojos tienes un video que no deberías dejar de ver, donde por medio de la inteligencia artificial ponen la cara del actor Steve Buscemi al cuerpo de Jennifer Lawrence en una intervención de una gala. Y por si el anterior video te sabe a poco aquí tienes otro de deepfake de Barack Obama.

A su vez los deepfakes pueden ser de tipo deepface o deepvoice. El deepface es cuando se trata de una imagen y audio o lo que es lo mismo de un video y el deepvoice cuando solo se trata de la manipulación de la voz.

A continuación, verás algunos consejos para poder hacer una buena criba de la información que te encuentres:

- Revisa la URL: mira que se trate de una web legítima.
- Revisa el titular: haz una búsqueda del titular para poder contrastar su autenticidad.
- Contrasta la información en la red: realiza una búsqueda para comprobar la veracidad.

- Busca la fuente: comprueba si la fuente es legítima.
- Comprueba la autoría: si no aparece el autor es posible que no sea de fiar.
- Comproba el formato: imágenes de poca calidad, redacción con errores gramaticales, faltas de ortografías, portal poco cuidado, etc.
- Revisa la imagen de la noticia: para comprobar que la imagen realmente corresponde con la información y no esta sacada de otra noticia, que además no guarde ninguna relación con esta. Para ello tienes este par de recursos Google images search y Tineye.
- Aplica el sentido común.

En el caso de tratarse de una deepfake ten encuenta los siguientes:

- Fíjate en los fondos: fondos desconfigurados o poco fiables.
- Busca deficiencias en los movimientos: movimientos extraños en el personaje.
- Céntrate en los gestos: gestos faciales no naturales o falta de parpadeo, teniendo en cuenta que el ser humano parpadea aproximadamente cada 5 o 10 segundos.
- Agudiza el oído: fallos en el audio o ruidos extraños.
- Mira la duración: al ser caros de editar suelen ser intervenciones breves.
- Reflexiona: piensa si lo que se dice concuerda con los valores e ideales de quién lo dice.
- Aplica de nuevo el sentido común.

En esta entrada de Google llamada Identifica la información falsa en línea con estos consejos encontrarás más consejos para que detectar fake news te resulte más sencillo.

El compartir bulos o fake news aunque no seas consciente de ello fomenta la desinformación, en algunos casos la propagación de virus, malware o cualquier otra amenaza de las que ya conoces y además puede llegar a afectar negativamente a tu reputación digital, sin olvidarnos que afecta a tus contactos y a tu relación con ellos (OSI, 2019b).

Cuando creas que te encuentras ante un posible bulo o fake news, ten en cuentas los siguientes:

- No los reenvíes.
- No abras enlaces ni realices descargas.

- Verifica la información.

En esta lista tienes plataformas que te ayudarán a identificar si estas ante un bulo o fake news:

- Google Fact Check Explorer
- Newtral
- Maldita
- Verifica RTVE
- Learn to check
- Salud sin bulos

En la plataforma Maldita, una de las actividades que realizan son la de desenmascarar estos bulos desgranando y dándote claves para que vayas aprendiendo a detectarlos.

Figura 7.1: Deepfake.

Una ciberestafa basada en la deepfake es la de la suplantación de un personaje público con el fin de ir creando un ambiente de confianza para finalmente pedir dinero. Si quieres más detalles sobre este fraude online lee el siguiente artículo del Incibe Intento de fraude amoroso utilizando técnicas de deepfake para suplantar a un personaje público.

7.4 Deep web

El tema de la Deep Web es quizá un tema polémico y estigmatizado, pero al tratarse de una pieza más en este inmenso puzle que es internet, es de recibo conocer al menos de que trata esto de la Web Profunda (Deep Web).

Existe una serie de contenido que por diversos motivos no está indexado en los buscadores convencionales como Google, Bing o Yahoo, entre otros y no siempre por temas de legalidad, moralidad o por no ser contenido lícito. Por ejemplo, si estas en china y quieres acceder a Google no te va a quedar otro remedio que hacer uso de este servicio, ya que como sabrás China no permite el uso de Google, entre otros muchos servicios de internet. Es por esto y otras razones por lo que existe la Deep Web (OSI, 2019a).

De otro lado, está el controvertido tema de las ilegalidades y otros asuntos turbios en lo que se conoce como la Dark Web y de los que no se va a tratar en este manual. Pero si quieres indagar por tu cuenta visita el siguiente enlace Una semana en la Deep Web y esto es lo que me encontrado.

Capítulo 8

Otras particularidades importantes

8.1 Otros conceptos relevantes

Existen otras muchas particularidades y conceptos que al no encajar de manera directa en unidades anteriores van a ser vistas en esta unidad. Aquí podrás ver otros aspectos relacionados con la privacidad y seguridad en internet que también te pueden ayudar a abordar todos estos temas.

8.2 Desinfecta tu dispositivo

Si crees que tu dispositivo puede estar infectado, aquí tienes una entrada de la Oficina de Seguridad de Internauta llamada desinfecta tu dispositivo, encabezada con los principales signos que pueden ponerte sobre aviso, así como las 3 fases de las que consta para solucionar este contratiempo y que son, una primera fase de primeros auxilios, una segunda fase de soluciones avanzadas y una tercera y última fase de solución definitiva.

8.3 Analizadores de virus online

En este punto tienes una lista de plataformas online que escanean y analizan cualquier tipo de fichero, url entre otras con la intensión de encontrar malware en ellos:

- VirusTotal.
- Internxt.
- Kaspersky.
- Metadefender.
- Eset.
- F-secure.

8.4 Menores en el uso de la red

En lo que concierne a menores, la cuestión se torna más delicada, ya que se trata de grupo más inexperto y vulnerable, siendo 1 de cada 3 usuarios de internet un niño. En este manual no se va a tratar en profundidad este tema, ya que por si solo podría tratarse de otro manual completo, pero si cabe destacar algunos conceptos bastantes relevantes como la educación, la concienciación y el seguimiento que tú, como padre, madre o tutor debes hacer del uso que hacen los menores de internet.

Por supuesto también has de conocer y hacerles saber de los peligros y amenazas con las que pueden encontrarse y que asechan tras la aparente inofensiva pantalla.

Sabes que entre el uso que hacen tus hijos de la red están actividades lúdicas como jugar, otras didácticas como aprender, otras sociales como relacionarse con amigos u otros y todo esto, en la mayoría de las veces a tan solo solo click.

Pero no olvides que debes ser tú quien los guíe en la educación y concienciación, además de hacer un seguimiento de cerca para saber el uso que hace de las tecnologías. Para todo esto dispones de guías, herramientas, consejos, etc. Cabe destacar que es importante guiarlos para que tus menores hagan un uso responsable, respetuoso y de carácter prudente en el ámbito tecnológico, y que a su vez sean conscientes de todas las particularidades que conlleva interactuar tanto con los medios como con los dispositivos.

Por todo lo anteriormente expuesto, a continuación, tienes estas sucintas listas como toma de contacto en lo que a menores se refiere.

Medidas con las que los menores deben comprometerse:

- No publicar fotos o vídeos de alguien sin permiso. Esto también hay que tenerlo en cuenta entre adultos.
- No usar la webcam con desconocidos. Además de tenerla tapada cuando no se esté usando, para ello existen adhesivos y otros artilugios.
- No creer en los regalos o chollos a los que se verán expuestos a través de ventanas pop-up, emails, etc.
- No aceptar amigos en las redes sociales que no conozcan, ya que en un principio no los deberían considerar como amigos reales.
- No ponerse en contacto con desconocidos.
- No acordar citas con desconocidos a través de internet.
- No facilitar datos personales.

- No contestar a las provocaciones e ignorarlas.
- No hacer en la Red lo que no harían a la cara.
- Tener cuidado con la información que comparten en línea, incluyendo el correo, redes sociales como Instagram, TikTok, etc.
- Comportarse con educación en la Red.
- Respetar los derechos de los demás en Internet y no reenviar material inadecuado por correo electrónico o cualquier otra plataforma de difusión.
- Si los molestan o amenazan, deben abandonar la conexión y pedir ayuda.
- Mostrarse más celoso de su vida privada. Ya que llega un punto en que no diferencian bien entre lo público y lo privado y acostumbran a sociabilizar todos los aspectos de su vida.

Principales amenazas a la que los menores están expuestos:

- Ciberbylling.
- Gossip o informer.
- Ciberadicción.
- Vamping.
- Grooming.
- Sexting.
- Obesidad digital.
- Cibercontrol.

Además, conforme vayan creciendo se podrán ir topando con todos los peligros anteriormente vistos en este manual.

Qué debes enseñar a tus hijos como padre, madre o tutor:

- Concienciarles sobre su actividad en la red. Aquello que salga de su móvil o correo no podrá recuperarlo jamás, perdurará en el tiempo y se trata de una información personal que cualquiera podría utilizarla.
- Hacerles conscientes de su identidad digital.
- Deben entender que navegar por Internet puede considerarse un derecho, pero también supone una responsabilidad. Al igual que pasear por la calle no les da derecho a cruzar con un semáforo en rojo, navegar por Internet no les da derecho a entrar en un lugar que no deben.

- Contraseñas seguras y diferentes. En la unidad de Gestión de la seguridad en la red de este manual encontrarás en el apartado de contraseñas todo lo que necesitas saber.
- Deben saber que es fácil deducir información personal de fotos o comentarios, como por ejemplo el lugar donde viven, los sitios que frecuentan y demás.
- Enséñales a no hacer descargas de programas sin tu permiso, para que sepan en que consiste la propiedad intelectual y a tener cuidado con programas con virus, etc.
- Ayudarles y enseñarles a protegerse del spam, correos phising, software espía, malware, etc.
- Alertar a los menores que deben avisarte siempre que algún "amigo de Internet" insista respecto a informaciones o hábitos personales.
- Deben saber que no están del todo seguro/a al otro lado de la pantalla.
- El riesgo es el mismo en el mundo digital que en el real.
- Ayúdalos a entender que no toda la información en internet es veraz o fidedigna, y que la información debe contrastarse en varias fuentes.

Cuál es tu compromiso como padre, madre o tutor:

- Establecer espacios de trabajo independientes. Es bueno que tus hijos tengan su propio espacio dentro del ordenador, su propio escritorio, su propio fondo de pantalla, su propia lista de favoritos, su propio sistema de carpetas. De esa manera proteges tus datos y les haces responsables de los suyos, pudiéndoles crear un control parental o restricciones mediante el navegador y apps para dispositivos móviles.
- Establecer un horario de tiempo máximo de conexión.
- Colocar el ordenador en una zona común.
- Navegar por internet solo en presencia de un adulto. De esta manera no crecerán como huérfanos digitales.
- Estar informado del tipo y tiempo de navegación que hacen.
- Mantente actualizado con la tecnología. No necesitas saber exactamente como funciona todo, sólo necesitas saber qué son y para qué se usan. Ejemplo: no es lo mismo un chat que una app de mensajería instantánea.
- Hablar habitualmente de las tecnologías y compartir actividad digital con ellos. Respecto a la navegación que practican, a respetar las reglas y cumplir con obligaciones y acuerdos, a negociar y dialogar sobre los límites (Reglas consensuadas) para navegar en Internet.

- Fomentar y premiar el uso adecuado y responsable de las tecnologías.
- Disponer de antivirus.
- Conocer el código PEGI (Pan European Game Information) que regula los juegos, donde se estipulan si son de carácter individual o colectivo, de estrategias, deportivos, shooting, aventura, la edad adecuada de consumo, etc.

Para ampliar la información dispones de dos exhaustivas guías de la Junta de Andalucia Guía de formación TIC para padres y madres de menores de 3 a 11 años y Guía de formación TIC para adolescentes.

Y en estos dos enlaces encontrarás dos prácticos recursos Family Link by Google y Secure Kids.

8.5 Utilidades interesantes

Aparte de todo lo visto en el manual existen muchas otras herramientas para ayudarte a salvaguardar tu privacidad y seguridad en internet, algunas de estas son:

- Correo electrónico (email):
  - Emails temporales: Si solo necesitas registrarte en una web para un recurso puntual, como por ejemplo descargarte un eBook, puedes utilizar Temporay email, TempMailo o Tempmail y no son los únicos servicios de este tipo, en el siguiente enlace tienes una lista más amplia de servicios de correos temporales. Y si usas el navegador Firefox, podrás tener este mismo servicio integrado en el propio navegador con solo la instalación del plugin Relay firefox.
  - Emails anónimos: Con Secure email puedes enviar correos electrónicos y SMS anónimos, falsificar el número del remitente de SMS y muchos más.
  - Modificar el alias o identidad del email: Simple login es un servicio con el que puedes crear tus alias o identidades para ocultar tu email personal, evitar spam y mantener tu privacidad.
- Escaneo de URLs maliciosas: UrlScan, Norton Safe Web o Urlvoid. Estas plataformas detectan las direcciones webs fraudulentas.
- Comprobar y mejorar tu privacidad y seguridad en internet: Lista de verificación de seguridad. Esta web esta en inglés, pero abarca un amplio espectro de herramientas y recursos diseñados para mejorar tu privacidad, seguridad y protección online y siempre dispones del traductor en línea de Google.

- Eliminar cuentas en Redes Sociales: Justdeleteme es una plataforma donde te facilitan los enlaces para eliminar tus cuentas de los servicios webs que ya no desees seguir usando.
- Números de teléfono de usar y tirar: Hushed es un servicio premium pero de coste muy económico. Solo es cuestión de ver si te compensa.
- Recibe SMS a un número de teléfono temporal: Online-sms te permite recibir SMS en línea a un nuevo número de teléfono temporal de forma gratuita.
- Nombres y direcciones desechables: Generador de nombres falsos. Como en el caso de los emails temporales este servicio puede ser un buen recurso.
- Aviso de webs sospechosas: En el Chrome Web Store encontrarás este plugin que se llama Suspicious Site Reporter y que se encargará de avisarte si estas ante una web de dudosa reputación.
- Aviso de actividades sospechosas: Con Get Logdog recibirás alertas cada vez que ocurra una actividad sospechosa en tu Gmail, Facebook y otras cuentas.
- Protección dispositivo móvil: Conan Mobile te permite conocer el estado de seguridad de tu dispositivo, mostrándote soluciones a posibles riesgos a los que estés expuesto y proporcionándote algunos consejos que te ayudarán a mejorar su seguridad.
- Verificadores de URLs acortadas: Comprobar la seguridad de una URL acortada antes de hacer click en ella es otra buena práctica para no acabar en una web de dudosa procedencia. A continuación, tienes estos verificadores Unshorten, Checkshorturl y VirusTotal o Urlex.
- Plugin o extensión antimalware: MyWot te mantendrá a salvo de estafas, malware, phishing y robo de identidad mientras navegas.
- Centros de Seguridad. Estos centros son los servicios con los que las grandes plataformas digitales se comprometen a velar por tu privacidad y seguridad:
  - Google.
  - Facebook.
  - Instagram.
  - Tiktok.
- Testigos online: Los testigos online te permiten certificar evidencias digitales en una fecha y hora determinada, o lo que es lo mismo, el contenido de una web concreta en un momento determinado, o el envío de un correo electrónico a una persona específica.

8.6 Ataques en tiempo real

En los siguientes enlaces tienes diferentes servicios en los que puedes ver en tiempo real los ataques a nivel global:

- Threatmap checkpoint
- Cybermap kaspersky
- Threatmap bitdefender
- Live threat map
- Threatmap fortiguard

8.7 Eventos internacionales

Durante el año, países e instituciones como la Comisión europea promueven iniciativas entorno al ecosistema tecnológico. Son organizadas a nivel internacional y donde pueden llegar a participar hasta más de 100 países. En la siguiente lista se muestran las de más repercusión mediática:

- Día de Internet (17 de mayo).
- Día Internacional de Internet Segura (Segundo martes de febrero).
- Día mundial de la contraseña (Primer jueves de mayo).
- Día mundial de la copia de seguridad (31 de marzo).

8.8 Colabora

Si eres una persona participativa y te gusta colaborar y aportar a los demás. Más abajo encontrarás una lista de actividades que podrás realizar, en las que no solo estarás ayudando a divulgar contenido y ayudar a otros, sino que además, repercutirá de manera positiva en tu vida.

- Cibercooperante (Incibe).
- Cibervoluntario (Ciber voluntarios).
- Voluntario digital (Ayuda en acción).
- Voluntariado digital (Click_A).

ANÍMATE!!!

Capítulo 9

Formación y conocimientos

9.1 Aprendizaje y reciclado continuo

El aprendizaje y el reciclado continuo son dos de los pilares más importantes donde sustentar la educación. Por lo tanto, sabrás que una buena educación abre puertas, facilita una mejor toma de decisiones y ayuda a evitar posibles escenarios futuros no deseados. Por ello, es solo deber tuyo no descuidar la formación en conocimientos si quieres que sea tu mejor aliada para tu yo presente y futuro.

9.2 Formación como medida preventiva

En estos tiempos en los que de manera sutil nos vamos acercando a la cuarta revolución, marcada principalmente por la evolución de las tecnologías, la comunicación y la información entre otras. En los que estamos empezando a coquetear con los nuevos cambios de paradigma económico, con la aparición de las criptomonedas, en lo social con la multitud de plataformas y medios digitales de repercusión mediática, con la descentralización de la nueva web 3.0, la tecnología Blockchain y el protocolo IPFS (InterPlanetary File System), solo nos puede llevar a pensar, que no mantener una formación activa y estar actualizados, puede repercutir de manera desfavorable o negativa en la esfera social, profesional y personal en la que todos nos movemos.

Pon lo tanto, piensa que formarte para protegerte y sentirte seguro en el uso de las tecnologías es una inversión en bienestar y tranquilidad y que a mayor conocimiento, mayor protección y mejor gestión resolutiva.

En todo el grueso de esta manual tienes a tu disposición multitud de plataformas, recursos y herramientas con las que poder aprender y seguir instruyéndote en todo lo concerniente a privacidad y seguridad en internet, por lo tanto, te animo a ir ampliando tus conocimientos cuando quieras y a tu propio ritmo. Porque ya sabes lo que dicen “más vale prevenir que curar”.

No obstante, si estás pensando dedicarte a esto de la ciberseguridad dentro del ámbito profesional, a continuación tienes un lista de formaciones más específicas y/o regladas.

- Ciberseguridad en el Teletrabajo.
- Seguridad en internet.
- Catálogos de formación en ciberseguridad.
- Retos descargables.

9.3 Desarrolla tu ciberinteligencia

El término ciberinteligencia no es nuevo como tal, pero sí, que cada día cobra más vigencia y relevancia tanto en el mundo de los negocios como en el uso que hacen todos los usuarios del ciberespacio (Ambit, 2020).

Según el Centro de Tecnologías Emergentes de la Universidad Carnegie Mellon, que es uno de los más destacados centros de investigación superior de los Estados Unidos en el área de ciencias de la computación y robótica, define la ciberinteligencia como:

"La adquisición y el análisis de información para identificar, rastrear y predecir las capacidades, intenciones y actividades cibernéticas que apoye la toma de decisiones"

Esta definición encaja muy bien en términos empresariales. Pero, ¿cómo podría entenderse este concepto en el uso que hace el común de los mortales de internet?. Para responder a esta pregunta analicemos con más detalle la definición anterior. Si prestas atención verás que las pautas a seguir son:

- Adquisición de la información: Podría entenderse como los conocimientos adquiridos a través de la formación y el reciclado continuo.
- Análisis: La formación adquirida provee de conocimientos para poder analizar el entorno donde mejor se mueven los ciberdelincuentes.
- Predecir las capacidades, intenciones y actividades cibernéticas: Se entiende como la capacidad detectar posibles amenazas.
- Toma de decisiones: Actuar en consecuencia para no llegar a ser una cibervíctima.

En definitiva, la ciberinteligencia entendida desde el punto de vista de las personas podría entenderse como: Las competencias en conocimientos de las ciberamenazas existentes, la gestión de la privacidad y seguridad en los dispositivos y la red, apoyado en el uso de plataformas y software destinados

a tal cometido. Siendo todo lo anterior lo que va a permitir desarrollar las capacidades necesarias para la prevención, detección y reacción adecuada ante posibles ciberataques.

9.4 Pon a prueba tus conocimientos

Una manera de saber que conocimientos tienes sobre privacidad y seguridad en internet es poniéndote a prueba. Es por ello, que a continuación tienes los siguientes recursos donde podrás calibrar cuanto sabes sobre tema. Porque recuerda, a mayor conocimiento, mayor protección.

- ¿Cuánto sabes?: Batería de cuestionarios de la Oficina de Seguridad del Internauta.
- ¿Puedes detectar cuándo te están engañando?: Prueba anti-phishing de Google.
- Diagnóstico de competencias digitales: Autodiagnóstico para conocer el nivel de competencias digitales.
- ¿Sabes escapar de los fakes?: Un sencillo test de autoevaluación para saber cómo de inmune eres a los bulos.

9.5 Canales de avisos y alertas

Una buena manera de estar al tanto, es poder estar al día en sentido literal, de gran parte de lo que esta aconteciendo en lo referente a ciberdelitos, para ello a continuación, tienes dos recursos para que nada o poco de la actualidad ciber criminal no llegue a tu conocimiento.

- Canal de avisos de seguridad de la Oficina de seguridad del internauta.
- Blog HispaSec una al día.

Ambas dos disponen de newsletter a las que suscribirte para que las noticias lleguen a ti y no necesitas visitar las plataformas para estar al tanto. Además también están presentes en la mayoría de redes sociales.

Capítulo 10

Entidades y plataformas de ayuda

10.1 Ayuda y soporte desde instituciones

En internet existen multitud de plataformas y webs que te brindan la oportunidad de formarte y estar informado sobre ciberdelitos, ciberamenazas, privacidad y seguridad en internet y otro montón de conocimientos más. Además, si sabes como abordar la plataforma verás que muchas de ellas son de autoridad reconocida. Aun así, no deja de ser importante saber que desde nuestras instituciones existen proyectos específicos y gestionados por verdaderos expertos en la materia. Y es en esta unidad donde vas a ver con que entidades y plataformas puedes contar.

10.2 Instituto nacional de ciberseguridad

El Instituto Nacional de Ciberseguridad de España INCIBE, es una sociedad dependiente del Ministerio de Economía y Empresa a través de la Secretaría de Estado para el Avance Digital y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

La misión de INCIBE es por tanto reforzar la ciberseguridad, la confianza y la protección de la información y privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, Administración, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones. Aunándolo en estas tres siguientes líneas de actuación:

- Al internauta.
- Al menor.
- A la empresa.

Informan entre otros sobre:

- Protección de redes, equipos y sistemas.
- Cumplimiento de obligaciones relativas a la seguridad de la información.
- Diferentes tipos de incidentes de seguridad.
- Seguridad en las conexiones y redes wifi.
- Configuración de la privacidad en dispositivos y servicios de internet.
- Situaciones de infección por virus.
- Contenidos inadecuados para menores y comunidades peligrosas en línea.
- Ciberacoso escolar.
- Controles parentales.

El Incibe tiene a disposición del ciudadano varios canales de comunicación:

- Teléfono gratuito **017**.
- WhatsApp: **900 116 117**.
- Telegram: **@INCIBE017**.
- Formulario web: **http://incibe.es/linea-de-ayuda-en-ciberseguridad#formulario**.

10.3 Oficina de seguridad del internauta

La Oficina de Seguridad del Internauta OSI es una plataforma que proporciona información y soporte necesarios para evitar y resolver los problemas de seguridad a los que pueda enfrentarse el ciudadano en el uso de Internet.

El objetivo principal de esta entidad es reforzar la confianza en el ámbito digital a través de la formación en materia de ciberseguridad. Desde la Oficina de Seguridad del Internauta conjuntamente con el INCIBE trabajan para:

- Ayudar a los usuarios a llevar a cabo un cambio positivo de comportamiento en relación con la adopción de buenos hábitos de seguridad.
- Hacerles conscientes de su propia responsabilidad en relación con la ciberseguridad.
- Contribuir a minimizar el número y gravedad de incidencias de seguridad experimentadas por el usuario.

- En este portal encontrarás información general sobre la seguridad en Internet y herramientas que te ayudarán a navegar más seguro.

Además de llevar a cabo todas estas líneas de actuación, a través de este portal también:

- Dispones de un canal de avisos para estar actualizado de las últimas alertas de seguridad.
- Podrás hacer reportes de fraudes.
- En el menú de navegación encontrarás una pestaña de juegos educativos donde encontrarás recursos para aprender jugando, entre ellos toda una batería de juegos de mesa.
- Campañas de concienciación.
- Guía para saber qué hacer si eres víctima de un fraude.

Y esto no es todo, en esta plataforma encontrarás multitud de recursos y herramientas para gestionar o solventar cualquier incidencia en matería de privacidad y seguridad en internet.

10.4 Agencia española de protección de datos

La Agencia Española de Protección de Datos AEPD es una entidad de ayuda a la ciudadanía más orientada a la privacidad en lo concerniente a tus datos personales. Actúan para proteger tus derechos de acceso, rectificación, limitación, oposición, supresión (derecho al olvido), portabilidad y oposición al tratamiento de decisiones automatizadas.

Entre los recursos que encontrarás en la plataforma están los siguientes:

- Derechos y deberes en el tratamiento de datos.
- Ayuda a la ciudadanía.
- Ayuda específica a menores.
- Guías y herramientas.

10.5 ObservaCIBER

Plataforma especializada en aportar información sobre ciberseguridad a la ciudadanía y a empresas, con el propósito de aumentar la cultura de la ciberseguridad. Siendo los principales objetivos del ObservaCIBER:

- Unir en un espacio común, con una identidad compartida, todos los estudios de ciberseguridad desarrollados por los organismos que participen en este proyecto.
- Impulsar la cultura de la ciberseguridad y su divulgación entre la ciudadanía, las empresas, y demás actores involucrados.
- Compartir conocimiento para facilitar un proceso de transformación digital más seguro y más fuerte.

Aportando estudios, informes, infografías, métricas y más, sobre la ciberseguridad en nuestro ecosistema. Gestionada por el INCIBE (Instituto Nacional de Ciberseguridad) y el ONTSI (Observatorio Nacional de Tecnología y Sociedad). Ambos dos pertenecientes al Ministerio de Asuntos Económicos y Transformación Digital.

10.6 Internet segura para niños

Internet Segura for Kids IS4K es el Centro de Seguridad en Internet para menores de edad en España y tiene por objetivo la promoción del uso seguro y responsable de Internet y las nuevas tecnologías entre los niños y adolescentes. Las principales tareas que tiene encomendadas son:

- Sensibilizar y formar a menores, jóvenes, familias, educadores y profesionales del ámbito del menor, a través del desarrollo de campañas, iniciativas y programas de ámbito nacional.
- Ofrecer un servicio de línea de ayuda con el que asesorar y asistir a menores, familias, educadores y profesionales del ámbito del menor sobre cómo hacer frente a los riesgos de Internet: contenidos perjudiciales, contactos dañinos y conductas inapropiadas.
- Organizar el Día de la Internet Segura (Safer Internet Day) en España.
- Reducir la disponibilidad de contenido criminal en Internet, principalmente de abuso sexual infantil, dando soporte a las FFCCSE (Fuerzas y Cuerpos de Seguridad del Estado).

Algunos de los medios que ponen a disposición de las familias son:

- El conocimiento de las mayores ciberamenazas a la que están expuestos los menores. Algunos ejemplos son: sexting, grooming, ciberacoso escolar, etc.
- Un apartado de utilidad donde encontrar, herramientas, material didáctico, catálogos, juegos, test, etc.

- Una sección de programas con jornadas y eventos.
- Un espacio de campañas para divulgación mediática.

10.7 Pantallas amigas

Pantallas amigas es una plataforma cuyo propósito es la promoción del uso seguro y saludable de Internet y otras TICs, así como el fomento responsable en la infancia y la adolescencia del uso de las tecnologías y la digitalización. Desarrollando proyectos y recursos educativos para la capacitación de niños, niñas y adolescentes de forma que puedan desenvolverse de manera autónoma en Internet, siendo el objetivo final que desarrollen las habilidades y competencias digitales que les permitan participar de forma activa, positiva y saludable en la Red.

Los pilares de actuación de esta plataforma son:

- La comunicación educativa.
- La educación en habilidades para la vida digital.
- La innovación.
- La transversalidad con otros aspectos educativos.
- La promoción de valores universales.

Y por supuesto cuentan con innumerables recursos, herramientas, servicios, canales de divulgación, etc.

Pantallas amigas desarrolla su actividad con el apoyo de entidades e instituciones comprometidas con este objetivo.

10.8 Foro Info Spyware

El Foro Info Spayware es una plataforma que lleva operando en internet desde el año 2005 y se trata de la mayor comunidad en español de ayuda e información sobre virus, spyware, adware, ransomware y malwares.

En este foro encontrarás toda la información por categorías:

- News: Las últimas noticias sobre seguridad, virus, antivirus, hacking, phishing, spam, ataques, timos, estafas, malware y otras amenazas de seguridad informática.
- Bienvenidos: Anuncios, conversación y discusión acerca del foro y la web. Su organización, cómo funciona y cómo mejorarla.

- Eliminar Malwares: Ayuda para eliminar virus, troyanos, spyware, adware, ransomware y otros malwares.
- Ayuda General: Esta categoría brinda ayuda general con el funcionamiento de los equipos (Windows, Mac, Linux, Android, iOS), programas (antivirus, firewalls, optimizadores) y componentes (hardware).
- Sistemas Operativos: Todo lo relacionado a los sistemas operativos: Windows 10 - Windows 8 - Windows 7 - Windows XP, Mac OSX, Linux, Android…
- Guías, manuales, tutoriales y más: Categoría en la que encontrarás guías de eliminación de malware para troyanos, adware, ransomware y otros tipos de códigos maliciosos de Windows. También encontrara manuales de antivirus, trucos, y otras recomendaciones de seguridad informática.

10.9 Fuerzas y cuerpos de seguridad del estado

En otras líneas de actuación con el propósito de velar por la ciudadanía en general, existen departamentos específicos contra los delitos informáticos de las fuerzas y cuerpos de seguridad del estado, como lo son:

- Brigada central de Investigación Tecnológica de la Policía Nacional (BCIT).
- Grupo de Delitos Telemáticos de la Guardia Civil (GDT).

Y en esta última, es donde debes interponer una denuncia en caso de ser víctima de algunos de los ciberdelitos que has podido ver en las unidades anteriores, accediendo desdes este enlace denuncia electrónica.

Además, es importante que puedas adjuntar la denuncia con pruebas, para ello, toma capturas de pantallas o cualquier prueba que pudiese ser relevante. Ten en cuenta, que si se trata de una prueba que pueda ser borrada por la persona que ha realizado el delito, necesitarás un testigo online o garante. Se trata de una entidad que certifica que ese delito fue cometido aun cuando ya no esté disponible en la red. En el siguiente enlace tienes una es estas entidades eGarante - testigo online

Bibliografía

Agencia española protección de datos (2021). *Oversharing o sobreexposición*.

Ambit (2020). Ciberinteligencia. *Ambit - Building solutions together*.

Avast (2018). Vpn o red privada virtual. *Avast*.

Avast (2020). Spyware o programa espía. *Avast*.

Avast (2021). Adware. *Avast*.

Blog de ayuda ley protección de datos - encriptación (2020). Cifrado de unidades del almacenamiento. *Ayuda ley protección de datos*.

Blogthinkbig by telefónica (2014). ¿qué son las cookies? *Blogthinkbig*.

Computer Hoy (2021). Brushing. *Computer Hoy*.

Cícero Comunicación (2021). Huella digital o reputación online. *Cicerocomunicacion*.

Enetic (2021). Diferencias entre firewall, antivirus, antispyware y antimalware. *Enetic Soluciones Tenológicas*.

ESET (2012). Malware qr. *ESET*.

ESET (2015). *Guia de privacidad en internet*.

ESET (2021). Juice jacking. *ESET*.

Fuentes de información (2016). La importancia de contrastar la información. *Fuentes de información*.

GCFGlobal (2021). Seguridad en internet. *Goodwill Community Foundation*.

Genbeta (2018). Guia para saber si me estan usando para minar criptomonedas en internet. *Genbeta*.

Genbeta (2021). El derecho de poder rechazar las cookies. *Genbeta*.

Google books (2021). Software alterado. *Google Books*.

Grupo Ático (2018a). Derechos arco. *Grupo Ático*.

Grupo Ático (2018b). Derechos pol. *Grupo Ático*.

INCIBE (2017). Vulnerabilidad. *INCIBE*.

INCIBE (2018a). *Estrategia copia de seguridad 3-2-1*.

INCIBE (2018b). Novias o novias de orígenes exóticos. *INCIBE*.

INCIBE (2020). Ganador sorteo o premios online. *INCIBE*.

INCIBE (2021a). Correos de sextorsión. *INCIBE*.

INCIBE (2021b). Smishing. *INCIBE*.

INCIBE (2021c). Warshipping. *INCIBE*.

INCIBE (2021d). ¿qué es un botnet? *INCIBE*.

INCIBE (2022). Whatsapp fraude familiar. *INCIBE*.

INCIBE (2023a). Estafas bizum. *INCIBE*.

INCIBE (2023b). Falsas ofertas de empleo. *INCIBE*.

INCIBE (2023c). Falsos alquileres. *INCIBE*.

INCIBE (2023d). Falsos préstamos. *INCIBE*.

Infospyware (2021). Phishing. *Infospyware*.

Innovation and Entrepreneurship Business School (2021). Cryptojacking. *IEBS*.

IONOS by 1and1 (2019). Nfc - comunicación de campo cercano. *IONOS Guía digital*.

IONOS by 1and1 (2020a). Bluetooth. *IONOS Guía digital*.

IONOS by 1and1 (2020b). Plugin, complemento o extensiones. *IONOS Guía digital*.

IONOS by 1and1 (2021a). Aviso legal. *IONOS Guía digital*.

IONOS by 1and1 (2021b). Política de cookies. *IONOS Guía digital*.

IONOS by 1and1 (2021c). Política de privacidad. *IONOS Guía digital*.

Kaspersky (2021a). Pharming. *Kaspersky*.

Kaspersky (2021b). Scareware. *Kaspersky*.

Kaspersky (2021c). Troyano o caballo de troya. *Kaspersky*.

Kaspersky (2023a). Doxing. *Kaspersky*.

Kaspersky (2023b). Sextorsión. *Kaspersky*.

Katemangostar - Freepik (2021). Imagen portada.

Mailfence (2020). Ataque quid-pro-quo. *Mailfence*.

Media Cloud (2021). Diferentes tipos de copias de seguridad. *Mediapro*.

Moodle-Universidad de Alicante (2021). Baiting. *Universidad de Alicante*.

Muy computer (2018). Navegación privada. *Muy computer*.

OEDI (2021). Estadísticas ciberataques. *Obsevatorio Español de Delitos informáticos*.

OSI (2015). Malvertising. *Oficina de seguridad del internauta*.

OSI (2019a). Deep web. *Oficina de seguridad del internauta*.

OSI (2019b). Frena y evita los bulos o fakenews. *Oficina de seguridad del internauta*.

OSI (2020a). Buenas prácticas contra los bulos. *Oficina de seguridad del internauta*.

OSI (2020b). Derecho al olvido. *Oficina de seguridad del internauta*.

OSI (2020c). Petróleo del siglo xxi. *Oficina de seguridad del internauta*.

OSI (2020d). Shoulder surfing. *Oficina de seguridad del internauta*.

OSI (2021a). Actualizaciones. *Oficina de seguridad del internauta*.

OSI (2021b). Crea tu contraseña segura. *Oficina de seguridad del internauta*.

OSI (2021c). Cuentas de usuario. *Oficina de seguridad del internauta*.

OSPI (2018). *Panorama actual de la ciberseguridad en España*.

Panda Security (2021a). Gusano informático. *Panda Security*.

Panda Security (2021b). Sim swapping o duplicación de tarjeta sim. *Panda Security*.

Panda Security (2021c). Virus informático. *Panda Security*.

Proofpoint (2022). spear phishing. *Proofpoint*.

Redeszone (2019). Formjacking. *Redeszone*.

Redeszone (2020). Descarga de software malicioso. *Redeszone*.

Redeszone (2021). Pretexting. *Redeszone*.

Unicef (2021). Ciberacoso. *Unicef*.

Valencia Plaza (2014). Decálogo para una buena reputación online. *Valencia Plaza*.

Wikipedia (2018). Autenticación de factor múltiple. *Wikipedia*.

Wikipedia (2020). Concepto de privacidad. *Wikipedia*.

Wikipedia (2021a). Clickjacking. *Wikipedia*.

Wikipedia (2021b). Contraseña o password. *Wikipedia*.

Wikipedia (2021c). Copias de seguridad. *Wikipedia*.

Wikipedia (2021d). Deepfake. *Wikipedia*.

Wikipedia (2021e). Dumpster diving. *Wikipedia*.

Wikipedia (2021f). Fake news. *Wikipedia*.

Wikipedia (2021g). Malware o software malicioso. *Wikipedia*.

Wikipedia (2021h). Meta datos. *Wikipedia*.

Wikipedia (2021i). Protocolo seguro de transferencia de datos https://. *Wikipedia*.

Wikipedia (2021j). Ransomware o software de secuestro. *Wikipedia*.

Wikipedia (2021k). Reglamento general de protección de datos. *Wikipedia*.

Wikipedia (2021l). Spam o correo malicioso. *Wikipedia*.

Wikipedia (2021m). Typosquatting. *Wikipedia*.

Wikipedia (2021n). Usurpación o robo de identidad. *Wikipedia*.

Wikipedia (2023). Timo nigeriano. *Wikipedia*.

Xataka (2019a). Borrado definitivo dispositivos de almacenamiento. *Xataka*.

Xataka (2019b). Sombra digital. *Xataka*.

Xataka (2020). Wps - wifi protected setup. *Xataka*.

Xie, Y. (2021). *Bookdown: Authoring Books and Technical Documents with R Markdown*. Chapman and Hall/CRC, Boca Raton, Florida, 2nd edition. ISBN 978-1138700109.