Seguridad, privacidad y seguridad

Conocimientos básicos | un módulo del proyecto CUMILA | www.cumila.eu

Impresión

Este documento forma parte del proyecto “CUMILA - Guía curricular para la alfabetización de los medios y la tecnología para adultos”.
Nombre del módulo: "Seguridad, privacidad y protección"
KA204-45D50F70
Más información en https://www.cumila.eu

Socios / Entidades que participan:
Medienkompetenz Team e.V.
Sophienstr. 120
76135 Karlsruhe – DE

Akademie für Politische Bildung und demokratiefördernde Maßnahmen
Hauptplatz 23
4020 Linz – AT

CIDET - Centre for the innovation and development of education and technology, S.L
Carrer Pintor Ribera 18
Entresuelo, local 3
12004 Castellón - ES

Sobre este módulo:
Organización responsable **CIDET**
Gráficos y diseño Ann-Kathrin Giuriato

Autores: Roger Esteller Curto, Daniel Nübling, Helmut Moritz

Cofinanciado por el programa Erasmus+ de la Unión Europea

Índice de contenidos

1. Identidad digital **4**
1.1 Nuestro segundo 'yo' 5
1.2 Confianza y seguridad 6
1.3 Fake identity 8
1.4 Vinculando las identidades 9
1.5 Alimentando las identidades 10
1.6 Pruebas de confirmación de identidad 11
1.6.1 Captcha 11
1.6.2 Cuenta de correo electrónico 12
1.6.3 Número de teléfono o tarjeta de crédito 13
1.6.4 Factor de autenticación doble 14
1.6.5 Certificados digitales 15

2. Mis datos, mis derechos **16**
2.1 Legislación Europea 17
2.1.1 Derecho de acceso 17
2.2 La protección de datos 22
2.2.1 De Safeharbour al Escudo de Privacidad UE-EEUU. 22
2.3 Consejos y recomendaciones 23

3. Riesgos y desafíos **24**
3.1. ¿Estamos realmente informados cuando damos nuestro consentimiento? 25
3.2 Las "Cookies" o galletas 27
3.3 Robo de identidad; phishing 29
3.4 Instalar apps, widgets y otras cosas 32
3.5 Acceso remoto 33
3.6 Los Antivirus 34
3.7 Dejar tus datos en la red, el "big data" 35
3.8 La Red profunda (deep web) y la red oscura (dark web) 36

4. Modelos de negocio Internet **38**
4.1 Publicidad oculta 39
4.2 Tus datos son muy valiosos 41
4.3 Leer no es gratuito 42
4.4 Servicios gratuitos, esperando a que te enganches 43
4.5 Ser creadores 44
4.6 Micro-pagamentos 45

1. Identidad digital

Hoy en día, casi todo el mundo tiene una identidad digital. Ya sea a través de una cuenta de correo electrónico, una cuenta en una red social o un canal de Youtube. Incluso aquellos que no están interesados en dejar su rastro en Internet, no pueden evitar que otra gente publique videos, fotos o que aparezca su nombre u otro tipo de información personal en la red. Teniendo en cuenta esto, podemos afirmar que aún sin tener Internet, puedes tener una identidad digital.

En este capítulo aprenderás acerca del sistema general para identificarte a ti mismo, a identificar la información personal que dejamos en Internet (ya sea de manera consciente o inconsciente) y finalmente, porque resulta interesante, a la par que arriesgado, para la gente y las organizaciones. Esto te ayudará a ser más consciente y por lo tanto, a proteger tu información y ser más cuidadoso cuando compartes información al mismo tiempo que, aumentará tu confianza y podrás sacar más provecho de las oportunidades y los servicios que ofrece Internet.

Identidad digital		
Entiende la importancia de la identidad digital cuando accede, crea o comparte contenido en Internet, también cuando se trata de uno mismo y es capaz de reconocer si las identidades de otras personas son falsas o fiables.		
Conocimientos	**Habilidades**	**Competencias**
Él/Ella • es consciente de las potencialidades y los riesgos que implica tener una identidad digital. • reconoce la necesidad de proteger e introducir su propia identidad digital. • conoce los métodos existentes para verificar una identidad.	Él/Ella puede • gestionar su propia identidad digital, y usarla según sus propósitos. • crear conexiones seguras entre identidades basadas en la confianza y el respeto.	Él/Ella es capaz de • crear, mantener y apoyar una identidad digital. • reconocer las identidades digitales de otra gente y filtrar aquellas identidades falsas.

1.1 Nuestro segundo 'yo'

Sherry Turkle, psicólogo, socióloga y profesora del MIT, en su libro "Second Self: Computers and the Human Spirit" intenta entender a la vez que explicar el impacto que tiene Internet en las personas y en la sociedad. Los ordenadores (móviles, tablets...) e Internet no se tratan de herramientas simples, nos ayudan a tener una proyección de nosotros mismos en los demás, dando forma, de esta manera, a nuestro sentimiento de identidad. Los estudios de Turkle así como de otros investigadores nos muestran la complejidad de la relación humano-máquina-humano y es que todo empieza cuando pasamos de ser simples lectores en Internet a participantes que crean su propia representación en Internet. El primer paso para nuestra representación visual es elegir el avatar o icono que las páginas web nos ofrecen la posibilidad de incluir en nuestra cuenta (como en Gmail, entre muchas otras). Lo que escogemos, una foto bonita de nosotros mismos en vacaciones, una foto de nuestro perro, una frase de uno de nuestros autores favoritos, etc. cualquiera de estas elecciones, ya está creando una nueva identidad.

En Internet, ahora es más fácil que nunca tener una segunda identidad, pero esto no quiere decir que esté mal o sea peligroso, sino que se tratan de nuevas maneras de hacer lo que nos gusta, tener más libertad, y permitir que nuestro desarrollo personal se beneficie de ello.

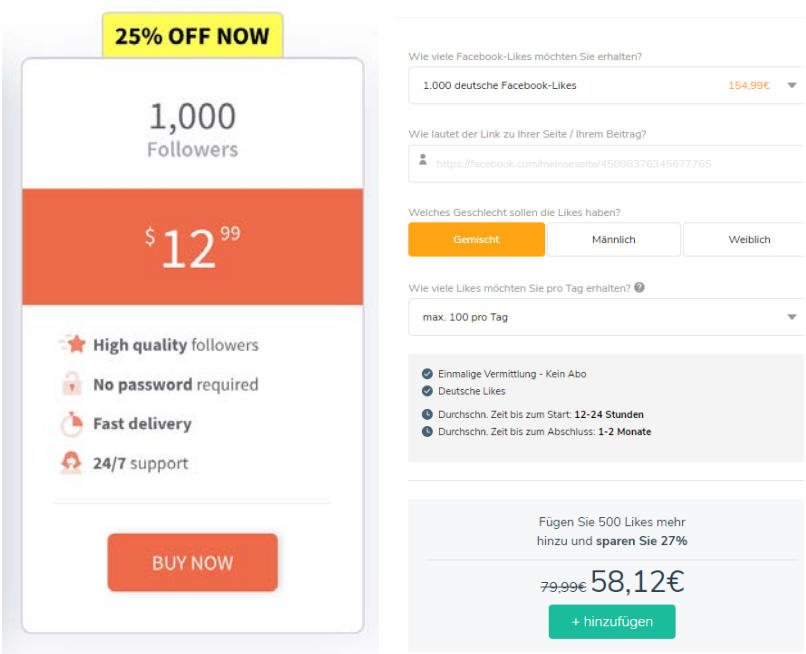
Dicha identidad puede empezar cuando creamos una cuenta e interactuamos con otros (como en el correo electrónico) y puede consolidarse incluso más cuando empezamos a publicar cosas (álbumes, blogs...) o participar en comunidades (como foros, redes sociales...). Es importante saber que nuestra identidad también se forma a través de la participación de otra gente, por ejemplo cuando alguien publica algo sobre nosotros, sube una foto y nos etiqueta o cuando una organización publica algo sobre nosotros (por ejemplo, si hemos sido seleccionados para cualquier tipo de proceso). Tenemos un cierto control acerca de la información que publicamos sobre nosotros mismos, pero no sobre la que el resto de la gente publica sobre nosotros. Por esta razón, hay mucha gente que se niega a estar en Internet y que no quiere tener ninguna cuenta ya que no quieren que nadie les reconozca. Nuestro consejo para esta gente es que si esta es la única razón por la que no quieren digitalizarse, entonces no solamente están perdiendo un montón de oportunidades, sino que a la vez, están dejando que sean otros los que construyan su identidad.

El "Segundo yo" se entiende como el construir una nueva identidad que puede ser distinta de la primera (la real). Las personas pueden tener más de una identidad, y algunas de estas puede que incluso no tengan relación con la realidad. No pienses que esto es un fraude o una forma de estafar a los demás, sino que se trata de una forma de ganar una libertad que sería difícil de conseguir en nuestra vida real. Internet permite crear nuevas identidades que pueden ser más fieles a nuestra forma de pensar que nuestro verdadero yo.

1.2 Confianza y seguridad

Para los que temen ser engañados por alguien en Internet que se haga pasar por nuestro personal bancario, nuestro agente de seguros, un funcionario de Hacienda del gobierno, o incluso alguien que conocemos (como un amigo o miembro de nuestra familia) sólo hay que recordar una cosa: "no te fíes de nadie". Este principio se aplica incluso a los correos que recibes de tus amigos, presumiblemente. De hecho, este es el caso de una táctica de estafa común que se aplica cuando alguien puede sustituir a tu amigo en un correo electrónico, y te pide dinero porque le han robado estando en un país extranjero. Esa persona puede incluso intentar convencerte mencionando algo personal o íntimo. En primer lugar, recuerda que ninguna red social o sistema de correo electrónico proporciona un método para garantizar la identidad del remitente, de hecho es muy fácil enviar un correo electrónico en nombre de otra persona. En segundo lugar, el hecho de que otras personas conozcan algo personal no es una garantía segura, recuerda que hoy en día hay mucha información sobre nosotros en la red. Simplemente, si alguien te pide algo inusual, lo primero que debes hacer es sospechar.

Siento decirlo... pero en Internet no te puedes fiar ni de un correo electrónico que hayas recibido de tu amigo. Los correos electrónicos no son difíciles de suplantar, lo mismo que el correo postal, lo único es que no estamos acostumbrados a recibir el correo habitual.



Pagando casi 13$ puedes conseguir 1.000 seguidores en Instagram (izquierda) o si lo que buscas es conseguir 100 likes en tu cuenta de Twitter, lo puedes tener por 4$ (derecha).

Hay personas que crean muchos perfiles o cuentas , como diez, cien o mil cuentas. En ese caso, estas cuentas están creadas a partir de procesos automatizados. El objetivo de eso es “vender personas" que luego puedan dar su opinión o votar en un lugar. Es decir, imagina que tienes un restaurante y necesitas tener votos positivos, entonces puedes crear diez cuentas de correo electrónico y esas personas podrían luego votar y dejar una buena opinión acerca de tu restaurante. Por supuesto, hay métodos para tratar de evitar estos perfiles falsos (lo verás en la siguiente sección), pero aún así debes ser consciente que esto ocurre. Otro ejemplo: eres un político que tiene pocos seguidores en una red social, hay sitios web donde puedes comprar cientos o miles de cuentas y entonces todos esos perfiles fantasmas pueden apoyarte, aumentando así tu reputación. Cuando un perfil o página tiene más referencias o seguidores, entonces es más probable que aparezca en la página de resultados de Google o en las noticias.

1.3 Fake identity

No porque recibas un correo electrónico de una persona que tiene el nombre y el apellido de tu hermano significa que sea tu verdadero hermano. Lo mismo ocurre con las redes sociales y otras plataformas de comunicación o publicación de medios. Crear un perfil en una página web con la foto y el nombre y apellido de alguien que conoces no significa que seas esa persona.

Por ejemplo; los políticos más famosos del mundo tienen cuenta de Twitter, pero hay decenas de cuentas de twitter con el mismo nombre (realmente es un nombre ligeramente distinto pero que parece el mismo). Nunca hay que fiarse de un mensaje o comentario de una persona, sólo el tiempo puede proporcionar esa confianza, y aún así a veces podemos encontrarnos con la situación de que nos roben o toparnos con una cuenta robada. ¿Te creerías una carta de un amigo pidiéndote dinero? Aunque esa carta esté firmada... o incluya alguna referencia personal..., seguramente sospecharas, y por si acaso para asegurarte, llamarás a tu amigo para comprobar que todo está bien. Depositamos demasiada confianza en las identidades digitales en Internet, y las redes sociales y plataformas mediáticas son para la comunicación informal y el entretenimiento. Sólo merecen confianza los canales de comunicación oficiales que están verificados (como los del gobierno o los servicios públicos).

Como conclusión, sé cauto la primera vez que alguien te agregue en una plataforma social o te contacte por correo electrónico. Incluso si le conoces. Y si algún contacto te envía algo inapropiado, antes de pensar que se ha vuelto loco, pregúntate: ¿lo está escribiendo él/ella realmente?

1.4 Vinculando las identidades

Es evidente que los contenidos en Internet son creados por personas: las noticias, mensajes, imágenes, etc. por lo que la confianza en el mensaje está marcada por la confianza que tenemos en su autor. Los vínculos de confianza se crean mediante la vinculación de identidades: es como el dicho popular "los amigos de mis amigos son también mis amigos", en este sentido los canales de confianza son los mejores métodos para avalar la identidad. En este aspecto, la identidad está avalada por la comunidad.

Basándonos en el ejemplo del apartado anterior: Supongamos que una persona que tiene el nombre y el apellido de nuestro hermano solicita nuestra amistad en una red social y nosotros aceptamos. Más tarde vemos que esta persona no tiene ningún otro amigo en común, entonces podríamos empezar a sospechar. Obviamente alguien que se identifica como nuestro hermano ha encontrado nuestro perfil siguiendo un vínculo común (por ejemplo, trabajo, gimnasio, asociación, academia, etc). That is a profile we would very much like to explore.

Los vínculos entre identidades proporcionan ahora una forma de asegurar la identificación (no completamente segura, pero sí en un alto grado). La confianza se basa en el enlace y en la comunidad, es decir, en el grupo. Sólo en esta circunstancia nuestra identidad se verifica en ambos sentidos.

En segundo lugar, la vinculación entre identidades permite encontrar a otras personas y compañeros que conocemos en la vida real, pero con los que no hemos tenido ningún contacto virtual. Al vincular las identidades también podemos encontrar contenidos interesantes en Internet. Por ejemplo: Me gusta un grupo de música local, he encontrado a alguien a quien también le gusta esa música, por lo tanto, probablemente, también me gustará la música que le gusta a esta persona. De este modo, estamos creando canales que van más allá de la confianza, que son maravillosos para conocer y descubrir cosas nuevas. Antes teníamos que usar Google para buscar las cosas que nos gustaban, a partir de ahora, podemos descubrir cosas nuevas siguiendo lo que les gusta a nuestros amigos..

1.5 Alimentando las identidades

Al nutrir nuestra identidad nos referimos a decir lo que nos gusta, lo que no nos gusta, subir imágenes o reenviar mensajes. Esto se basa en los principios de "Vinculación de identidades" que hemos visto en la sección anterior y el mismo ejemplo del amigo al que le gusta el mismo grupo de pop que a nosotros. Haciendo visibles nuestros intereses o lo que creamos que nos identifica también estamos ampliando nuestras conexiones. Esto amplía enormemente nuestros grupos virtuales.

Otro ejemplo: te encanta caminar por la montaña, has encontrado una web que muestra senderos de un parque natural que te gusta mucho. Decides publicar en tus redes sociales una foto de una ruta preciosa que hiciste la semana pasada. Al hacerlo estás haciendo crecer tu identidad, estás diciendo que te gusta caminar por la montaña, y también que te encanta ese parque natural. Además, decides poner un comentario en la web del parque natural dando alguna recomendación y sugerencia sobre un lugar. Otra persona puede leer ese comentario y empezar a seguirte en alguna red social. Este vínculo es bidireccional y entonces los dos podéis empezar a seguir las aventuras del otro, descubriendo nuevos lugares para caminar y ayudándoos mutuamente.

Ser amigo de alguien en la vida real es muy distinto de ser amigo de alguien en Internet. En Internet podemos tener amigos basados simplemente en intereses. Por ejemplo, colegas cuyos nombres reales ni siquiera conocemos pero compartimos una afición. Internet permite este tipo de relación y es maravilloso ya que nos permite estar en contacto, compartir, descubrir, aprender, crear y disfrutar con el único vínculo de un objetivo común.

No malinterpretes nuestro objetivo, probablemente nunca os conoceréis ni os veréis cara a cara. Ese vínculo solamente está basado en vuestro interés por el senderismo y nada más. Esta es la gran ventaja de Internet: sus posibilidades de conectividad en cualquiera de las comunidades sociales que existen (comunidades basadas en aficiones, imágenes generales, trabajos, etc). Siempre y cuando no publiques información personal o privada, verás como ser activo en Internet, crear contenidos y hacer crecer tu identidad con tus aficiones y lo que te gusta será gratificante, ya que recibirás feedback y esto enriquecerá tu experiencia a la vez que ayudarás a los demás.

1.6 Pruebas de confirmación de identidad

Las organizaciones se esfuerzan por minimizar el uso de perfiles o cuentas masivas (aquellas creadas con el propósito definido en el apartado anterior). Algunos de los métodos utilizados para controlarlo son los captchas, otros correos electrónicos o números de teléfono.

1.6.1 Captcha

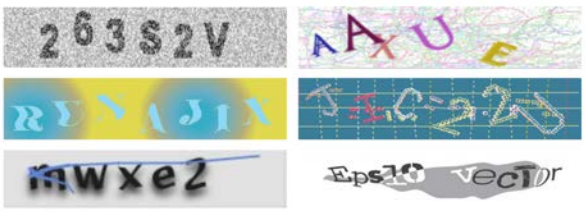
CAPTCHA en inglés significa Completely Automated Public Turing test to tell Computers and Humans Apart. Los captchas son un enrevesado grupo de letras que los sitios web muestran para asegurarse de que somos humanos. Se trata de escribir en un recuadro las letras y números que leemos. Se supone que ningún proceso automatizado puede leer e identificar los símbolos. De este modo, los sitios web evitan las cuentas masivas o los mensajes masivos.

Esto es un captcha, se supone que solamente los humanos pueden leer y escribir lo que está escrito aquí.

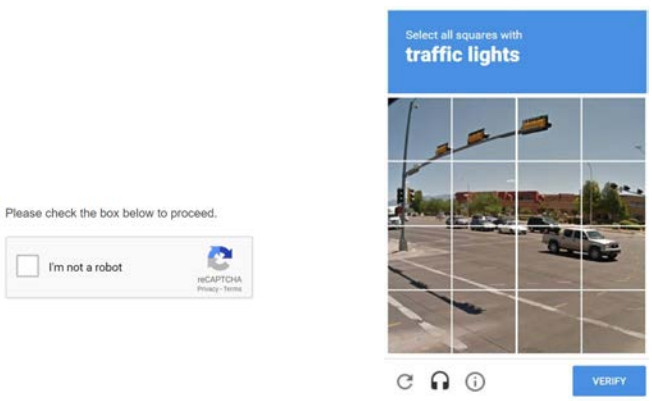
Los captchas pueden ser muy molestos, pero es la única forma de evitar el abuso y el uso inadecuado de muchas páginas web, por ejemplo cuando pides un presupuesto en una web, o intentas reservar un asiento. Imagina que en lugar de ti, fuera un proceso automático: el que llena el buzón de cotizaciones falsas o el que reserva todos los asientos en un espectáculo. Por lo tanto, los captchas también están para protegernos.

Los captchas, sin embargo, sólo impiden el proceso automatizado. Sin embargo, un estafador (humano) puede crear una cuenta con un nombre falso y hacerse pasar por otra persona.

El test de Turing, originalmente llamado juego de imitación por Alan Turing en 1950, es una prueba de la capacidad de una máquina para mostrar un comportamiento inteligente equivalente o indistinguible del de un humano. Por lo tanto, una Captcha es una prueba para asegurar que quien está accediendo es humano.



Esto es un captcha, se supone que solamente los humanos pueden leer y escribir lo que está escrito aquí.



Otro método de captcha; identificar elementos en una foto (semáforos)

1.6.2 Cuenta de correo electrónico

Cuando creas una cuenta en un sitio (en un foro, para una encuesta, una tienda...) te piden una dirección de correo electrónico. Esto es, por supuesto, para obtener tu dirección de contacto, enviar promociones u otra información, pero también para comprobar la veracidad de tu identidad. Es habitual que esos sitios web te envíen un correo de confirmación que tienes que verificar. Esa verificación se hace asegurando que sólo el legítimo propietario de la cuenta de correo electrónico podrá hacer clic en el enlace que hay en el correo. Si alguna vez intentas registrarte en el mismo sitio (es decir, en el mismo foro, rellenar la misma encuesta o en la misma tienda) te saldrá un error diciendo que ya estás registrado y te invitará a recuperar tu contraseña si no la recuerdas.

1.6.3 Número de teléfono o tarjeta de crédito

Cada vez son más los sitios web que piden el número de teléfono o la tarjeta de crédito. Verifican que eres el propietario del número enviando un mensaje con un número que tienes que rellenar de vuelta. También es posible autorizar tu tarjeta de crédito (sin proceder a un pago). Los números de teléfono en la Unión Europea siempre están relacionados con una persona, lo mismo ocurre con las tarjetas de crédito. Así, el hecho de que algunos servicios en línea requieran su número de teléfono es también una forma de asegurarse de que hay una persona que lo solicita. Servicios como Gmail o Twitter piden cuentas de correo electrónico y números de teléfono como forma de asegurarse, por lo que cada vez es más habitual que las webs soliciten tu número de teléfono.

Debes tener cuidado con las condiciones de privacidad de la web y no facilitar el número de teléfono a no ser que estés seguro de que van a hacer un uso legítimo. En caso de duda, no lo des. Si es posible, pregunta a una persona con más experiencia.

1.6.4 Factor de autenticación doble

Normalmente, los sitios web utilizan el nombre de usuario y la contraseña para asegurarse de que eres el único que utiliza tu cuenta. Esto suele ocurrir con las cuentas de correo, en bancos, tiendas, etc. La autenticación de dos factores (2FA) añade una doble capa de seguridad. Desde 2019, la directiva de la Unión Europea obliga a utilizar la autenticación de dos factores en los servicios de pago, y cada vez más servicios (no solo relacionados con los pagos) también la utilizan.

El primer factor de autenticación es el nombre de usuario y la contraseña. El segundo puede ser un mensaje al móvil, un número de una coordenada determinada que sólo tienes tú, o un código generado por una App que puede estar almacenado en tu ordenador o móvil. El fraude en la autenticación se minimiza incluso tratando de adivinar los intentos de inicio de sesión sospechosos. Por ejemplo, si las últimas cien veces que te has conectado a tu cuenta de correo ha sido desde París, si estás de vacaciones e intentas abrir tu correo, el sistema lo percibirá como un intento sospechoso y te pedirá alguna verificación extra, como tu fecha de nacimiento, un correo, o cualquier otro dato que se supone que sólo tú puedes saber.

Por lo tanto, no deberías sorprenderte por estos pasos o procesos, a veces, molestos. Son para tu seguridad y para evitar que alguien más acceda a tus datos.

La autenticación de factor doble es obligatoria para muchos servicios, uno de ellos es el pago con tarjeta de crédito a través de Internet, hoy en día, en la UE, es obligatorio que el comercio se asegure de que se trata de un uso legítimo de la tarjeta de crédito solicitando otra forma de verificación, como un mensaje a nuestro móvil.

1.6.5 Certificados digitales

Varios países europeos facilitan identificaciones digitales. Es decir, de la misma manera que los pasaportes o los documentos de identidad nos identifican al cruzar fronteras, ir al banco o hacer nuestra inscripción en una academia, lo mismo ocurre en el mundo virtual. Cada vez más, las personas y organizaciones realizan procesos administrativos con el requisito de ir al mostrador y mostrar nuestro DNI y nuestra firma. En el mundo virtual, las identificaciones digitales hacen esa función. Estos métodos de identificación pueden utilizarse para reconocernos y firmar documentos electrónicos. La iniciativa de la Unión Europea de unificar las identificaciones nacionales está establecida en el reglamento 910/2014, y esperemos que pronto empecemos a ver más implementaciones de esta solución.

Las firmas digitales podrían ser la solución a los correos electrónicos falsos, a la pérdida de identidad en los sitios web y a las transacciones seguras, pero su uso no está muy extendido, ya que requieren un hardware adicional (en el caso de las tarjetas) o una configuración informática. Afortunadamente, las cosas están empezando a ser más amplias y comunes.

Si dispones de una identificación digital puede que entonces ya sea innecesario usar nombres de usuario y contraseñas en los bancos, tiendas u otros sitios web que requieran nuestra identificación. Así, nuestra identificación se verificaría con esa tarjeta. Además, en caso de transacciones (pagos con tarjeta de crédito, firma de formularios, etc.) no sería necesario firmar un papel de forma presencial. Estos métodos también proporcionan una capa extra de seguridad, ya que las firmas manuscritas pueden ser falsificadas. Una firma digital puede verificarse inmediatamente, por lo que también es imposible modificar los datos del documento sin que la firma quede invalidada.

Podría parecer que todo son ventajas, y en algunos aspectos es así, pero recuerda que los DNIs digitales vendrían a ser algo parecido a lo que en la vida real son los DNIs. Te proporcionan la seguridad de quien está haciendo una transacción (como comprar algo, o pagar...), tener un DNI no significa que no debas ser prudente ya que la otra persona puede seguir engañándote (como pasa en la vida real), ahora tendrás la certeza al menos de saber a quien denunciar a la policía (y es una gran ventaja en seguridad en Internet nunca antes).

Teclado que incluye un lector de tarjetas. La tarjeta incluye un chip que almacena nuestra identificación digital

2. Mis datos, mis derechos

Sin duda, tus datos personales son tuyos (tu nombre, fecha de nacimiento, lugar donde vives, cosas que compras, películas que ves, hoteles que reservas, restaurantes que visitas, etc). La mejor práctica es proporcionar esa información sólo cuando sea necesario y ése es también el principio que dirige la normativa actual: cualquier sitio web, persona u organización sólo debe pedir, conservar y procesar los datos necesarios para realizar la actividad o el servicio que usted solicitó. Un ejemplo de ello sería solicitar su dirección particular en caso de que quiera que se le entregue un paquete en su lugar de residencia. También el uso de cookies (de las que hablaremos más adelante), sólo debe recogerse y tratarse cuando sea necesario; por ejemplo, para mantener sus artículos en la cesta mientras compra en línea, o cuando abre de nuevo el navegador, para que los artículos que había recogido permanezcan allí.

Las organizaciones en Internet están recopilando sus datos personales. A veces lo hacen de forma consciente, en otros casos lo hacen sin un consentimiento explícito o, al menos, sin indicar claramente las implicaciones que podría representar para su privacidad e identidad. ¿Por qué es tan importante esta información para las organizaciones? ¿Qué van a hacer con ella? ¿Debemos preocuparnos?

Mis datos, mis derechos		
Conocer los derechos de información personales y ejercer esos derechos.		
Conocimientos	**Habilidades**	**Competencias**
Él/ella • conoce la legislación vigente relacionada con los datos personales. • entender los formularios de consentimiento y el significado de términos como tratamiento de datos o cancelación • conoce los riesgos de facilitar datos fuera de la UE	Es capaz de • localizar y acceder a la información de las organizaciones para acceder a sus regalos • acceder o solicitar datos personales almacenados por una organización	Puede • proteger y ejercer sus derechos

2.1 Legislación Europea

La Carta de Derechos Fundamentales de la UE (anunciada en 2000 en Niza, actualizada en 2012) estipula que los ciudadanos de la UE tienen derecho a la protección de sus datos personales, en este sentido la normativa se ha adaptado también al mundo digital para proteger nuestros derechos.

En las siguientes secciones te mostraremos los detalles del GDPR de la UE, destinados a proteger los derechos de los ciudadanos. El GDPR (Reglamento General de Protección de Datos) fue legislado por la Unión Europea en 2016 y entró en vigor en mayo de 2018. Representa la regulación más ambiciosa en materia de protección de datos. Obliga a las organizaciones a solicitar su consentimiento explícito sobre cómo se utilizarán sus datos y también te permite ejercer tus derechos de manera fácil.

Sin embargo, hay que seguir preguntándonos: ¿con quién estamos compartiendo nuestros datos? Y para ser más precisos, en lugar de preguntarse a quién se comparten los datos, la pregunta más precisa debería ser: ¿dónde se encuentra esa empresa?

Las empresas que almacenan y procesan nuestros datos personales deben estar ubicadas en la Unión Europea (o en terceros países con acuerdos). Esto hace posible que las empresas se ciñan a la legislación correspondiente y podamos estar seguros de que nuestros datos están bajo el paraguas legal de la UE. Por otro lado, si envías tus datos a un sitio web cuya sede principal está fuera de la UE, entonces tus datos podrían ser procesados sin control. Hoy en día, las empresas más importantes, como Google, Facebook, Twitter, etc., pueden tener delegaciones en países de la UE o al menos, sus países tienen un acuerdo con la UE.

2.1.1 Derecho de acceso

Tienes derecho a saber cuales son los datos que la empresa sabe sobre ti. A continuación, el ejemplo de Google, estos iconos están disponibles cuando te conectas en https://myaccount.google.com y vas a la sección "Datos". Cada icono te permite saber qué datos conoce Google sobre tus búsquedas, lugares, suscripciones o vídeos subidos a youtube, correos, eventos, aplicaciones, etc.

Las secciones anteriores permiten conocer lo que Google sabe de usted.

En caso de que quieras saber lo que otras organizaciones saben de ti y no haya un lugar claro para obtener esa información, puedes ponerte en contacto con la organización y solicitar esa información.

Ese derecho de acceso incluye el derecho a corregir sus datos. Por ejemplo, si un sitio web almacena tu apellido con un error ortográfico, puedes solicitar su corrección. Los datos son tuyos, literalmente, eso significa que no pueden obligarte a mantener un servicio porque son los dueños de tus datos. Esto facilita la transferencia de tus datos de una empresa a otra, por ejemplo si cambias de compañía de telecomunicaciones o de proveedor de internet y quieres mantener tu número de móvil.

El derecho a ser olvidado

En el apartado anterior hemos visto el control que tenemos sobre los datos que publicamos, pero ¿qué ocurre con los datos que otras personas publican sobre nosotros? o con los datos que se publicaron con nuestro consentimiento, pero que unos años después queremos eliminar? El "derecho de supresión" está presente en el GDPR, pero se debe examinar más detalladamente,, ya que es importante señalar que también debemos tener control sobre aquellos datos personales que no han sido creados por nosotros mismos.

Puedes solicitar que se elimine cualquier información pública o privada que contenga datos personales. Un ejemplo sería cuando apareces en el sitio web de otra persona, cuando quieres eliminar tu cuenta de Facebook o Google.

A continuación se muestra un ejemplo de las posibilidades que ofrece Google para eliminar sus cuentas. Está en myaccount.google.com, sección "Datos", subsección "Descargar, borrar o crear un plan para los datos".

Estos son los iconos de Google para borrar un servicio de Google o tu cuenta completamente, también para descargar tus datos

Si los datos se almacenan en el lugar de otra persona (como en un muro de Facebook, o un vídeo de Youtube) aún puedes denunciar la publicación o el vídeo como inapropiado o ilegítimo. Esto inicia un procedimiento no formal para ayudar a esas organizaciones a eliminar el contenido ilegal, aunque puedes iniciar un procedimiento formal poniéndote en contacto con ellas (observa la sección siguiente sobre cómo contactar con el responsable de un sitio web).

El derecho a ser informado

Cuando se recogen los datos, se debe informar claramente de algunos datos básicos.
Dos ejemplos siguientes. Hemos reproducido a christ the redeemer in the studio
El derecho a ser informado incluye la obligación por parte de la organización de explicar las cosas con claridad, evitando ambigüedades o abusos de tu confianza.

También requiere que se acepte de manera explícita, es decir, la casilla no puede estar marcada por defecto.

Área	Ejemplo
Consentimiento informado	"Acepto aparecer en fotos y vídeos y que se publiquen en Internet y otros medios"
Qué	Imágenes que se sacarán durante el aprendizaje
Quién es la entidad responsable del tratamiento de datos	English Academy (Academia de inglés)
Cuál es la finalidad del tratamiento de datos	Promoción de actividades extraacadémicas en las redes sociales
Por qué esta solicitud es legítima	Consentimiento por parte del participante
Sitio donde ejercer tus derechos	Puedes acceder a tus derechos en la Plaza del Emperador, 1, 12.345 Roma o por correo peticiones@romeacademy.it

El derecho a ser informado incluye la obligación por parte de la organización de explicar las cosas con claridad, evitando ambigüedades o abusos de tu confianza. También requiere que se acepte de manera explícita, es decir, la casilla no puede estar marcada por defecto.

Otro ejemplo que no requiere el consentimiento informado sería:

Área	Ejemplo
Consentimiento informado	(ninguna, no hay ningún tipo de consentimiento)
Qué	Información fiscal, incluyendo nombre, apellido y dirección.
Quién es la entidad responsable del tratamiento de datos	Academia de Inglés
Cuál es la finalidad del tratamiento de datos	Contabilidad
Por qué esta solicitud es legítima	Exigido por la normativa fiscal sobre la contabilidad de las entidades privadas
Sitio donde ejercer tus derechos	Puedes acceder a tus derechos en la Plaza del Emperador, 1, 12.345 Roma o por correo peticiones@romeacademy.it

En los campos de arriba puedes observar claramente qué y por qué necesitan tus datos. Pueden solicitar tu consentimiento o si algo es obligatorio, tu consentimiento está implícito, entonces sólo se te informa. También se indica claramente un lugar donde acceder a tus derechos. Las peticiones en los campos anteriores deben

ser razonables, es decir, que aunque nos des tu consentimiento, esto podría ser considerado ilegal por ser un abuso:

Área	**Ejemplo**
Consentimiento informado	Sí, lo acepto todo
Qué	Todos los datos que proporcione
Quién es la entidad responsable del tratamiento de datos	Academia de Inglés
Cuál es la finalidad del tratamiento de datos	Para compartirlo con nuestros compañeros
Por qué esta solicitud es legítima	Nos diste permiso
Sitio donde ejercer tus derechos	peticiones@romeacademy.it

Los campos anteriores son un abuso porque no indican a qué datos se refieren (está escrito de forma demasiado ambigua), y además... ¿por qué los datos van a compartirse con los socios? ¿Quiénes son? También deben proporcionar una dirección física para ejercer sus derechos, de hecho, tener una dirección de correo electrónico es opcional, pero deben tener una oficina en la UE.

Tus derechos versus lo imposible

En los apartados anteriores has observado tus derechos, pero también debes ser consciente de que todavía hay algunos derechos que se equilibran del lado de las empresas o, al menos, que les permiten hacer su trabajo de protección más realista. La ley se refiere a que las empresas deben tomar "medidas razonables" para proteger tus datos, y tratar de satisfacer tus peticiones "sin esfuerzos desproporcionados" o denegar las solicitudes cuando "no exista otro motivo legal para el tratamiento". También debes estar preparado para que algunas de tus solicitudes se queden sin atender, no porque la empresa no quiera cumplir tus deseos, sino porque puede ser técnicamente tan difícil que resulte casi imposible.

Un servicio completamente seguro sería tan caro que es casi imposible de proporcionar. Todo el mundo acepta el "esfuerzo razonable", y tu también debes entender que aunque tengas tus derechos, algunas cosas son imposibles y por lo tanto, tus derechos puede que se apliquen completamente.

Todo el mundo sabe, porque ha aparecido en las noticias, que incluso las empresas más seguras y hasta los gobiernos están expuestos al robo de datos. La seguridad al 100% nunca existe, de la misma manera que algunas rupturas de privacidad y errores humanos ocurren, y en segundo lugar, tampoco existen garantías al 100% sobre la privacidad y la seguridad. A continuación, vamos a mostrarte dos ejemplos:
Estos son los ejemplos que más cuentan para hacer este tipo de cosas pero no sé que es lo que esta pasando en realidad.

Primero imagina que solicitas a una plataforma social que elimine todos los mensajes, fotos y vídeos que citen alguna referencia a ti o muestren tu cara. Es técnicamente imposible estar seguros de eliminar cualquier referencia a ti, foto o vídeo en el que aparezcas, su mejor esfuerzo sería eliminar una lista de vídeos si les proporcionas esa

lista, pero también en el caso de que no haya ningún otro derecho de la otra persona anulado (por ejemplo si apareces en un evento público de otra persona grabando). Y aunque pudieran borrar ese contenido, no hay garantía de que la otra persona no suba inmediatamente una nueva foto tuya.

Un segundo ejemplo podría ser una encuesta anónima. La organización puede hacer todo lo posible por anonimizar la respuesta de esa encuesta no guardando ninguna información personal suya, pero en el mundo de Internet todo queda registrado y técnicamente (con un gran esfuerzo) es posible rastrear el origen de cualquier información.

Con los ejemplos anteriores no pretendemos hacerte sentir inseguro, pero hay algunas cosas que se escapan de la ley y de la organización de las empresas. Debes ser consciente de ello.

Contacto y responsabilidades

Casi todos los sitios web ofrecen una forma de ponerse en contacto con ellos. Debe buscar una dirección de correo electrónico, un formulario de contacto u otros datos (como teléfono, dirección, etc.). Seguramente deben tener una página de "Política de privacidad" o "Términos legales" o algo similar, donde describan lo que hacen con los datos que recogen y proporcionen los datos de contacto. Y luego deben proporcionar la forma oficial de dirigirse a ellos.

Si sientes curiosidad busca en un buscador web las últimas o más altas multas por demandas GDPR.

Para una empresa, no responder o satisfacer los derechos del consumidor, puede terminar con una enorme multa. Hasta ahora (2020), la mayor multa ha sido de 50 millones de euros, a Google, 35,2 M.€ a H&M o 27,8M. a TIM Telecom, y la más pequeña 90 € a un hospital en Hungría o 48€ a la Policía de Estonia. La mayor multa a Google se debió a la falta de información o al tratamiento de datos sin el consentimiento del consumidor. En el caso de H&M se trató de un error técnico que hizo pública información privada de todos los miembros de la empresa. La multa no se debió a ese error técnico, sino a que luego se descubrió que H&M estaba recopilando datos personales sensibles de sus empleados a través de campañas de cotilleos y otras fuentes para crear perfiles de los empleados y utilizar esos datos en el proceso de contratación. La multa de TIM se debió a un conjunto de razones; desde la recogida inadecuada de consentimientos hasta la retención excesiva de datos. El ejemplo del Hospital se debió a que el hospital cobró una cuota a un paciente pero no proporcionó la causa ni el resultado (el derecho a acceder a los datos). En el caso de la Policía de Estonia fue porque un agente de policía utilizó la base de datos de la policía para actividades de investigación privadas (uso indebido).

2.2 La protección de datos

Es casi imposible poner barreras a Internet, sólo unos pocos países en el mundo tienen filtros estrictos sobre los datos que entran y salen a través de sus fronteras, para el resto de la mayoría de los países es imposible restringir los negocios o el intercambio de datos. Hoy en día podemos comprar en una tienda o utilizar un servicio web que está en otro continente, no ser conscientes de ello puede ponernos en riesgo. No hay ningún problema en comprar un gadget en Hong-Kong (esto es sólo un ejemplo) siempre que sepamos que lo estamos haciendo, y algunos de nuestros derechos como consumidores podrían verse debilitados. Crear un blog, o un perfil en un servidor que está en otro país afecta también a nuestros derechos de tratamiento, acceso y corrección de datos. Como ya se ha dicho, no dude en utilizar sitios de otros países, pero tenga siempre cuidado. Como es bastante difícil estar seguro de dónde se encuentra una organización, no recomendamos centrarse en el lugar del servidor en el que está haciendo negocios, aconsejamos confiar en la organización; ¿es fiable? ¿tiene buena reputación? ¿es mundial? ¿has oído hablar de ella en foros u otros lugares? ¿qué piensa la gente? De hecho, en otros países del mundo existe una protección de los datos y de los usuarios similar a la de la UE.

2.2.1 De Safeharbour al Escudo de Privacidad UE-EEUU.

En un mundo donde las organizaciones son globales (como Facebook, Twitter, Google...) la protección de datos debe darse desde una perspectiva global; los acuerdos entre países y áreas económicas hacen posible el intercambio de nuestros datos personales con garantías.

Safeharbour fue el primer marco legal que se originó para regir el intercambio de datos entre países, asegurando que los datos personales serían tratados y procesados con la misma garantía, asegurando también que cualquier petición y queja sería atendida, acuerdos que ahora han sido sustituidos por el Escudo de Privacidad. El hecho es que hoy en día muchos otros países ofrecen una buena seguridad y no debe haber razón para preocuparse, al menos, no más de lo necesario, de todas formas, trata de seguir los consejos de la siguiente sección:

2.3 Consejos y recomendaciones

Existen dos grandes tipos de sitios web basados en el origen de los datos y la finalidad del tratamiento, por lo que debemos considerarlos de forma separada.
El primer grupo son las organizaciones gubernamentales y públicas, y también las privadas como bancos, universidades, servicios sanitarios, administración fiscal, etc. Los sitios web que prestan este tipo de servicios deberían considerarse los más seguros de todos. De todos modos hay que tener cuidado, ¡no olvides leer sobre el phishing! Este es un riesgo real que se origina por la confianza que damos a ciertos sitios web u organizaciones, pero recibimos un mensaje o vemos una página que simula ser esa organización.
Es el caso de ese tipo de organismos gubernamentales, públicos o privados con alto grado de confianza en que nuestros registros sanitarios, académicos, contables, etc. estén seguros. Se espera (y también lo garantiza la normativa de la UE) que el riesgo sea mínimo.

En cuanto a las tiendas u otro tipo de comercios, reservas de servicios online, compra de entradas, etc., debes seguir un proceso cuidadoso (al menos la primera vez que compres o utilices el servicio). A menos que adquieras suficiente experiencia, es mejor que te limites a tiendas que también tengan un comercio físico, teatros, cines u otro tipo de establecimientos en los que puedas adquirir los bienes o los servicios también físicamente o tengas algún lugar donde puedas pedir ayuda o verificar el proceso. Por supuesto, cuando adquieras más confianza, comprar y reservar será más rápido, fácil y no tan estresante.

Al publicar cosas (como vídeos, fotos, textos) en blogs, foros, redes sociales, etc. El principio fundamental es que no debes publicar nada que no quieras que sea público. Por supuesto, hay redes sociales que permiten subir algo de forma privada, pero el principio fundamental es que si estás usando Internet para disfrutar, gozar y divertirte, sube o envía sólo cosas que no te importe que sean vistas por todo el mundo.

3. Riesgos y desafíos

En este capítulo vamos a resumir algunos de los riesgos existentes a los que nos enfrentamos habitualmente cuando navegamos por Internet y que pueden poner en riesgo nuestra identidad desde dos perspectivas: que alguien acceda a nuestros datos personales y los utilice para su conveniencia (por ejemplo, robando información bancaria) o que alguien robe nuestra cuenta (por ejemplo, para difamar publicando información no fiable sobre nosotros o). Algunas técnicas utilizadas por los ladrones de datos son el phishing, los sitios web falsos, las identidades falsas, los virus (por ejemplo, los registradores de teclado) o el uso inadecuado de los gestores de contraseñas.

Riesgos y desafíos		
Conoce los riesgos generales que pueden afectar a nuestra seguridad y privacidad y cómo estar preparados.		
Conocimientos	**Habilidades**	**Competencias**
Él/ella • conoce las técnicas y los procedimientos usados para recoger nuestros datos • conoce la existencia de retos y fallos de seguridad en Internet • sabe tomar las medidas adecuadas para reducir o prevenir los riesgos	Puede • entender los principales riesgos y pedir ayuda en caso de duda • proteger el ordenador y nuestro acceso a internet	Es capaz de • tomar medidas para aumentar la seguridad de nuestras actividades en Internet

3.1. ¿Estamos realmente informados cuando damos nuestro consentimiento?

¿Sabemos lo que realmente estamos consintiendo? Esto ocurre cuando instalamos ciertas Apps en nuestro móvil; nos pide permiso para acceder a nuestros contactos, nuestra cámara, localización, etc. ¿Qué debemos hacer?, ¿es peligroso?, ¿son obligatorias?, ¿opcionales? También puede ocurrir cuando nos logueamos usando una plataforma de terceros (como google o facebook). Deberíamos ser conscientes de lo que ocurre aquí. ¿Debemos confiar en esas aplicaciones? ¿Cuál es el peor escenario? ¿Qué podemos hacer para protegernos?

¿Has leído alguna vez las Condiciones de Servicio (ToS)? Creo que nadie lo ha hecho. El día de los Santos Inocentes de 2010, la empresa Gamestation cambió las condiciones de servicio y escribió: "Al realizar un pedido a través de este sitio web el primer día del cuarto mes del año 2010 Anno Domini, usted acepta concedernos una opción no transferible para reclamar, por ahora y para siempre, su alma inmortal. En caso de que deseemos ejercer esta opción, aceptas entregar tu alma inmortal, y cualquier reclamación que puedas tener sobre ella, en un plazo de 5 (cinco) días laborables a partir de la recepción de la notificación por escrito de gamesation.co.uk o de uno de sus subordinados debidamente autorizados." Ahora son dueños de 7.500 almas de clientes.

Del mismo modo, cuando creamos una cuenta, instalamos un programa, etc. aparece un texto enorme y largo que debemos aceptar para seguir utilizando el programa. Son los términos de servicio que incluyen las condiciones de licencia y privacidad. Los términos de servicio (ToS) son un texto que se proporciona tal cual, sin opción a cambiar una palabra, sólo a aceptar o rechazar. Según SelectOut, la longitud media de esos textos es de 2.462 palabras, y se tarda 10 minutos en leerlos (sólo leerlos, no entenderlos y decidirlos), aunque la ley dice que deben ser concisos, transparentes, inteligibles y fácilmente accesibles). Hay iniciativas como https://tosdr.org que intentan informarte de forma concisa sobre otros sitios web, este sería un ejemplo de Facebook:

Pequeño resumen de Facebook proporcionado por tosdr.org

Desgraciadamente no hay solución al problema anterior. Si queremos usar la aplicación o el servicio tenemos que aceptar los ToS. Si no estamos de acuerdo, no podemos usar el programa. Lo que la mayoría de la gente hace es aceptar sin

considerar los riesgos. No podemos como tú leer esas cláusulas, sólo podemos pedir al gobierno y al poder público que legislen para proteger al consumidor de las cláusulas abusivas. A continuación, algunas recomendaciones:

- Si es posible, confía sólo en aplicaciones y servicios en los que confíe otra gente. Esto no es una garantía de un ToS inadecuado, pero al menos, las grandes empresas y proveedores de servicios tienen más probabilidades de ser supervisados por los servicios de control.
- Los servicios o programas gratuitos probablemente le costarán 0 euros, pero obtendrán dinero de otras maneras. Así que ten cuidado.
- En caso de sospecha, haz una búsqueda rápida en Internet. Por ejemplo, "Facebook use of images property" obtendrás información sobre si Facebook es o no propietario de las fotos que subes.
- Intente relajarse y disfrutar. A no ser que seas un creador de contenidos, que subas o descargues materiales con fines no personales (como editoriales, comerciales, etc.) o que tengas un negocio en Internet, entonces eres como el 99% de los usuarios de Internet; simples lectores o personas que comparten con otros simples imágenes o textos sin importancia, así que no te preocupes, intenta disfrutar de ser un usuario de Internet. Eso no significa que tengas que ser un insensato, y eso nos lleva al siguiente punto:
- Sé lógico; no subas ni compartas contenidos a nadie ni a ningún sitio web que quieras mantener en privado. Si compartes contenido privado, entonces debes empezar a ser más cauteloso con los términos de servicio, los problemas de privacidad y las licencias.

3.2 Las “Cookies” o galletas

Poca gente sabe qué son las cookies y cuál es su finalidad, pero todo el mundo ha oído hablar de ellas. Desde la promulgación del Reglamento General de Protección de Datos en 2016, todos los sitios web que utilizan cookies deben advertirte. De hecho, como el 99% de los sitios web de Internet utilizan cookies, dio lugar a que casi todos los sitios web te muestren un mensaje sobre el uso de Cookies. Pocos te ofrecen la opción de seguir navegando, deshabilitando las cookies, pero en la mayoría de los casos, si quieres seguir navegando por la web, entonces tienes que aceptarlas. En algunos casos, el simple hecho de seguir navegando implica la aceptación de las cookies. Pero, ¿sabe usted lo que realmente está aceptando?

Casi todos los sitios web utilizan cookies, es tan obvio que hay plugins que aceptan automáticamente todas las cookies, se llama "no me importan las cookies".

Las cookies son piezas de información que se guardan en su navegador. Estos datos sirven para que el sitio web recuerde cierta información sobre usted, por ejemplo, quién es, el idioma que ha seleccionado, los artículos que tiene en su cesta (si está comprando en una tienda online), etc. Gracias a las cookies puede solicitar a un sitio web que recuerde su nombre de usuario y no se autentique continuamente.

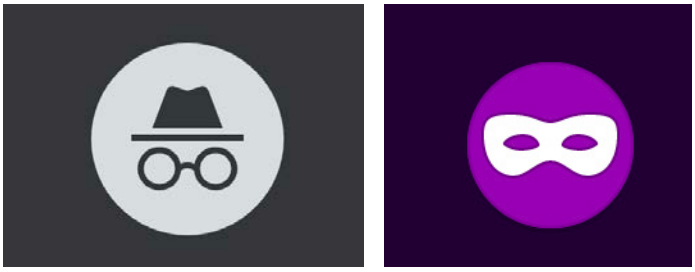
Por otro lado, las cookies también se utilizan para almacenar lo que has hecho mientras navegabas: por ejemplo, si has buscado un hotel en París, o has buscado un electrodoméstico para tu cocina. Después de haber realizado esta búsqueda, notará que en otros sitios web (noticias, blogs, vídeos, etc.) aparecen entonces anuncios relacionados con la búsqueda que ha realizado previamente.

Por lo tanto, las cookies permiten identificarle, o para ser más precisos, identificar sus acciones. En la medida en que los sitios web dejan cookies en el navegante mientras está leyendo noticias, comprando, buscando, etc. otros sitios web pueden recogerlas para saber si usted es apto para la publicidad u otras acciones.

Aparte de las páginas que venden cosas o muestran publicidad también utilizan cookies. El uso más común de las cookies es para rastrear sus actividades dentro del sitio web. Es una información muy valiosa para el diseñador del sitio web. No pretenden conocer sus intereses sobre otros temas (de hecho, sería difícil recopilar este tipo de información ya que sólo funciona en sitios web asociados y empresas de publicidad), sino que pretenden saber qué páginas son las más visitadas, cuándo una persona se convierte en un lector recurrente, cuántos minutos pasa en el sitio web y cuál fue la última página que visitó. Como se puede adivinar, se trata de información estadística que no tiene ningún interés personal, por lo que la enorme cantidad de cookies que hay en Internet son piezas de información inofensivas, sin. El problema está en los posibles problemas de privacidad que podrían transmitir las páginas que luego podrían intentar obtener información privada de usted. Ten en cuenta que por información privada no nos referimos a los datos que almacenas en tu ordenador, sino a cualquier información relacionada con la interacción con los sitios web, por ejemplo: qué página has visitado, vídeos que te han gustado o cosas que has comprado. El

peligro viene con la relación de este tipo de información, ya que si los sitios web están asociados, podrían vincular esa información a cualquier otro dato personal (como tu cuenta de correo o tu perfil en una red social).

Si realmente te preocupa no compartir ese tipo de información con nadie, lo mejor es iniciar una ventana privada o de incógnito en tu navegador, en lugar de rechazar las cookies.



Izquierda, icono de incógnito en Google Chrome. Icono derecho de incógnito en Firefox

Puede iniciar una ventana de incógnito o privada accediendo al menú Archivo del navegador. En este caso, todas las cookies se mantendrán en esta ventana y se eliminarán una vez que la cierre. Cuidado: eso no significa que navegues de forma anónima: cualquier información que envíes (correo, tarjeta de crédito, etc) o si sigues navegando (comprando, buscando, etc) será enviada, por lo tanto, ventana privada o de incógnito no es sinónimo de anónima. El anonimato depende de ti, y de la información que envíes. La ventana de incógnito o privada se refiere a que cualquier información relacionada con tu navegante será destruida una vez que la cierres. Ejemplo: si quieres hacer un regalo a tu prometido reservando un viaje y un hotel a París, mejor hazlo en una ventana privada. Una vez reservado el viaje, cierra el navegador. Por supuesto, la reserva será válida (en la medida en que envíes a la agencia de viajes y a la compañía aérea tus datos y los de la tarjeta de crédito) pero al día siguiente, en el navegador no aparecerá ningún anuncio sobre hoteles bonitos a París, ya que el navegador actual no podrá relacionar tu actividad de búsqueda de viajes.

3.3 Robo de identidad; phishing

"Phishing" es el término inglés que se refiere a la práctica de utilizar correos electrónicos fraudulentos y copias de sitios web legítimos para extraer datos financieros de los usuarios de ordenadores con fines de robo de identidad, es decir, cuando recibimos un correo electrónico que parece ser de nuestro banco, empresa, o incluso amigo pidiendo los datos de la cuenta de la tarjeta de crédito, la contraseña, o cualquier información privada. Este e-mail está escrito de manera urgente, como este:

> Banco internacional
> Oficina central
> Departamento de seguridad del consumidor
>
> Querido señor,
>
> Esta es una advertencia de seguridad urgente. Nuestros registros muestran que la información de su tarjeta de crédito ha sido comprometida, ha sido bloqueada para su seguridad, por favor vaya a:
>
> http://www.interationalbank.eu y regístrese, luego introduzca los datos de su tarjeta de crédito para desbloquearla.
>
> Saludos cordiales
>
> Departamento de Seguridad
> Banco Internacional

Este primer ejemplo del correo del "Banco Internacional", se entrega utilizando un correo que realmente tiene la apariencia de una comunicación oficial, con el logo y los colores del banco. Parece un asunto urgente y pide al lector que haga clic en la dirección e introduzca algunos datos.

El sitio web que se abre después de hacer clic en la dirección va a un sitio web que tiene la apariencia del banco, con todas las imágenes, textos y campos de contraseña, por lo que podría introducir sus datos bancarios, información de la tarjeta de crédito, etc, mientras que usted piensa que ese sitio web es realmente el sitio de su banco. Por supuesto, no lo es y usted está proporcionando su información privada a otra persona.

Los servicios de correo intentarán ayudarte y si creen que un correo es sospechoso te mostrarán un recuadro rojo muy brillante (esto lo hace Gmail) informándote de que tengas cuidado que probablemente el remitente del correo no es el que dice ser.

Hay muchos correos que puedes recibir que te piden alguna información (encuestas, confirmación de cuenta, etc) y es un buen consejo hacer clic en el enlace que te proporcionan en el cuerpo del correo, el consejo en este ejemplo es que te asegures que la dirección es la de tu banco, y no te abre una página con alguna letra

cambiada: por ejemplo www.interationalbank.eu en lugar de www.internationalbank.eu; (fíjate en un pequeño error ortográfico de la dirección). Un pequeño cambio en el nombre te lleva a una página web diferente. En caso de duda, llama primero a tu oficina.

A continuación, otro ejemplo:

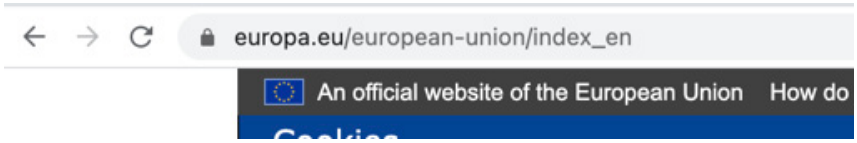
> Hola amigo mío
>
> Siento molestarle pero estoy en un problema. Estaba haciendo turismo en Londres y luego me robaron, ahora estoy usando un ordenador de un CiberCafé.
>
> Recuerdo nuestro proyecto en común y donde nos encontramos juntos ..... [algunos datos personales aquí]
>
> Por favor, pueden transferirme urgentemente algo de dinero a esta oficina de Direct Money:
>
> Money Transfer Ltd.
> Oficina de la Estación Central de Londres
>
> Por favor, introduzca este código como referencia 324114-34533 ya que mi pasaporte también ha sido robado y proporcionaré el secred como referencia.
>
> Tan pronto como regrese a mi país, le enviaré el dinero.
>
> Gracias

Eso sucede cuando alguien que se supone que es tu amigo requiere alguna ayuda urgente para ti. Esta carta está muy bien escrita y proporciona y él / ella proporciona alguna información privada que sólo debe saber. La confianza en esta carta se basa en esa información privada, pero el hecho es que el impostor podría tener acceso a las fotos de tu amigo, mensajes, correos, etc, y por lo tanto sabe muchas cosas sobre ti.

Aquí algunos consejos:

El correo electrónico no es un sistema certificado para el envío de mensajes. Usted podría recibir un correo de la dirección de su banco o de un amigo y aún así ser un mensaje falso. Piense en lo contrario: su amigo podría recibir un correo de su dirección y usted no enviar ese correo. Recuerde: el correo electrónico es un método de comunicación poco fiable.

Nunca puedes estar seguro de que el sitio web que estás leyendo es el que realmente dicen. Si buscas un sitio web, haces clic en la dirección de un correo, o en cualquier otro lugar (como en un foro, una red social, etc.) puedes ir a otro sitio web. La recomendación es que escribas la dirección. Deberías hacerlo al menos en los sitios web más privados que utilices (como bancos, entidades financieras, registros sanitarios...). Un candado cerrado cerca de la dirección no significa que el sitio web sea de confianza, sólo significa que la comunicación entre usted y el sitio web es segura (útil para las conexiones wifi públicas). Ver la siguiente imagen:



El candado cerrado es una conexión https (s=segura)

Hay otras formas de asegurarse de que una dirección es de confianza, es decir, que la organización del sitio web es la que usted espera, pero la forma de estar seguro de ello es asegurándose de que está poniendo la dirección adecuada.

3.4 Instalar apps, widgets y otras cosas

En términos generales las apps y widgets son herramientas útiles que instalamos intencionadamente en nuestro ordenador o dispositivos móviles, para poder disfrutar de nuevas funcionalidades. Un ejemplo de App que seguramente utilizas es el navegador web (puede ser Chrome, Firefox, Safari, entre otros). Otras Apps pueden ser un redactor de documentos, un procesador de imágenes, un juego, un reproductor de música, etc. Los widgets, extensiones o también conocidos como add-ons son como pequeñas apps que se adjuntan a otro programa. Por ejemplo, hay widgets para Microsoft Word que pueden ayudarte a hacer etiquetas, dibujos o bonitos títulos. También hay widgets para Chrome para Firefox que te ayudan a eliminar los anuncios, guardar tus pestañas, y mil funciones más.

Instalar este tipo de apps puede ser muy útil, de hecho, sin apps, nuestro móvil, tablet u ordenador no podría hacer nada, sería sólo un trozo de hierro.

El punto clave aquí es que instalar una app o una extensión es también la acción más peligrosa que podrías hacer en tu ordenador. Es una acción intencionada, pero a veces se hace sin que nos demos cuenta, esta sería la secuencia de acciones de un simple ejemplo:

1. Primero navegamos, aparece una página web diciendo que tenemos 3 virus y que podremos limpiar nuestro dispositivo pulsando el botón
2. Cuando hacemos clic en un botón se descarga un archivo
3. La página web nos pide entonces que hagamos clic en el archivo que se acaba de descargar. Diciendo que es 100% seguro y que si no limpiamos el virus que la web ha detectado vamos a perder todos nuestros datos
4. Hacemos clic en el archivo que acabamos de descargar. Nuestros sistemas operativos (Windows, OSX-Apple, Android...) nos advierten, diciendo que sólo debemos continuar si confiamos en la fuente del archivo
5. Aceptamos y entonces la App se instala en nuestro ordenador

El error ha estado en el paso 5; ¿realmente confiamos en la fuente del archivo?

La App recién instalada puede hacer lo que quiera, ejemplos:

- borrar nuestros datos en nuestro ordenador
- enviar a cualquier otra persona cualquier archivo que encuentre en nuestras carpetas
- mostrar publicidad de casinos, medicamentos, etc.
- cambiar el motor de búsqueda por defecto por el suyo propio (que dicen que es el más rápido y mejor del mundo, pero que sólo muestra anuncios)
- añadir algunas cosas más molestas

3.5 Acceso remoto

Por acceso remoto nos referimos a la posibilidad de que alguien acceda a tu ordenador. Esto puede hacerse a propósito, por ejemplo, cuando tienes un problema o una duda en tu ordenador y pides ayuda a un familiar o amigo. Entonces, esa persona podría acceder a tu ordenador y ver lo que está pasando e intentar resolver el problema. El acceso remoto es proporcionado por un programa que debe ser instalado en tu ordenador y también en el de tu amigo. El acceso remoto es un recurso muy útil ya que hay problemas o dudas que no se pueden resolver por teléfono y necesitan que alguien vea el error y pruebe cosas. No debes preocuparte por el acceso remoto, sino por la persona que está al otro lado.

Al estar en acceso remoto, la otra persona tendrá acceso a tu ordenador como si estuviera en tu asiento (usando tu teclado, ratón y viendo tu pantalla). Cuando la otra persona esté usando tu ordenador y abra una ventana, escriba algo o haga clic en alguna opción, tú podrás verlo, podrás ver cómo se mueve el ratón y cómo aparecen las cosas en la pantalla. Recuerda: la otra persona está usando el teclado y el ratón, esta es la capacidad del Acceso Remoto. Este tipo de programas no están hechos para acceder a tus carpetas, robar tus datos o instalar un virus. Otra cosa es que tus amigos borren o hagan algo desagradable mientras acceden a tu ordenador, pero este es otro tema, si detectas eso, puedes desconectarlo inmediatamente de la aplicación (cerrando la aplicación de acceso remoto).

El acceso remoto es una buena opción para pedir ayuda o prestarla sin tener que desplazarse a casa de la otra persona. Aun así, ten en cuenta que si alguien te llama o te ofrece ayuda diciendo que llama de Microsoft, del Banco o de algún otro sitio, puede intentar instalar algún programa en tu ordenador que tenga otras intenciones ocultas (puede ser un virus, o algo más).

.

3.6 Los Antivirus

Tener un programa antivirus es algo totalmente recomendable, pero permítanos algunas sugerencias:

Ve a una tienda de confianza y compra una suscripción anual del antivirus que te recomienden. Es mejor comprar y renovar una suscripción porque recibirás actualizaciones del antivirus. Cada dia puede aparecer un virus, por lo que es imprescindible mantener tu antivirus actualizado.

Te sugerimos que tengas un antivirus básico. Hay otros que tienen muchas más funcionalidades y dicen que te protegen contra páginas web falsas, correos maliciosos o robo de datos de tu ordenador. Eso sólo proporciona una falsa sensación de seguridad. Deja que tu antivirus sea la última barrera de defensa. Debes aprender a navegar con precaución y con confianza, sólo si eso falla y descargas un programa que es un virus sin ser consciente de ello, entonces tu antivirus debe ser el que te impida abrir ese programa.

En el mismo sentido que antes, es mejor tener un buen antivirus, pero no demasiado; me refiero a que hay antivirus que no paran de lanzarte mensajes sobre cualquier cosa: esto es seguro, esto no es seguro, precaución, ¿cómo quieres proceder?, etc. etc. Tantas preguntas y mensajes pueden hacer que los críticos pasen desapercibidos.

.

Ten en cuenta que al tener un antivirus activo, el ordenador irá más lento ya que el antivirus tiene que comprobar y verificar todos los datos que almacenas y recuperas de tu ordenador. Ese es el precio que hay que pagar por tener un antivirus.

3.7 Dejar tus datos en la red, el “big data”

Por lo general, navegamos inconscientemente en Internet, incluso cuando los sitios web nos piden permiso sobre el tratamiento de datos; tendemos a aceptarlos sin leer. Damos información sobre lo que buscamos o nos gusta y todo lo que hacemos en Internet. Hay algunas excepciones (por ejemplo, cuando accedemos a nuestro banco a través de una conexión segura), pero en general proporcionamos más información de la esperada. ¿Quién utiliza estos datos? ¿Pueden utilizarse estos datos en nuestra contra? En esta sección presentaremos algunos conceptos sobre las cookies, la recopilación de datos del sitio web (a veces estadísticos y otras demográficos), cómo podemos intentar minimizarlos (mediante la ventana de incógnito y presentando consejos) y, por último, por qué toda la enorme información que las empresas están recopilando sobre nosotros puede ser útil para ellas.

¿Nos suele preocupar lo que las organizaciones van a hacer con nuestros datos? ¿O a otras personas? ¿Cómo nos pueden afectar? Vamos a plantear esto desde dos perspectivas, por un lado, la recogida de datos que realizan las organizaciones con fines estadísticos o comerciales. Incluso puede parecer que estamos recibiendo ofertas comerciales personalizadas en base a nuestro historial de navegación, vamos a explicar que no es personal sino que se trata de big data. En segundo lugar, se trata de un tratamiento de datos más individualizado, es decir, cuando alguien busca datos precisos sobre nosotros o utiliza un software para rastrearlos. Este es el verdadero peligro, ya que podemos estar desprotegidos por la ley.

.

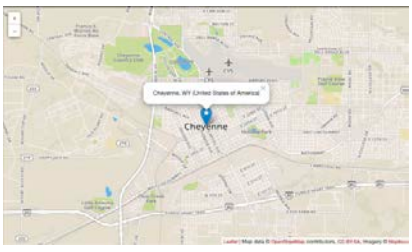
3.8 La Red profunda (deep web) y la red oscura (dark web)

Como navegantes ordinarios podemos buscar alrededor del 10% de los datos en Internet, por ejemplo: Wikipedia, Amazon, Twitter, Youtube, y muchos más sitios web públicos de gobiernos o periódicos.

El 90% de Internet es la Deep-web. Contenidos a los que no podemos acceder si no tenemos permiso: historiales médicos, información sobre suscripciones, documentos legales, registros financieros, informes científicos, etc.

Todavía hay otros contenidos que no se incluyen en el porcentaje anterior ya que no se puede estimar su tamaño, se trata de la dark-web. Se trata de una Internet paralela en la que utilizando algunas técnicas es posible simular quiénes somos y dónde estamos ubicados. A continuación, un ejemplo de geolocalización. A la derecha, estoy usando Google Chrome, puedo buscar usando Google cualquier tipo de información y si le pido a Google "Localizar IP" obtendrá el lugar donde se encuentra su ordenador. Si conoces la dirección del ordenador de un amigo, puedes preguntarle a Google dónde está ese ordenador. No se trata de una localización precisa, ya que esa información se obtiene mediante la IP (la IP es la dirección de Internet de tu ordenador) y en el caso de un teléfono móvil, o de una gran ciudad, la localización de esa IP no será tu casa, sino el centro de comunicaciones más cercano.

En la imagen de la derecha, estoy usando Tor, que es un navegador utilizado para acceder a la web oscura. Hice la misma pregunta y me dijo que estoy en Estados Unidos. Tor está ocultando mi IP y ubicación, por lo que nadie sabría quién soy, pero también es el otro lado: no puedo estar seguro de a qué lugares estoy accediendo, por lo que proporcionar mis datos o comprar en la web oscura puede ser peligroso.



Busca en Google "Locate IP" para encontrar sitios web que te permitan saber dónde se encuentra un determinado ordenador (siempre que conozcas la dirección IP). Las pantallas anteriores son del sitio web https://www.infosniper.net. Izquierda: surfista ordinario, derecha: Navegante Tor en la web oscura La imagen inferior es un sitio web de geolocalización, sin saber dónde estoy.

Los contenidos de la web oscura no pueden localizarse mediante un buscador ordinario (como Google o Bing), por lo que son inútiles a menos que se conozca la dirección exacta del sitio web que se quiere visitar. Además, las direcciones cambian a diario, lo que dificulta aún más a la policía la localización de contenidos ilegales y la identificación del propietario. Los contenidos de la web oscura no son necesariamente ilegales, sino que son utilizados por activistas y organizaciones que se encuentran en países con restricciones a la libertad de expresión. Por desgracia, esta web también es utilizada por terroristas, vendedores de drogas, vídeos ilegales, etc.

La forma en que se construyó Internet y las reglas que rigen cómo fluye la información por todos los hubs y subredes del mundo, hacen que sea imposible controlar la red, incluso para los países que filtran el contenido de Internet, siempre hay una brecha por donde la gente puede comunicarse. La única manera de impedir el uso de la web oscura sería cambiar los protocolos de Internet (que es como funciona internamente) y hoy en día eso sería un cambio enorme.

Si sientes curiosidad por el contenido de la web oscura, puedes instalar Tor surfer (www.torproject.org) y empezar a navegar, pero a menos que sepas a dónde ir, no notarás ninguna diferencia con la web ordinaria.

.

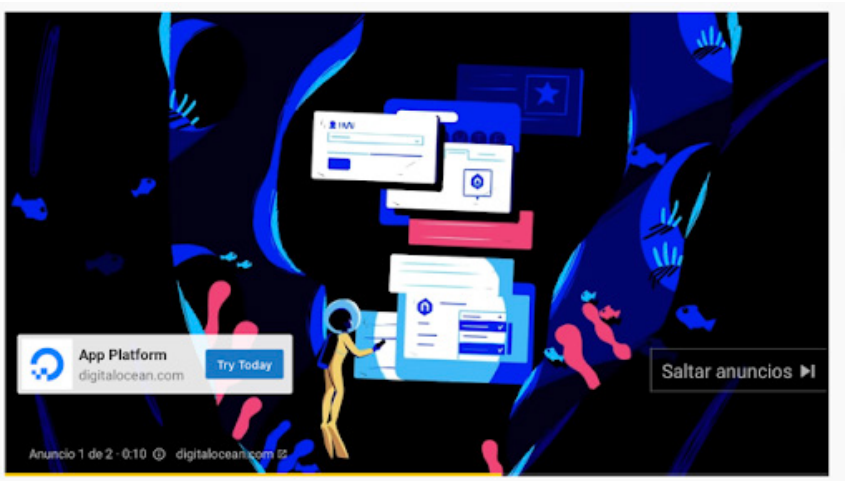
4. Modelos de negocio Internet

En Internet encontramos mucha información y servicios de uso gratuito, esos datos son proporcionados por personas y organizaciones que tienen que pagar por los servidores y los enlaces que conectan todas las casas, países y continentes. Aun así, hay mucha información y servicios que se ofrecen de forma gratuita, ¿cómo es posible? ¿Qué debemos tener en cuenta?

Modelos de negocio en Internet		
Es capaz de entender cómo los sitios web obtienen beneficios y cómo eso puede afectarnos a la hora de pagar por algún servicio.		
Conocimientos	**Habilidades**	**Competencias**
Pueden • entender cómo se trasladan los modelos de negocio al mundo de Internet • aumentar la concienciación a la hora de comprar o acceder a los servicios • saber cómo ganan dinero los sitios web y las aplicaciones gratuitas	Es capaz de • navegar por sitios web y acceder a la información con más confianza, identificar los anuncios y los contenidos sesgados • Identificar los diferentes tipos de pagos y tomar medidas para evitar estafas	Es capaz de • pagar o comprar servicios y productos con más seguridad

4.1 Publicidad oculta

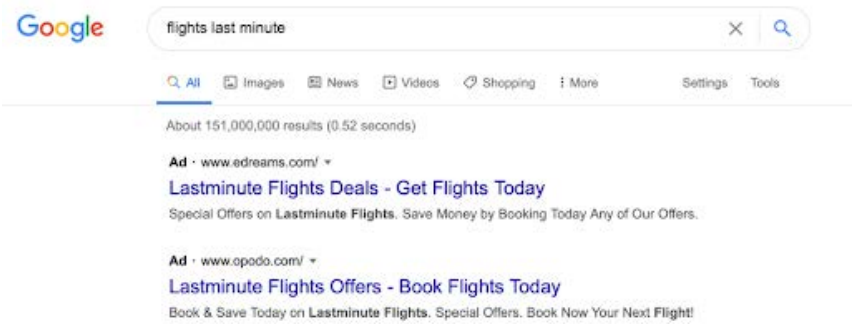
Estamos muy acostumbrados a los anuncios, los vemos en la televisión, los escuchamos en la radio y los vemos en los periódicos. Internet no iba a ser una excepción y vemos anuncios mientras leemos periódicos online e incluso cuando vemos vídeos. Este es el ejemplo de Youtube: aparece un banner para proponernos comprar o reservar algo o el vídeo se detiene y muestra un anuncio sobre un buen producto o lugar. Deberíamos ser capaces de diferenciar lo que es el contenido propio de la página web o del vídeo y lo que es un anuncio, para no confundirnos y pensar que el anuncio es un contenido proporcionado por el editor.



Este es un vídeo sobre la Historia de Internet, en el que aparece un anuncio

Este es un ejemplo de un anuncio en un video de youtube, esta sugerencia no es proporcionada por el creador del video, sino por la plataforma de youtube, por lo tanto debemos tener cuidado de no confiar o hacer clic en el anuncio, a menos por supuesto que lo hagamos a propósito.

A continuación se muestra un ejemplo de un anuncio que puede pasar desapercibido, y podemos decir que los resultados de búsqueda son los adecuados, pero hay que tener en cuenta que los resultados de búsqueda que tienen el encabezado "Anuncio", son los primeros no porque merezcan estar en la primera posición, sino porque han pagado para aparecer allí. De hecho, en este caso, pagarán a Google sólo si haces clic en esos enlaces.



Por lo tanto, hay que tener cuidado con los anuncios que se ocultan o simulan el contenido de la web, incluso podemos encontrar trucos sobre anuncios que simulan botones, por lo que hacemos clic en ellos pensando que estamos accediendo a algún lugar de la web pero en lugar de eso, estamos yendo a otra web completamente. La siguiente pantalla sería un ejemplo: ¿qué botón es el correcto: "Empieza la descarga" "EMPIEZA LA DESCARGA" o "Descarga ahora"?

Por último, hay otros anuncios que se muestran como si fueran alertas, este sería un ejemplo, donde el anuncio simula ser un mensaje de su sistema operativo. Es sólo una imagen que se encuentra en el sitio web, y si se hace clic allí se instalará un programa en su ordenador:

4.2 Tus datos son muy valiosos

Otra forma de pagar los sitios web que visitamos es proporcionando nuestros datos personales. El más común es el correo electrónico, en otros casos puede ser nuestro número de teléfono o dirección. Esa información se utiliza luego para vendernos productos o servicios. Por ejemplo, si visita una web sobre seguros de salud y le piden su correo electrónico y número de teléfono para enviarle un presupuesto, no se sorprenda si en las próximas semanas recibe llamadas sobre otro tipo de seguros, préstamos o cualquier otro producto.

Si visitas la página web de un colega que busca un curso de postgrado o un máster, entonces puedes recibir no sólo correos sino también llamadas telefónicas sobre nuevos estudios, cómo mejorar en tu carrera o nuevas oportunidades de trabajo. Todo eso puede ser bonito, siempre y cuando seas consciente de lo que va a pasar cuando facilites tus datos a cualquier página web.

Los datos personales son muy valiosos, pero más si están relacionados con algo más, como su interés por determinados productos, su nivel de ingresos, su edad o su situación financiera.

A veces no pagamos con dinero, sino con nuestros datos, que pueden ser tan simples como nuestro correo, para luego recibir algunas promociones, o más complejos; qué restaurantes, tiendas compramos o tipo de noticias leemos.

4.3 Leer no es gratuito

Al principio de la popularización de Internet en nuestras casas, lo utilizábamos para leer las noticias y las revistas. Podíamos obtener la información sin pagar en lugar de ir al quiosco y comprar un periódico. Desde entonces, los periódicos impresos han ido disminuyendo, poniendo en peligro el modelo de negocio tradicional. Era agradable obtener información gratuita en línea, pero no era un modelo de negocio sostenible para las empresas de comunicación.

Crecemos usando Internet y nos acostumbramos a conseguir cosas gratis y entonces pensamos que así es como deben ser las cosas. Nada más lejos de la realidad y ahora nos encontramos con que las empresas de comunicación nos piden que nos suscribamos a algunas de las secciones de la web o nos limitan la cantidad de páginas a las que podemos acceder online.

Incluso Wikipedia de vez en cuando pide algo de dinero, probablemente estás familiarizado con un banner que una vez al año, durante algunos días aparecen en Wikipedia:

Mensaje común de Wikipedia pidiendo donaciones

Nosotros, como usuarios de Internet, empezaremos a cambiar de opinión y a plantearnos pagar por las actividades más básicas que creíamos gratuitas, como simplemente leer páginas, y si no aceptamos eso, entonces empezaremos a acostumbrarnos a ver los anuncios o, lo que es peor, a encontrarnos con que la información que leemos está modificada en función de patrocinadores o lobbies.

4.4 Servicios gratuitos, esperando a que te enganches

Otra forma de pagar los sitios web que visitamos es proporcionando nuestros datos personales. El más común es el correo electrónico, en otros casos puede ser nuestro número de teléfono o dirección. Esa información se utiliza luego para vendernos productos o servicios. Por ejemplo, si visita una web sobre seguros de salud y le piden su correo electrónico y número de teléfono para enviarle un presupuesto, no se sorprenda si en las próximas semanas recibe llamadas sobre otro tipo de seguros, préstamos o cualquier otro producto.

Si visitas la página web de un colega que busca un curso de postgrado o un máster, entonces puedes recibir no sólo correos sino también llamadas telefónicas sobre nuevos estudios, cómo mejorar en tu carrera o nuevas oportunidades de trabajo. Todo eso puede ser bonito, siempre y cuando seas consciente de lo que va a pasar cuando facilites tus datos a cualquier página web.

Los datos personales son muy valiosos, pero más si están relacionados con algo más, como su interés por determinados productos, su nivel de ingresos, su edad o su situación financiera.

4.5 Ser creadores

Para la generación "X" (personas nacidas entre 1969-1980) o antes, durante la infancia generalmente querían ser policías, bomberos, médicos, etc. Para los que pertenecen a la generación "Z" (nacidos entre 1994-2010) y antes deseaban ser youtubers, influencers, gamers, viajeros, etc. Hay nuevos trabajos que aparecen gracias a la era de Internet, y "youtuber" podría ser uno de ellos, aunque es muy difícil vivir de esa carrera.

Cuando ves un vídeo en Youtube, lees un blog sobre alguna de tus aficiones, o una foto de un bonito vestido o comentas sobre un restaurante, probablemente estás haciendo que otra persona gane algo de dinero. En este sentido, el comentario sobre ese vestido o el plato podría no ser tan sincero como cabría esperar, pero así es como funcionan las cosas; Internet ha hecho posible que personas con talento puedan difundir sus vídeos, textos, comentarios con una inversión muy baja comparada con la que podían requerir en la época anterior a Internet. Un ejemplo de esto podría ser un grupo de rock o escritores que necesitan un productor o editor. El distribuidor y la tienda se quedaban con mucho dinero. Hacerse famoso en aquella época era muy difícil. Hoy en día, publicar tu música o vídeos en un canal de youtube es gratis (el equipo sería tu única inversión) y tener un blog para escribir tus poemas es muy barato. Por lo tanto todo el mundo puede ser creador, y si eres lo suficientemente bueno, obtendrás dinero por tus creaciones. Para tu curiosidad, por 2.000 reproducciones de vídeos puedes ganar 1 euro. Si tienes un blog, por cada 1.000 visitas puedes recibir 1 o 1,5 €. En Instagramers u otros medios de redes sociales, las empresas de moda o los restaurantes pueden pagarte si llevas sus vestidos o compartes tus platos favoritos.

Internet ha permitido encontrar millones de vídeos, fotos y comentarios sobre cualquier tema imaginable. La gente se ha hecho famosa por sus creaciones y opiniones. Ahora son "influencers" y esta palabra representa lo mejor y lo peor de Internet; todo el mundo puede ahora convertirse en creador y distribuir globalmente lo que desee, por otro lado, debemos ser conscientes de que las cosas que vemos y leemos no son tan sinceras como podríamos esperar. Al sesgo causado por la opinión y el punto de vista subjetivo que todo el mundo puede tener hay que añadir ahora una mayor distorsión causada por los intereses comerciales.

4.6 Micro-pagamentos

Comprar (en Internet o en una tienda de nuestra ciudad) es un proceso muy consciente; sabemos lo que estamos adquiriendo; un libro, reservar un hotel, un billete de avión... y también el precio, los impuestos y las condiciones de reembolso. Es más confuso cuando compramos una suscripción mensual a una plataforma de cine, o cuando facilitamos nuestra tarjeta de crédito para los pagos en una tienda de nuestro móvil. Incluso pueden ser micropagos (por ejemplo, 1 € el primer mes, o 0,5 € para su App) y luego nos confiamos, sin saber lo que puede pasar después (el segundo mes son 9 €, o tendrás que volver a pagar 0,5 €).

El mayor peligro que entrañan los micropagos es que se trata de cantidades tan pequeñas que podemos gastar mucho sin ser conscientes de ello.

Los micropagos empezaron a ser habituales en los juegos gratuitos. Hay juegos en los que puedes jugar y pasarte horas intentando conseguir algunos recursos (como armas más potentes, más vidas, más capacidades, más escenarios, etc), pero el juego te ofrece la posibilidad de que con una cantidad muy pequeña de dinero (pueden ser unos céntimos de euro) consigas ese preciado recurso que te permitirá conseguir un arco mejor que llegue más lejos la flecha (esto es un ejemplo, claro). Es tan barato que los jugadores tienden a gastar esa pequeña cantidad de euros en esa mejora. Por supuesto, siempre hay nuevas mejoras o nuevas características de los juegos que sólo se pueden conseguir pasando horas o pagando algo de dinero. El problema es que esos juegos utilizan incluso tácticas propias de las máquinas tragaperras (iconos, luz, música, texto). Por ejemplo, te ofrecen pagar por un arma más potente, pero está escondida en una de las 3 casillas, así que eliges una, y si tienes suerte ganas un arma mejor, pero puedes perder.

Las suscripciones mensuales son un buen método de pago, el único peligro está en la información oculta y en cómo podemos confundirnos. Los servicios de suscripción (como Netflix, HBO) ofrecen un mes gratis, pero hay que poner la tarjeta de crédito. Esto es muy bueno y no hay ningún truco en eso. Hay una gran ventaja: puedes probar la plataforma durante un mes y si no te gusta, puedes darte de baja sin ningún coste. Pero recuerda, tienes que darte de baja, si no pagarás la renovación. Afortunadamente, gracias a la normativa de la Unión Europea, la cancelación de la suscripción tiene que ser tan fácil como la suscripción, así que no te preocupes por eso. Nuestra única recomendación es que te asegures de que el servicio te ofrece claramente las condiciones, y que te acuerdes de cancelarlo antes de que termine el periodo.