Conceptos básicos de ciberseguridad que debes conocer

La ciberseguridad nos rodea y está al alcance de todos nosotros. Comprenderla no requiere de grandes conocimientos, sino de interés en saber cómo actuar y protegernos ante las distintas amenazas a las que estamos expuestos cuando hacemos uso de nuestros dispositivos y navegamos por Internet. En este artículo vamos a realizar el primer acercamiento a la ciberseguridad, mostrando diferentes escenarios y conceptos clave, con los que dar el paso para convertirnos en usuarios concienciados y ciberseguros.

Hoy en día todos somos conscientes de los beneficios que nos reporta la tecnología e Internet. Sin embargo, con sus ventajas también llegan los aspectos menos positivos, como son las amenazas en forma de virus y fraudes o la pérdida de privacidad. Por tanto, como usuarios tenemos por delante la misión de preocuparnos y hacer algo al respecto para que nuestra experiencia en el uso de las tecnologías e Internet sea lo más segura posible.

Si has decidido que ahora es el momento de ponerte al día en temas de ciberseguridad, ¡enhorabuena! No importa nuestra edad o habilidades en el manejo de la tecnología, pues al final, todo reside en seguir una serie de pautas y buenas prácticas.

A continuación, veremos varios escenarios y elementos básicos que son clave dentro del mundo de la ciberseguridad:

Dispositivos

Aparatos tecnológicos con los que interactuamos, como nuestro ordenador, el móvil, la *tablet*, la impresora, el *smartwatch* e incluso el robot de cocina o aspirador.

Contraseñas

Claves que utilizamos para iniciar sesión o registrarnos en alguna aplicación o página web. Están formadas por una serie de caracteres (letras, números y caracteres especiales), que, en función de su complejidad, pueden hacerlas más seguras.

Router

Dispositivo que nos permite conectarnos a Internet en nuestro hogar. Podemos conectar nuestros dispositivos a Internet a través de un cable de red o mediante la conexión wifi.

Wi-Fi

Conexión inalámbrica que permite conectar nuestros dispositivos a Internet.

Información sensible o privada

Información que contiene datos privados o confidenciales: nombre, apellidos, fecha de nacimiento, ubicación, datos bancarios, número de tarjeta de crédito, etc.

Bloqueo de pantalla

Todos los dispositivos cuentan con un sistema de bloqueo de pantalla para impedir que lo usen otras personas sin nuestro permiso. Este bloqueo se puede establecer configurando un patrón, una clave, PIN o incluso una huella digital o reconocimiento facial.

Copia de seguridad

Copia de nuestros archivos y programas que puede almacenarse en otros dispositivos o soportes para evitar perder nuestra información en caso de fallo, pérdida o robo.

Antivirus

Programa que detecta cualquier amenaza, como los virus, y la elimina de nuestro dispositivo. Es necesario mantenerlo actualizado para que nos proteja correctamente, incluso de los virus más nuevos.

Cortafuegos

Cuando navegamos por la Red y accedemos a una web, esta se comunica con nuestro equipo para establecer la conexión entre ambos. Las herramientas conocidas como *firewall* o cortafuegos analizan esas conexiones para impedir aquellas que puedan suponer un riesgo para nosotros.

Actualización

Todos los dispositivos y programas instalados evolucionan y se actualizan a nuevas versiones. Con la actualización se solucionan errores y problemas de seguridad y rendimiento, por lo que debemos asegurarnos de actualizarlos siempre.

Software

Programas informáticos que sirven para realizar tareas específicas. Cualquier herramienta que instalemos o utilicemos en nuestro ordenador es un ejemplo de *software*, como el navegador, el correo electrónico, un juego o cualquier otra aplicación que ofrezca alguna funcionalidad concreta.

***Software* pirata**

Un programa descargado de una página web que no sea la del desarrollador, fabricante o un repositorio oficial de aplicaciones, como pueden ser Google Play o Apple Store, se considera un *software* pirata y puede ser una gran amenaza para nuestro equipo, ya que puede contener virus u otras amenazas (*malware*).

Spam

Correo de tipo publicitario o malicioso no deseado que llega a nuestra bandeja de entrada con el único propósito de vendernos un producto, hacernos caer en algún fraude o infectar nuestros dispositivos.

Ingeniería social

Estrategia de engaño que utilizan los ciberdelincuentes para ganarse nuestra confianza y conseguir que compartamos nuestros datos con ellos, como contraseñas o datos de nuestra tarjeta, o que les demos acceso a nuestros dispositivos.

Phishing

Técnica donde los ciberdelincuentes se hacen pasar por otra persona o entidad a través del correo electrónico, como puede ser el banco, una red social o incluso un servicio público, para engañarnos y que realicemos alguna acción bajo cualquier excusa, generalmente acceder a una página fraudulenta o descargar un fichero infectado.

Archivo adjunto

Fichero o documento que viene junto a un correo electrónico y que podemos descargar. Si la persona que nos envió el correo es desconocida o el contenido del mensaje nos resulta raro, no debemos descargarlo hasta saber que no estamos ante un fraude.

Cifrado

Proceso que sirve para convertir un documento o un archivo en una versión ilegible para todas aquellas personas que no posean la clave para descifrarlo. Sirve para proteger la información de todas aquellas personas que no deberían acceder a ella bajo ningún concepto.

Navegador web

Programa utilizado para navegar por Internet. Nos permite visitar páginas web e interactuar con ellas. Los más famosos son Google Chrome, Mozilla Firefox, Edge o Safari.

Buscador

Herramienta que nos permite realizar búsquedas de información en distintos sitios web de Internet bajo términos concretos. El más conocido es Google, y si realizamos una búsqueda por cualquier palabra o frase, nos mostrará los resultados que mejor se ajusten a nuestra petición.

Barra de direcciones

Espacio dentro de nuestro navegador donde podemos escribir la dirección de la página web o URL. Se encuentra siempre en la parte superior del navegador.

Complemento/extensión

Programa informático o *software* que se instala en nuestro navegador y que nos permite personalizarlo. Hay de muchos tipos, algunos, por ejemplo, añaden mejoras de seguridad, bloquean anuncios de las páginas web o nos permiten gestionar nuestras contraseñas de acceso a distintos servicios online.

Correo electrónico

Servicio que nos permite enviar y recibir mensajes mediante Internet. Para utilizarlo necesitamos un gestor de correo (Gmail, Outlook/Hotmail, Yahoo!, etc.), que es la herramienta desde la que enviamos, recibimos o eliminamos correos, y crear una cuenta de correo en dicho gestor, que está formada siempre por un nombre/alias + @ + el nombre del servidor de correo donde la hemos creado. Ejemplo: esteesminombre@osi.es.

URL

Cadena de caracteres que permite acceder a una página web o contenido alojado en Internet. Se compone de varias partes: el protocolo, que puede ser “http” o “https”, y el domino, que es el nombre o dirección de la página web concreta. Ejemplos de URL: https://www.osi.es y https://www.incibe.es

HTTP/HTTPS

Siglas de los protocolos más utilizados para la navegación por Internet. HTTPS es la versión segura y nos garantiza que la información que se transmite entre nuestro dispositivo y la página web está cifrada y protegida, especialmente en el envío de datos personales, como contraseñas o datos bancarios.

Certificado digital

Icono en forma de candado que suele aparecer a la izquierda de algunas URL de páginas web. Este icono significa que es una web que ha sido certificada por una entidad certificadora que acredita que se trata de una web segura

Lamentablemente, por sí mismo no implica que la web sea segura, ya que los ciberdelincuentes son capaces de engañar a estas entidades para utilizar sus certificados en sitios web fraudulentos y dotarlos de mayor credibilidad.

Pop-ups

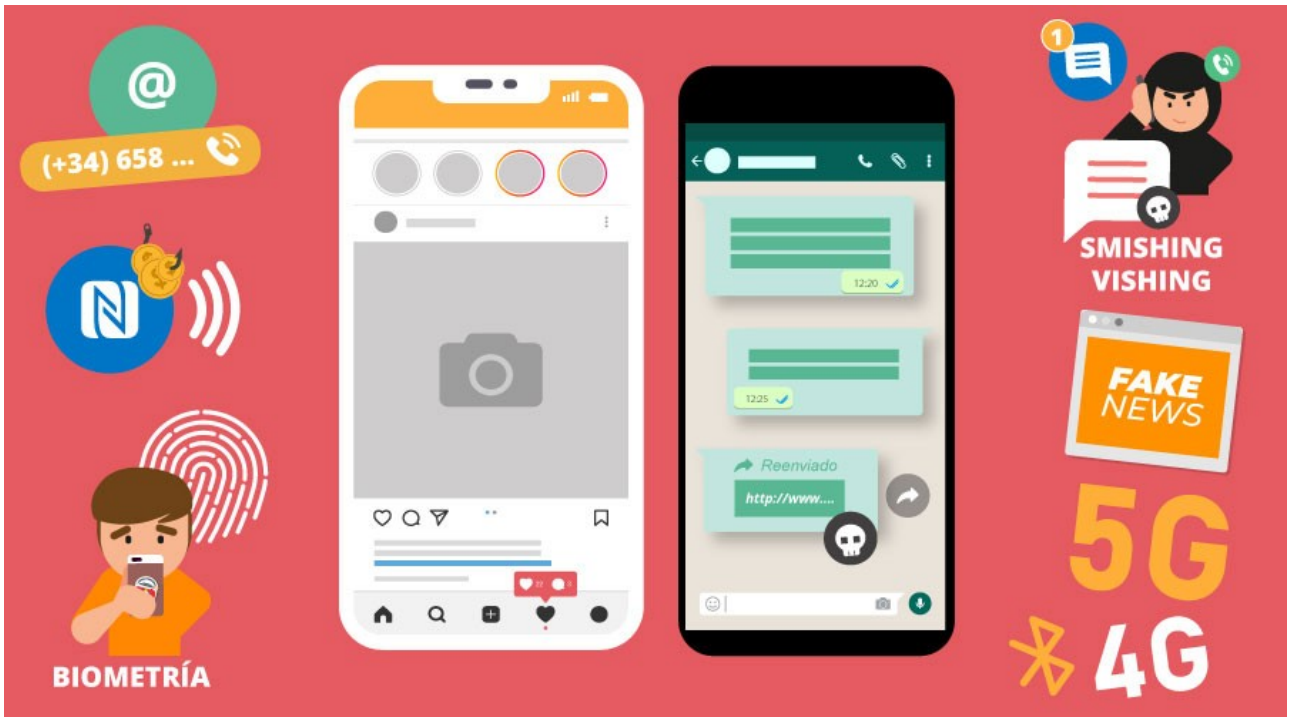
Ventanas o notificaciones que suelen contener información o anuncios y que aparecen en nuestros dispositivos. Lo más común es que aparezcan cuando navegamos por Internet en forma de pequeñas ventanas y, dependiendo del sitio web que estemos visitando, puede haber más o menos, e incluso contener enlaces maliciosos o estafas.

Cookies

Pequeños archivos que contienen información que ha recopilado una determinada página web que hemos visitado y que se almacenan en nuestros dispositivos. Sirven principalmente para recabar información sobre nuestros hábitos de navegación y mostrarnos publicidad dirigida con información que pueda ser de nuestro interés.

Historial

Histórico de todas las páginas web y sitios online que hemos visitado, que se almacenan en el navegador web y que pueden ser consultadas por el usuario.



Biometría

Mecanismo para bloquear el acceso a nuestros dispositivos que, en vez de utilizar una contraseña o un patrón, utiliza algún elemento de nuestro cuerpo, como la huella dactilar o nuestro rostro.

Bluetooth

Conexión inalámbrica que permite intercambiar información, datos o archivos entre dos dispositivos. También permite sincronizar o conectar dos dispositivos para hacer que interactúen, por ejemplo, cuando conectamos nuestra pulsera de actividad a nuestro *smartphone* para que se sincronice nuestra ruta y nos informe de cualquier notificación.

NFC

Tecnología que nos permite realizar pagos con nuestro dispositivo móvil, de la misma forma que funcionan las tarjetas bancarias “contactless”. Con solo apoyar nuestro *smartphone* en el datáfono o TPV se realizará el cobro.

Apps

Aplicaciones que instalamos en nuestro dispositivo móvil, *smartphone* o *tablet*, y que nos proporcionan alguna funcionalidad extra. Existe una gran variedad (juegos, redes sociales, financieras, utilidades, monitorización de actividad, entretenimiento, etc.), pero como ocurre con los programas de nuestro ordenador, debemos descargarlas siempre de sitios oficiales para evitar instalar aplicaciones maliciosas.

Permisos

Recursos, información y funciones que una aplicación que instalamos en nuestro dispositivo necesita para funcionar. Por ejemplo, una app para editar fotografías es muy probable que necesite acceder a la cámara de nuestro teléfono, por lo tanto, solicitará el permiso de nuestra cámara.

Por otro lado, algunas aplicaciones solicitan permisos abusivos, como acceder a nuestros contactos y archivos que tenemos almacenados, o realizar llamadas sin ser necesario para su correcto funcionamiento.

4G y 5G

Tecnologías que utilizan nuestros dispositivos móviles para conectarse a Internet. La "G" hace referencia a las generaciones y evolución de este tipo de tecnología, que nos permite navegar cada vez más rápido desde nuestro *smartphone* o *tablet*.

Smishing

Ataque basado en ingeniería social, donde los atacantes se hacen pasar por otras personas o entidades de confianza, a través de mensajes de texto o SMS, con el fin de engañarnos para que realicemos un pago, nos descarguemos un archivo infectado o hagamos clic en un enlace malicioso.

Vishing

Ataque basado en ingeniería social, donde el atacante se hace pasar por una persona que no es, llamándonos por teléfono e intentando que le facilitemos información personal, accedamos a una página web fraudulenta o instalemos algún programa para tomar el control de nuestro dispositivo. Frecuentemente se hacen pasar por el servicio técnico del sistema operativo de nuestros dispositivos.

Fake news

Noticias falsas que circulan principalmente por Internet a través de redes sociales o apps de mensajería como WhatsApp. Suelen incluir un titular muy atractivo, pero la información que contienen es falsa o está manipulada. Generalmente, es fácil identificarlas, pues solo necesitamos contrastar la información con otras fuentes de confianza o realizar una búsqueda sobre la noticia en Internet para darnos cuenta de que no son verdad.

Bulos

Cadenas de mensajes con noticias o eventos alarmantes que no provienen de ninguna fuente fiable y solo buscan desinformar y crear confusión entre los usuarios que los reciben, principalmente a través de redes sociales y *chats*.