Recomendaciones: Ciberseguridad básica para usuarios

Índice

Introducción

En el mundo digital actual, la ciberseguridad es una herramienta esencial para proteger nuestra identidad, información personal y bienestar financiero. Al igual que cerramos las puertas de casa para mantener nuestra seguridad física, debemos tomar medidas similares en el entorno digital.

Este manual está diseñado para ser una guía práctica, ligera y accesible, pensada para personas cotidianas que buscan entender mejor cómo protegerse en el entorno digital. No necesitas ser un experto en tecnología para seguir estas recomendaciones. Nuestro objetivo es que te sientas más seguro y confiado cada vez que uses Internet o tus dispositivos móviles.

INCIBE

El Instituto Nacional de Ciberseguridad (INCIBE) es una entidad pública fundamental en la protección digital de los ciudadanos españoles. Su misión es garantizar un entorno seguro para el uso de tecnologías digitales, abarcando desde la educación hasta la asistencia técnica especializada. INCIBE no solo se enfoca en la protección frente a amenazas cibernéticas, sino que también promueve la conciencia y la educación en ciberseguridad, proporcionando a los usuarios las herramientas necesarias para cuidar su seguridad en línea de manera efectiva.

Una de las iniciativas más útiles de INCIBE es su línea de ayuda gratuita, el **017**. Si alguna vez te encuentras con un problema de seguridad en internet, ya sea un posible fraude, un virus en tu ordenador o incluso si sospechas que alguien está acosando a tu hijo en línea, puedes llamar a este número. Expertos en ciberseguridad te atenderán y te guiarán sobre qué hacer, sin importar la hora o el día. Además, INCIBE ofrece guías prácticas, consejos de seguridad y herramientas gratuitas en su web, todas diseñadas para que cualquier persona, sin necesidad de ser un experto en tecnología, pueda protegerse eficazmente en el entorno digital.

Página web de Incibe: https://www.incibe.es/

Protege el dispositivo frente a malware y actividad maliciosa

El **malware**[1] es una amenaza constante en el mundo digital actual, capaz de dañar nuestros dispositivos y robar información personal. Los ataques de malware[1] pueden provenir de fuentes diversas, como archivos descargados de internet, correos electrónicos con adjuntos maliciosos o incluso aplicaciones que parecen legítimas, pero que en realidad esconden intenciones dañinas. Además, el malware puede propagarse rápidamente a través de redes, afectando no solo a dispositivos individuales, sino también a sistemas enteros.

Siempre es recomendable instalar un buen antivirus y mantenerlo actualizado. Un antivirus es tu primera línea de defensa. Asegúrate de elegir un programa confiable y mantenerlo siempre actualizado para que pueda detectar y eliminar las últimas amenazas. En el último punto de este documento te contamos cómo podemos ayudarte en este apartado.

Actualización de dispositivos

Mantener tus dispositivos actualizados es una de las prácticas más importantes para garantizar su seguridad y buen funcionamiento. Las actualizaciones del sistema operativo y las aplicaciones no solo traen nuevas funciones o mejoras de rendimiento, sino que también corrigen vulnerabilidades que los ciberdelincuentes podrían aprovechar para acceder a tu información personal o comprometer tus dispositivos. Ignorar estas actualizaciones puede dejarte expuesto a riesgos innecesarios, como ataques de malware[1], robo de datos o incluso el mal funcionamiento del equipo. Configurar las actualizaciones automáticas es una forma sencilla de asegurarte de que tu móvil, ordenador u otros dispositivos estén siempre protegidos y funcionando de manera óptima.

Gestión de credenciales

La gestión adecuada de credenciales es un pilar fundamental en la protección de nuestra identidad digital. En un mundo donde cada vez tenemos más cuentas en línea, desde redes sociales hasta servicios bancarios, es crucial adoptar prácticas seguras para la creación y mantenimiento de nuestras contraseñas. Una contraseña robusta es nuestra primera línea de defensa contra accesos no autorizados y posibles fraudes.

Para crear contraseñas seguras, recomendamos seguir las siguientes pautas:

- **Utilizar una contraseña única para cada servicio, aplicación o cuenta de usuario.**
- Longitud mínima de 16 caracteres.
- Combinación de letras mayúsculas, minúsculas, números y símbolos.
- Contraseñas aleatorias y sin patrones.

No es recomendable almacenar las credenciales en el navegador, o utilizar características de inicio de sesión automáticas mediante el navegador. Para poder cumplir estas pautas, es imprescindible la utilización de gestores de contraseñas.

Gestores de contraseñas

Los gestores de contraseñas son herramientas que almacenan y administran nuestras credenciales de forma segura. Cifran todas nuestras contraseñas bajo una única contraseña maestra, permitiéndonos usar claves complejas y únicas para cada servicio sin tener que memorizarlas. Además, ofrecen funciones como la generación automática de contraseñas y el autocompletado de formularios.

Aunque existen multitud de gestores de contraseñas, nosotros utilizamos y recomendamos **KeePassXC** (https://keepassxc.org/) y puedes acceder a nuestra guía de instalación y uso mediante el siguiente enlace: https://drive.google.com/file/d/1rUN974gvywYzFqHMoACMcyPXb6e_WIad/view?usp=sharing

Doble factor de autenticación (2FA) y autenticación de múltiples factores (MFA)

La autenticación de dos factores (**2FA**) y la autenticación multifactor (**MFA**) son medidas de seguridad esenciales en un mundo digital donde las contraseñas por sí solas ya no son suficientes para proteger nuestras cuentas. Estos sistemas añaden capas adicionales de verificación, combinando algo que sabemos (como una contraseña), algo que tenemos (como un código enviado al móvil) o algo que somos (como una huella dactilar). Al implementar estas medidas, incluso si un ciberdelincuente logra obtener nuestra contraseña, necesitará superar barreras adicionales para acceder a nuestras cuentas.

Existen multitud de métodos de doble factor, pero el más común y el que recomendamos utilizar (si es posible) es **Google Authenticator**. Genera códigos únicos de seis dígitos que cambian cada 30 segundos, necesarios para acceder a servicios compatibles. Es fácil de configurar escaneando un código QR proporcionado por el servicio que se quiere proteger. Puede encontrarse para dispositivos móviles en la Play Store buscando "Google Authenticator" de Google LLC o mediante el enlace: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=es

Copias de seguridad

Las copias de seguridad son una de las medidas más importantes que podemos tomar para proteger nuestros datos personales y profesionales en el entorno digital. Al realizar copias de seguridad regulares, podemos asegurarnos de que nuestros recuerdos digitales, como fotos y videos, así como nuestros documentos importantes, estén a salvo y puedan ser recuperados fácilmente si algo sale mal. Las copias de seguridad pueden realizarse de dos formas principales: locales y en la nube.

Las copias locales implican guardar nuestros datos en dispositivos físicos que tenemos a mano, como discos duros externos o unidades USB. Estas ofrecen un control total sobre nuestros datos y un acceso rápido, pero están sujetas a riesgos físicos como robos o daños. **Recomendamos encarecidamente realizar copias de seguridad locales** en unidades USB o discos duros externos de información importante como documentos o la base de datos de contraseñas del gestor de contraseñas. Es importante mantener estas copias de seguridad actualizadas.

Por otro lado, las copias en la nube de servicios como Google Drive, Dropbox o OneDrive almacenan nuestros datos en servidores remotos, permiten acceder a nuestros archivos desde cualquier lugar con conexión a internet y nos protegen contra pérdidas locales, aunque requieren confiar en un tercero para el almacenamiento de nuestra información. **Lo ideal es combinar ambos métodos:** mantener copias locales para un acceso rápido y control directo, y utilizar servicios en la nube para una capa adicional de seguridad y accesibilidad, creando así un sistema de respaldo robusto y versátil.

Navegación segura en Internet

Navegar por Internet de manera segura es fundamental para proteger tu información personal y evitar riesgos como el robo de datos. Una de las primeras medidas es asegurarte de visitar únicamente **sitios web confiables,** que además utilicen el protocolo **HTTPS**[2], identificado por un candado en la barra de direcciones y porque la URL[3] completa empezará por **https://**, por ejemplo, https://cloudyole.es/. Este protocolo únicamente cifra la información que compartes, por lo que no debes asumir que la página web es confiable o legítima únicamente por aparecer el candado verde.

Otra práctica esencial es utilizar redes Wi-Fi seguras. **Evita conectarte a redes públicas** sin protección o, en caso de necesidad, emplea una red privada virtual (**VPN**)[4] para cifrar tu conexión y mantener tu privacidad. También es recomendable mantener tu navegador actualizado y desactivar extensiones o complementos que ya no uses.

Descarga de aplicaciones y programas de forma segura

Descargar aplicaciones y programas de forma segura es crucial para evitar la instalación de software malicioso que pueda comprometer tus dispositivos o tu información personal. En dispositivos móviles, asegúrate de **utilizar únicamente tiendas oficiales** como Google Play Store o App Store, ya que estas plataformas verifican las aplicaciones antes de publicarlas. En el caso de ordenadores, **descarga los programas directamente desde las páginas oficiales** de los desarrolladores o de repositorios confiables. Evita sitios web de dudosa procedencia que ofrezcan descargas gratuitas de programas pagos, ya que muchas veces estos archivos están modificados para incluir malware[1].

Es importante mantenerse alejado de aplicaciones pirateadas o versiones no oficiales de software, ya que suelen ser una puerta directa para virus, spyware y otros tipos de amenazas. Aunque puedan parecer una opción atractiva por ser gratuitas, el riesgo para tu seguridad y privacidad es muy alto. Además, este tipo de prácticas puede violar derechos de autor y

exponerte a problemas legales. Optar siempre por software legítimo y actualizado no solo protege tus dispositivos, sino que también garantiza un mejor rendimiento y soporte técnico en caso de problemas.

Protección contra fraudes, phishings y otros tipos de estafas

Los fraudes en línea, como el **phishing**[5] (email fraudulento), el **smishing**[6] (mensajes SMS fraudulentos) y el **vishing**[7] (llamadas telefónicas falsas), son cada vez más sofisticados y buscan engañarte para obtener información confidencial o dinero. En el caso del phishing[5], los ciberdelincuentes suelen enviar correos electrónicos que simulan ser de instituciones confiables, como bancos, empresas o servicios públicos. Estos mensajes suelen incluir enlaces que redirigen a sitios web falsos diseñados para robar tus datos. Para protegerte, **nunca hagas clic en estos enlaces**; en su lugar, accede al sitio web escribiendo la dirección directamente en tu navegador, como harías normalmente. Además, **revisa siempre la URL**[3] **de cualquier página en la que te encuentres**, verifica que el **dominio**[8] es legítimo.

El smishing[6] y el vishing[7] son variantes del phishing[5] que utilizan mensajes de texto o llamadas telefónicas para engañarte. En estos casos, los estafadores intentan crear un sentido de urgencia para que compartas datos sensibles o realices pagos. Por ejemplo, podrían enviarte un SMS indicando un supuesto problema con tu cuenta bancaria o llamarte haciéndose pasar por un trabajador del banco. Es importante tener en cuenta que tanto los correos electrónicos como los SMS y las llamadas telefónicas están basados en protocolos antiguos que permiten técnicas de suplantación de identidad, lo que facilita a los ciberdelincuentes falsificar remitentes y números telefónicos. Por ello, **nunca proporciones información personal por teléfono, SMS o correo electrónico** sin verificar primero la autenticidad del remitente a través de los canales oficiales de la institución.

Otro tipo de fraude común son las estafas relacionadas con tiendas falsas y anuncios engañosos en redes sociales. Estas páginas suelen ofrecer productos a precios demasiado bajos para ser reales o utilizan imágenes robadas para atraer compradores. Antes de realizar una compra en línea, **verifica la legitimidad del sitio**, comprobando que la URL[3] sea correcta y asegurándote de que la tienda tenga políticas claras de contacto y devoluciones.

Para esta última recomendación, nos trasladamos al mundo real. En ocasiones, los ciberdelincuentes aprovechan el bullicio y la masificación de un entorno para robarnos los datos de nuestras tarjetas de crédito y débito. Esta acción maliciosa se realiza con dispositivos que roban la información de las tarjetas al pasar cerca de ellas, otra variante es la realización de cargos fraudulentos al pasar un dispositivo **TPV**[10] cerca de las tarjetas. Para protegernos frente a estos ataques, recomendamos utilizar **skimming blockers**, que son protectores físicos, como fundas o tarjetas especiales que se colocan junto a las tarjetas bancarias para evitar que sean leídas por estos dispositivos no autorizados.

Cómo podemos ayudarte desde Cloud y Olé

En Cloud y Olé, entendemos que la ciberseguridad puede parecer un laberinto complicado, pero estamos aquí para simplificarlo y ofrecerte soluciones prácticas y efectivas. Como expertos en ciberseguridad y ciberinteligencia, nuestra misión es proteger tu información y dispositivos de las amenazas digitales, brindándote la tranquilidad que necesitas para navegar y operar con confianza en el mundo digital.

Nuestros servicios de defensa digital se complementan con todas las recomendaciones anteriores, con nuestros planes enfocados en usuarios como tú, dispondrás de potentes herramientas que te ayudarán a mantenerte protegido:

- **Plan esencial:** Dispondrás de un potente **antivirus EDR** para la protección completa de tu ordenador, que no solo detecta y elimina amenazas conocidas, sino que también utiliza inteligencia artificial para identificar comportamientos sospechosos y prevenir ataques nuevos y sofisticados.

- **Plan completo:** Además del EDR, contarás con un servicio de **10 consultas mensuales** sobre correos sospechosos o intentos de phishing[5]. Gracias a estas consultas podrás diferenciar los correos legítimos de los fraudulentos, protegiendo así tu información sensible y evitando caer en estafas sofisticadas. Además, con nuestro servicio de Threat Intelligence, monitorizamos tu correo electrónico para descubrir brechas o información filtrada en la dark y deep web. Si encontramos cualquier información comprometida, como tus contraseñas, te alertaremos de inmediato y te proporcionaremos orientación experta sobre cómo mitigar los riesgos.

Si quieres más información sobre estos servicios, puedes contactarnos en comercial@cloudyole.es o llamando al teléfono **+34 697 282 568**.

Glosario

1. **Malware**: Es un programa malicioso diseñado para infiltrarse en dispositivos electrónicos, como ordenadores, teléfonos móviles o tabletas, sin el consentimiento del usuario. Su objetivo puede variar desde causar daños en el sistema, robar información personal o financiera, hasta permitir el control remoto del dispositivo por parte de ciberdelincuentes.

2. **HTTPS**: Es un protocolo que garantiza una conexión segura entre el usuario y una página web. Indica que los datos compartidos en el sitio están cifrados y protegidos contra accesos no autorizados, lo que resulta esencial para transacciones bancarias, compras en línea o cualquier actividad que implique compartir información sensible.

3. **URL:** Es la dirección única que identifica una página web en Internet. Se compone de diferentes elementos (como el nombre del dominio y el protocolo) y permite a los usuarios acceder a un sitio específico al escribirla en el navegador. Por ejemplo, "www.cloudyole.es" es una URL.

4. **VPN:** Es una herramienta que proporciona privacidad y seguridad al navegar por Internet. Crea una conexión cifrada entre el dispositivo del usuario y la red, ocultando su ubicación real y protegiendo sus datos frente a posibles interceptaciones, especialmente útil para aumentar la protección en redes Wi-Fi públicas.

5. **Phishing:** Es una técnica de fraude cibernético en la que se engaña a las personas para que revelen información confidencial, como contraseñas, números de tarjetas de crédito o datos bancarios. Esto se realiza mediante correos electrónicos o páginas web falsas que imitan entidades legítimas, como bancos o empresas reconocidas.

6. **Smishing:** Es una variante del phishing que utiliza mensajes de texto fraudulentos para intentar obtener información personal o financiera de las víctimas. Estos mensajes suelen incluir enlaces peligrosos o solicitudes urgentes que buscan manipular al receptor.

7. **Vishing:** Es un método de estafa telefónica en el que los delincuentes se hacen pasar por instituciones confiables, como bancos o empresas, para obtener información confidencial o dinero de forma fraudulenta. A menudo utilizan tácticas persuasivas para ganarse la confianza de la víctima.

8. **Dominio:** Es el nombre único asignado a un sitio web en Internet, utilizado para identificarlo y facilitar su acceso por parte de los usuarios. Por ejemplo, "cloudyole.es" es un dominio.