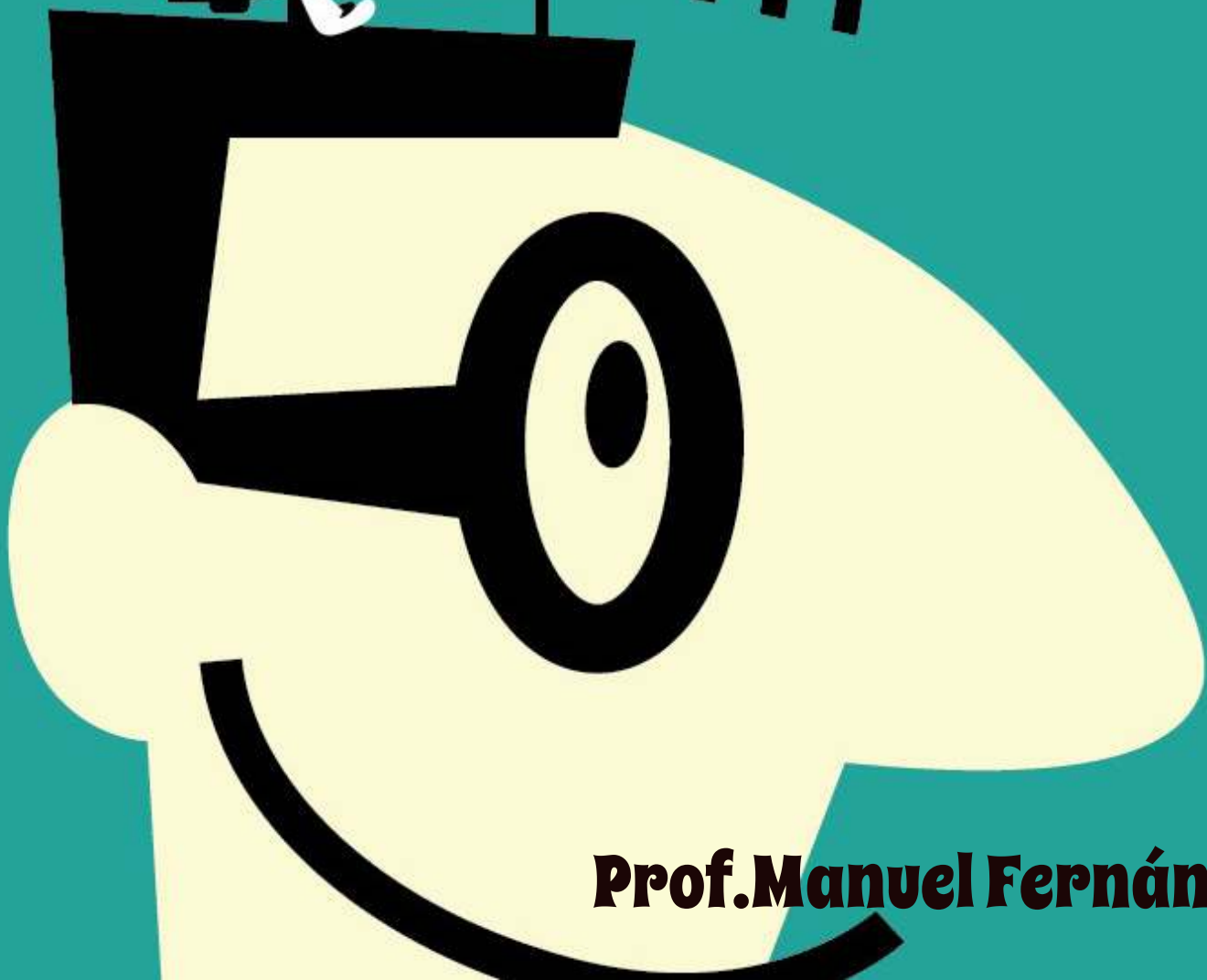
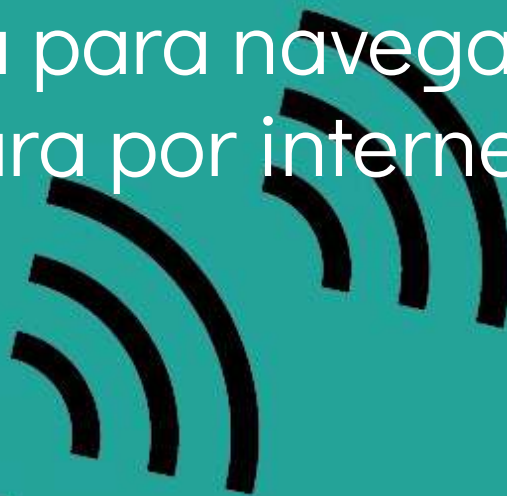


Internet

Guia completa para navegar
de forma segura por internet



Prof. Manuel Fernández

Guía completa para navegar de forma segura por internet

Guía completa para navegar de forma segura por internet

En la era digital, navegar por internet se ha vuelto una actividad común en nuestras vidas cotidianas. Sin embargo, también es importante ser conscientes de los peligros potenciales que existen en la red, como el robo de identidad, el phishing, el malware y el spyware, entre otros. En este manual, aprenderás a navegar de forma segura por internet con ejemplos concretos y recomendaciones útiles.

Guía completa para navegar de forma segura por internet

1. Mantén tu software actualizado Es fundamental mantener tu sistema operativo y tus aplicaciones actualizados, ya que las actualizaciones suelen contener correcciones de seguridad. Para asegurarte de que tienes la última versión, puedes activar las actualizaciones automáticas o revisar regularmente el sitio web del proveedor.
2. Utiliza contraseñas seguras Las contraseñas son la primera línea de defensa para proteger tus cuentas en línea. Utiliza contraseñas seguras y únicas para cada cuenta, con una combinación de letras, números y símbolos. Además, evita utilizar información personal o común, como fechas de nacimiento o nombres de mascotas.
3. Utiliza una VPN Una VPN o red privada virtual es una herramienta que encripta tu tráfico y protege tus datos mientras navegas por internet. Existen muchas opciones gratuitas y de pago, como NordVPN, ExpressVPN, Hotspot Shield, entre otros. Asegúrate de leer las políticas de privacidad antes de elegir una VPN.
4. Evita las redes públicas no seguras Las redes públicas no seguras, como las que se encuentran en aeropuertos, cafeterías o bibliotecas, pueden ser un riesgo para la seguridad de tus datos. Siempre que sea posible, evita conectarte a estas redes. Si necesitas conectarte a una red pública, utiliza una VPN para encriptar tu tráfico y proteger tus datos.
5. Utiliza software antivirus y anti-malware Un software antivirus y anti-malware es fundamental para proteger tu dispositivo de posibles amenazas en línea. Asegúrate de tener instalado un software actualizado y realiza escaneos periódicos para detectar y eliminar posibles amenazas.

6. Desconfía de correos electrónicos sospechosos El phishing es una técnica común utilizada por los hackers para robar información personal. Si recibes un correo electrónico sospechoso de una fuente desconocida o inusual, no lo abras ni hagas clic en ningún enlace adjunto. En su lugar, elimina el correo electrónico de inmediato.

7. Utiliza la autenticación de dos factores La autenticación de dos factores es una herramienta de seguridad adicional que protege tus cuentas en línea. Esta herramienta requiere que ingreses un código de seguridad enviado a tu teléfono móvil o correo electrónico después de ingresar tu contraseña. De esta manera, si alguien obtiene tu contraseña, no podrá acceder a tu cuenta sin el código de seguridad.
8. Utiliza sitios web seguros Cuando navegues por internet, asegúrate de que los sitios web que visitas son seguros. Para hacerlo, verifica si la dirección comienza con "https" en lugar de "http". Además, asegúrate de que el sitio web tenga un certificado de seguridad válido. Si tienes dudas sobre la seguridad del sitio web, no ingreses información personal ni hagas transacciones con tarjetas de crédito. Actualiza tus dispositivos y aplicaciones: Asegúrate de que tus dispositivos y aplicaciones estén actualizados con las últimas versiones de software y parches de seguridad. Los fabricantes de software lanzan actualizaciones para solucionar problemas de seguridad y proteger los sistemas de vulnerabilidades. Configura las actualizaciones automáticas en tus dispositivos para que se descarguen e instalen automáticamente.
9. Utiliza contraseñas seguras: Las contraseñas son la primera línea de defensa para proteger tus cuentas en línea. Utiliza contraseñas seguras y únicas para cada cuenta y cambia las contraseñas periódicamente. Las contraseñas seguras deben contener una combinación de letras mayúsculas y minúsculas, números y símbolos. Evita utilizar información personal en tus contraseñas, como tu nombre, fecha de nacimiento o número de teléfono.

10. Utiliza la autenticación de dos factores: La autenticación de dos factores es una capa adicional de seguridad que requiere que los usuarios ingresen dos tipos de información para acceder a una cuenta. Normalmente, esto significa ingresar una contraseña y un código de seguridad enviado a tu teléfono móvil o correo electrónico. Esto dificulta que los piratas informáticos accedan a tus cuentas, incluso si han obtenido tu contraseña.
11. Utiliza el sentido común: Si algo parece demasiado bueno para ser verdad, probablemente lo es. No hagas clic en enlaces sospechosos o descargues archivos de fuentes no confiables. Si recibes un correo electrónico o un mensaje que parece sospechoso, no respondas ni compartas información personal. Si tienes dudas sobre la legitimidad de un sitio web o un correo electrónico, realiza una búsqueda en línea para ver si hay informes de fraude o phishing.
12. Utiliza software de seguridad: Instala software de seguridad en tus dispositivos, como un antivirus y un firewall. Estos programas pueden detectar y bloquear virus, malware y otros tipos de amenazas en línea. Configura el software de seguridad para que se actualice automáticamente y realice exploraciones periódicas en tus dispositivos.

Siguiendo estas prácticas de seguridad en línea, puedes reducir significativamente el riesgo de ser víctima de fraudes en línea y proteger tu información personal y financiera. Recuerda que la seguridad en línea es un proceso continuo, por lo que es importante estar siempre alerta y actualizado sobre las últimas amenazas y medidas de seguridad.

Vivamos Seguros Navegando.



En la actualidad, internet se ha convertido en una herramienta imprescindible para la mayoría de las personas. A través de ella, podemos comunicarnos con amigos y familiares, trabajar, estudiar, comprar productos, entre muchas otras cosas. Sin embargo, también existen riesgos asociados al uso de internet, como virus, malware, phishing, estafas y robo de información personal. Por ello, es importante reflexionar sobre cómo podemos navegar de forma segura por internet. En primer lugar, es fundamental contar con un buen software de seguridad, como un antivirus y un firewall, para proteger nuestro equipo de posibles ataques. También es recomendable utilizar contraseñas seguras y cambiarlas periódicamente, así como evitar compartir información personal sensible en internet.

Además, debemos ser conscientes de los riesgos asociados a la navegación en redes sociales y correos electrónicos, ya que son medios frecuentes para la propagación de virus y estafas. Debemos tener cuidado