Instituto Nacional de Ciberseguridad

Decálogo de buenas prácticas

1. **Utilizar un antivirus que analice todas las descargas.** Asegúrate de tener un antivirus instalado, actualizado al día para que reconozca el mayor número de virus, y realiza análisis regularmente de todo el sistema.
2. **Mantener el sistema operativo y el navegador actualizados.** Los virus aprovechan los agujeros del SO y navegador para infectar los dispositivos. Como contramedida los fabricantes corrigen los programas a través de actualizaciones. La mejor forma para estar protegido es activar las actualizaciones automáticas de tu SO, navegador, plugins del navegador y resto de aplicaciones
3. **Cuidar las contraseñas.** Al introducirlas se debe estar seguro de que es la página correcta, ya que puede parecer idéntica a la legítima y tratarse de una suplantación (phishing). No se debe utilizar la misma contraseña en diferentes servicios porque si acceden a una cuenta fácilmente podrán acceder al resto. Tampoco se ha de compartir las contraseñas con nadie, aunque digan que son del servicio técnico, los servicios respetables nunca solicitarán las contraseñas por propia iniciativa.
4. **Confíar en la web, pero sin ser ingenuo.** Hay que permanecer alerta, no todo lo que se dice en Internet tiene por qué ser cierto. Ante la duda, contrastar la información en otras fuentes de confianza.
5. **No hacer clic en enlaces que resulten sospechosos.** Se debe ser precavido antes de seguir un enlace al navegar, en el correo, en la mensajería instantánea o en una red social. Los mensajes falsos que los acompañan pueden ser muy convincentes con el fin de captar la atención del usuario y redirigirle a páginas maliciosas.
6. **Tener cuidado con lo que se descarga.** No hay que precipitarse y descargarse cualquier cosa, ya que nuevas amenazas surgen cada día y los antivirus no pueden combatirlas todas. Hay que descargar los ficheros solo de fuentes confiables y los programas desde sus páginas oficiales.
7. **Desconfíar de los correos de remitentes desconocidos.** Ante la duda, es recomendable no responder a los mismos y eliminarlos directamente
8. **No abrir ficheros adjuntos sospechosos.** Si es de un conocido hay que asegurarse de que realmente lo quiso enviar. Los virus utilizan esta técnica para propagarse entre los contactos del correo, así como los contactos de la mensajería instantánea y de las redes sociales.
9. **Pensar antes de publicar.** Los servicios actuales de Internet facilitan las relaciones sociales, lo que conlleva a su vez se publiquen mucha información sobre las personas (datos personales, imágenes, gustos, preferencias, etc.). Dado el valor que tiene esta información, y las repercusiones negativas que puede tener su uso inadecuado por parte de otras personas, es necesario que se gestionen adecuadamente.
10. **Conoce los riesgos asociados al uso de Internet.** ¡Hay que mantenerse al día! Es aconsejable estar suscrito a los boletines de correo de la OSI, que incluyen los últimos avances de actualidad.
    https://www.osi.es/es/boletines/suscribirse
    comprobar su tu correo ha sido hakeado:
    https://haveibeenpwned.com/
    *** Fuente de la noticia: INCIBE