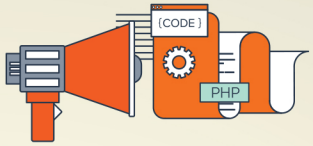
BUENAS PRÁCTICAS DE CIBERSEGURIDAD

SIEMPRE:

- Mantén actualizado el sistema operativo, aplicaciones y antivirus de los dispositivos (computadora personal, celular, tabletas, etc.).
- Realiza regularmente copias de seguridad.
- Utiliza software legal y descarga programas de sitios oficiales.
- Utiliza contraseñas robustas (letras, números, metacaracteres).
- Utiliza herramientas de seguridad (antivirus, firewall personal, etc.).



MENSAJERÍA INSTANTANEA (CHAT):

- No aceptes invitaciones a sitios WEB sospechosos.
- Rechaza archivos adjuntos.
- Ten precaución al agregar a contactos desconocidos.
- No facilites datos confidenciales.
- Ignora/borra mensajes de origen desconocido.
- Revisa que el intercambio de mensajes esté cifrado.

NAVEGACIÓN:

- No descargues/ejecutes archivos desde sitios sospechosos.
- Analiza con un antivirus antes de abrir cualquier archivo.
- Mantén actualizado los navegadores de Internet.
- Borra cookies, archivos temporales e historial de los navegadores.

CORREO ELECTRÓNICO:

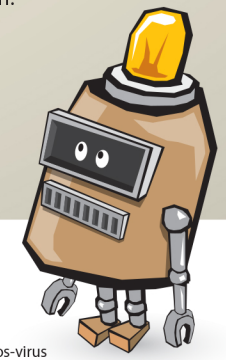
- No aceptes invitaciones a sitios WEB sospechosos.
- Rechaza archivos adjuntos.
- Ten precaución al agregar a contactos desconocidos.
- No facilites datos confidenciales.
- Ignora/borra mensajes de origen desconocido.
- Revisa que el intercambio de mensajes esté cifrado.

DISPOSITIVOS MÓVILES:

- No dejes la laptop desatendida en lugares públicos.
- Utiliza un candado físico.
- Activa y utiliza algún métodos de bloqueo (contraseñas, patrón) de los dispositivos.
- Habilita bluetooth siempre y cuando sea necesario.
- No aceptes conexiones de dispositivos desconocidos.
- Utilizar herramientas para localizar, bloquear e incluso eliminar información del dispositivo.
- Lee los acuerdos de usuarios del software que instalas.
- Cuidado con las redes wifi públicas a las que te conectas.

REDES SOCIALES

- No publiques más información de la necesaria.
- Revisa si tu perfil está visible a los buscadores de Internet.
- Antes de publicar información personal en una red social, plantéate qué quieres compartir y con quién.
- Revisa las opciones de configuración de cada red social para tener controlados los principales aspectos de privacidad y seguridad.
- Desactiva la geolocalización en tus redes sociales.
- No olvides cerrar siempre tu sesión.



Mtra. JULIA J. BERNUY S.
Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas

REFERENCIAS

https://www.seguridad.unam.mx/usuario-casero
https://digipadres.com/
https://www.is4k.es/jovenes
https://defensorasdigitales.org/que-es-la-violencia-digital/
https://www.osi.es/es/actualidad/blog/2014/07/18/fauna-y-flora-del-mundo-de-los-virus
http://inicio.ifai.org.mx/SitePages/ifai.aspx