¿Por qué es importante la seguridad en Internet?

En un mundo conectado estamos al alcance de ciberdelincuentes y otras personas que buscan la manera de aprovechar descuidos o prácticas erróneas.

El software malicioso (malware) inunda Internet y puede ocasionar molestias leves o ser causante de graves problemas personales. Puede colarse en nuestros equipos conectados, en caso de ataques, o puede que seamos nosotros, sin darnos cuenta, quienes lo introduzcamos.

La ciberdelincuencia también utiliza el engaño y busca sacar provecho de nuestros errores: entrega de información sensible en el lugar equivocado o dar por buena una información fraudulenta... Otras veces, por ejemplo, al no utilizar una contraseña robusta permite que sea fácilmente robada para que otras personas tomen el control de nuestros dispositivos y aplicaciones, y por tanto de nuestra vida e información digital.

¿Qué peligros acechan?

Utilización del equipo para finalidades ajenas. Se hace uso del dispositivo de la víctima de forma impersonal para acciones como la recopilación de información de navegación, la muestra de publicidad, o la integración en una botnet (red de bots o "zombies") utilizada para cometer otros ciberdelitos. La infección pretende pasar desapercibida y es habitual que quien la sufre no sea consciente.

Secuestro del dispositivo mediante ransomware. Bloquea el acceso a una parte del dispositivo y exige una condición, por lo general un pago, para liberarlo.

Acceso a datos sensibles o información personal. El robo de información personal (claves, fotografías, datos bancarios, documentos de identificación…) puede tener las más variadas finalidades y suele exigir una intervención complementaria de quien ataca. Entre las consecuencias más dañinas está la sextorsión o la usurpación de identidad, pasando por el ciberacoso o el espionaje mediante la activación de la cámara o el micrófono.

Estafas y fraudes. Tras el engaño, la víctima se ve expuesta al robo de dinero u otros bienes digitales… o incluso implicada en la comisión de ciberdelitos.

Marco legal en El Salvador

La Ley Especial contra los delitos informáticos y conexos de El Salvador fue aprobada en 2016 y regula las conductas delictivas cometidas por medio de las Tecnologías de Información y Comunicación (TIC). Específicamente, el capítulo IV está destinado a los delitos informáticos contra niñas, niños y adolescentes.

Para tener muy en cuenta

- El celular, la tableta o una laptop son dispositivos que cuando se conectan a Internet se convierten en objetivos vulnerables.
- Existen muchos tipos de amenazas informáticas, de malware, que pueden llegar por los distintos canales de la Red y cuyos efectos negativos son muy variados.
- Cuando tus dispositivos son infectados o atacados, incluso aunque no te estés dando cuenta de ello, eres tú quien puede sufrir graves consecuencias personales.
- Cuidar tu propia ciberseguridad es una labor personal cotidiana que debe irse adaptando a nuevas circunstancias y aplicaciones.
- Es muy importante que también prestes atención y apoyo a las demás personas. Si ellas están protegidas aumenta tu seguridad porque vivimos en conexión.
- Para mantenerte a salvo, es imprescindible que cuentes con un programa de seguridad o antivirus en todos tus dispositivos (celulares, tabletas o computadoras) y que tengas contraseñas seguras para el acceso a tus servicios, perfiles y aplicaciones online.

Referencias de apoyo

www.mined.gob.sv

www.cienciaytecnologia.edu.sv

www.miportal.edu.sv

www.unodc.org/ropan/es

www.dialogando.com.sv

Disfruta y cuídate en el Internet :)

Proyecto educativo de prevención del ciberdelito y para el buen uso del Internet

CIBERSEGURIDAD

¿Sabes que la seguridad de tus dispositivos es vital para ti?

¿Podrías identificar qué hacer para mantenerte a salvo?

UNODC | La Declaración de Doha: PROMOVER UNA CULTURA DE LEGALIDAD | educación para la justicia

MINISTERIO DE EDUCACIÓN GOBIERNO DE EL SALVADOR

Telefónica | movistar

State of Qatar

PantallasAmigas

Pautas para protegerte de las amenazas a tu ciberseguridad

- Usa un antivirus en los dispositivos (computadora, celular o tableta) con los que te conectes a Internet. Los hay gratuitos y para todos los sistemas operativos.
- Mantén tu sistema operativo y aplicaciones actualizadas porque incluyen refuerzos de seguridad.
- Cuando descargues apps, hazlo desde las tiendas autorizadas. Desconfía del software de dudosa legalidad o procedencia porque puede incluir malware.
- Evita acceder a enlaces o ficheros inesperados o de personas desconocidas. No los descargues de forma automática.
- Presta especial atención a dónde introduces tus contraseñas y quién te las pide. Cuando la dirección de una página web comienza por "https" significa que es segura y confiable.
- Conectarse a redes WiFi públicas y abiertas es arriesgado. Procura no realizar nada crítico porque tus comunicaciones podrían ser espiadas.
- Activa los servicios para compartir información de tu celular, como el bluetooth, únicamente cuando vayas a usarlos.
- Mantente alerta y contrasta las informaciones, las personas con las que te relacionas y los servicios que usas. Buscar datos o referencias online para comparar puede ayudar a descubrir fraudes y engaños.

La importancia de elegir contraseñas seguras

Las contraseñas son la primera protección del acceso a datos (conversaciones, imágenes…) y servicios personales que pueden ser utilizados para causarnos daño. Son la primera barrera de ciberseguridad, la puerta de entrada a nuestra vida digital y, como tales, deben ser robustas. Su elección es una decisión importante que se debe tomar con frecuencia.

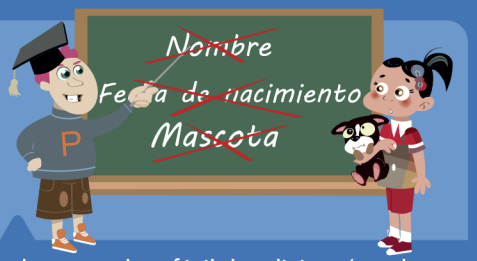
Ocho claves para una contraseña segura

Toda contraseña segura…

1

Debe tener al menos 8 caracteres

2



No puede ser un dato fácil de adivinar (nombre, fecha de nacimiento…).

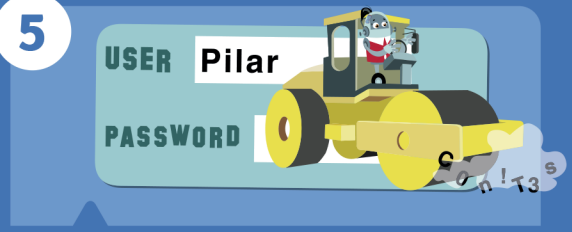
3

Tiene que incluir letras mayúsculas y minúsculas

4

Debe tener números y letras

5

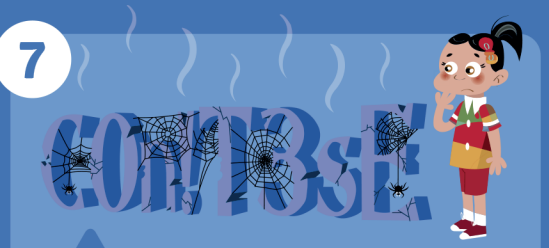


No debe dejarse escrita ni guardada sino introducirse cada vez que se use

6

Es un secreto que no debería compartirse con nadie ajeno a la familia

7



Debe ser cambiada de vez en cuando

8

Tiene que ser diferente para cada servicio, red social o app