ARL

Recomendaciones de seguridad para evitar fraudes por internet

Al igual que en el mundo real, en internet también hay personas que pueden engañarte.

Los delincuentes usan esquemas ingeniosos para defraudar a millones de personas cada año, combinando su astucia con las nuevas tecnologías, que hacen más sigilosa su acción delictiva. **Por esto es importante que cuides tus datos personales y financieros en el mundo digital.**

Verifica el registro de la empresa si vas a realizar algún tipo de compra o reserva de algún producto y servicio en línea. **Consulta previamente si aquella empresa está debidamente regulada,** llama a los teléfonos que proporcionan en el sitio web e investiga que la información brindada sea la correcta. Una persona o empresa que esconda sus datos personales o registro no es una buena opción para hacer negocios.

En la bandeja de entrada de nuestros correos electrónicos siempre hay algunos en los que envían **formularios en línea o se nos solicita que hagamos clic en un enlace sospechoso. Nunca lo hagas.** Bloquea el mensaje, al remitente y nunca descargues archivos adjuntos de correos de dudosa procedencia.

Intercambia información sólo con páginas que posean SSL (Secure Socket Layers). Este sistema emplea una llave pública para la encriptación en la cual el servidor será el único capaz de desencriptar la información con una llave secreta. El ícono del candado que aparece en tu navegador debe estar cerrado.

La Ingeniería social es un conjunto de **técnicas para manipular a las personas a través de engaño** telefónico o presencial, buscando apropiarse de su información personal y/o financiera como números de identificación, claves, códigos de seguridad, tarjetas o coordenadas.

Otra técnica utilizada por los delincuentes es la i**nvestigación de datos de las personas en redes sociales** y otras fuentes similares para obtener información que permita realizar suplantación de identidad o fraudes bancarios.

El clickjacking
o secuestro de clicks

En su forma más simple, es **poner botones invisibles u ocultos sobre otros botones** y hacen que los usuarios acepten desprevenidamente enviar información o instalar programas maliciosos.

Los Hoax
o correos en cadena

Son utilizados para **conseguir direcciones de correo electrónico para después enviar spam o realizar fraudes como el phishing.** Algunos tienen textos alarmantes sobre catástrofes o incluso la muerte, que supuestamente pueden ocurrirte si no reenvías el mensaje a todos tus contactos.

El Cross Site Scripting

Es una trampa que se produce sobre un sitio legítimo. Se basa principalmente en la vulnerabilidad de los sitios web y se aprovecha de los defectos de programación de las aplicaciones, formularios de registro o URL. Este tipo de código malicioso se introduce a través de enlaces en el sitio y permiten al ciberdelincuente realizar, desde el computador de la víctima, todas las acciones que le sean permitidas al sitio web vulnerado.

Cuando recibas correos electrónicos en los que se te solicite información personal, no los respondas. **Las empresas legítimas no utilizan mensajes de correo electrónico para solicitar este tipo de información.** En caso de duda, contacta a la empresa por teléfono o escribe la dirección web de la empresa en el navegador. No hagas clic en los vínculos de estos mensajes, ya que podrían conducirte a sitios web malintencionados y fraudulentos.

Cuando realices compras, operaciones bancarias, o visites sitios web que precisen de información confidencial, comprueba que haya una "S" tras las letras "http" en la dirección web, es decir: **https://www.ejemplo.com,** en lugar de http://www.ejemplo.com. La "s" significa seguro y debe aparecer siempre que estés en una zona en la que se te soliciten datos confidenciales. Otro de los signos que te indica que estás en una conexión segura es el **pequeño ícono de un candado que aparece en la parte superior del navegador,** normalmente en la esquina derecha izquierda.

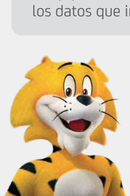
Presta atención a las políticas de privacidad de los sitios web y del software. Es importante que comprendas de qué modo una organización puede guardar y utilizar tu información personal antes de proporcionarles tus datos.

Usa contraseñas seguras. Hoy en día, las contraseñas son un elemento clave en Internet y son utilizadas para todo, desde encargar flores o efectuar operaciones bancarias en línea, hasta para conectarnos al sitio web de nuestra preferencia. Las contraseñas fuertes están formadas por **ocho caracteres como mínimo y utilizan una combinación de letras, mayúsculas, números y símbolos.**

No utilices ninguna de las siguientes opciones para tu contraseña: tu nombre, apellido, números de identificación o fechas de nacimiento. **Intenta seleccionar contraseñas muy sólidas y exclusivas** para proteger actividades como las operaciones bancarias en Internet.

Cambia las contraseñas con regularidad, al menos cada 90 días. De este modo, es posible limitar el daño causado por alguien que ya haya accedido a tu información. Si observas algo sospechoso con alguna de tus cuentas, lo primero que debes hacer es cambiar la contraseña. Recuerda desactivar la sugerencia “recordar contraseña” en las páginas en las cuales se te solicita ingresarla.

Para mantener un nivel de seguridad básico en Internet, es necesario disponer de varios tipos de software de seguridad. **Los programas de software de seguridad imprescindibles son los de firewall y antivirus.** El firewall es, por lo general, la primera línea de defensa del equipo, ya que controla quién y qué puede comunicarse con el equipo en Internet. Podríamos entenderlo como una especie de "policía" que vigila todos los datos que intentan entrar y salir de tu equipo en Internet.



Línea de atención 01 8000 511 414

arlsura.com