Gobierno de TLAQUEPAQUE

Unidos por la Ciudad que Queremos

SEGURIDAD DIGITAL EN EL HOGAR

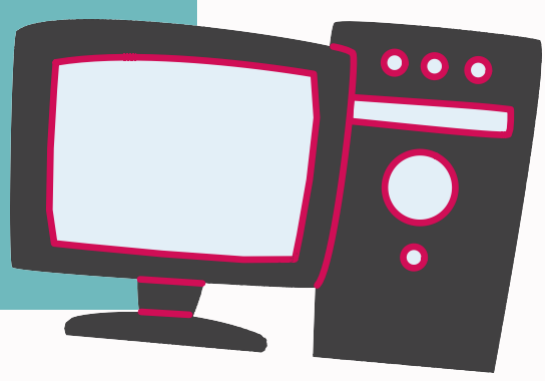
Usar su computadora. en la red doméstica puede presentar nuevos riesgos. Usted puede ayudar a reducirlo al hacer lo siguiente

- Usar un enrutador con capacidad de firewall/cortafuegos incorporada
- Mantener el antivirus actualizado

- Usar contraseñas únicas para cada sitio web/aplicación
- La contraseña debe ser compleja y larga
- Cambiar siempre las contraseñas que vienen asignadas

Comprobar las actualizaciones para su sistema operativo y software:

- Realizar actualizaciones periódicamente
- Habilitar actualizaciones automáticas



Gobierno de TLAQUEPAQUE

Unidos por la Ciudad que Queremos

SEGURIDAD DEL DISPOSITIVO MÓVIL

Los teléfonos inteligentes no están a salvo de los ataques cibernéticos, es por ello que debes tomar en cuenta estas recomendaciones.

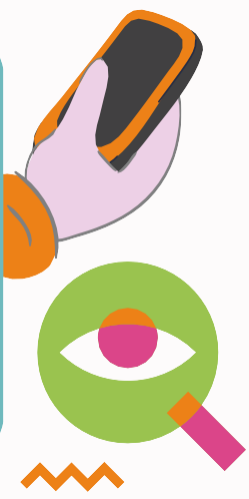
Tenga cuidado antes de:

- Hacer clic en los enlaces
- Abrir archivos adjuntos o imágenes

Los mensajes de texto y correos maliciosos pueden:

- Instalar virus
- Robar información
- Bloquear su dispositivo móvil

Recuerde que un número de teléfono pueden ser falsificados, así que, si recibe algo de un contacto que parece inusual, comuníquese con ellos a través de un medio alternativo para verificar si era legítimo.



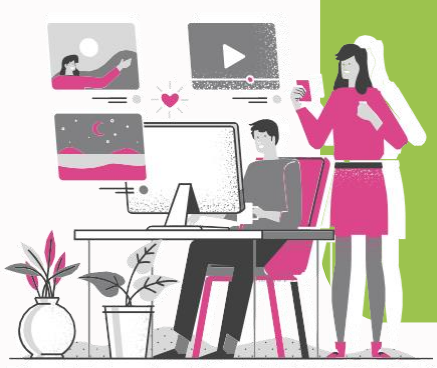
Gobierno de TLAQUEPAQUE

Unidos por la Ciudad que Queremos

¿QUÉ ES LA SUPLANTACIÓN DE IDENTIDAD (PHISHING)?

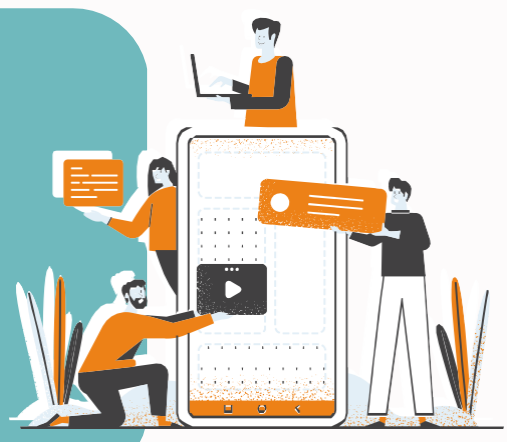
La suplantación de identidad (phishing) es una estafa por correo electrónico que busca robar datos (generalmente contraseñas), utilizando uno de estos métodos.

Enlaces que conducen a sitios web maliciosos/falsos.



Persuasión, es decir, lograr que usted realice acciones en nombre del estafador.

Documentos adjuntos que pueden infectar computadoras o redes completas con programa maligno.



Gobierno de TLAQUEPAQUE

Unidos por la Ciudad que Queremos

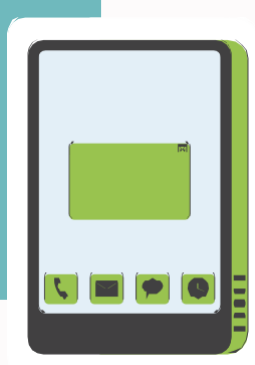
PHISHING, INSPECCIONAR ENLACES EN UNA COMPUTADORA

Los enlaces que espera recibir tienen más probabilidades de ser seguros, pero no siempre es así.

Si conoce al remitente, siempre puede comunicarse para confirmar, pero nunca responda al mismo correo electrónico para la confirmación, ya que el atacante, por supuesto, le responderá.

Inspeccione el enlace pasando el cursor sobre él y verificando que el texto que ve en el correo electrónico coincida con el enlace que aparece cuando pasa el cursor.

El procedimiento puede variar de una actualización de software a la siguiente. Puede terminar haciendo clic en un enlace peligroso por error.



Gobierno de TLAQUEPAQUE

Unidos por la Ciudad que Queremos

INGENIERÍA SOCIAL: DESCRIPCIÓN GENERAL

Ingeniería social es un intento de manipular a las personas para que entreguen información valiosa, credenciales o incluso dinero, por ejemplo:

Phishing: Situaciones que engañan a las personas para que compartan contraseñas o instalen malware a través de enlaces/archivos.
Spear phishing: Phishing personalizado dirigido a una empresa, empleado o ejecutivo.

Smishing: Mensajes SMS falsificados de "bancos", "autoridades sanitarias", etc.
Vishing: Phishing de voz, como ingeniería social por teléfono.

Baiting: Promesa de un artículo o premio utilizado para atraer a las víctimas, como dispositivos infectados con malware que se dejan deliberadamente para que otros los recojan y usen.
Tailgating: Alguien sin la autenticación adecuada que sigue a un empleado autenticado a un área restringida.

Pretexting: Los atacantes crean un pretexto, o situación inventada, para intentar robar la información personal de la víctima.
Quid Pro Quo: El atacante promete un beneficio a cambio de información. Este beneficio generalmente asume la forma de un servicio.