Buenas prácticas para evitar el robo de identidad

Precaución en los emails

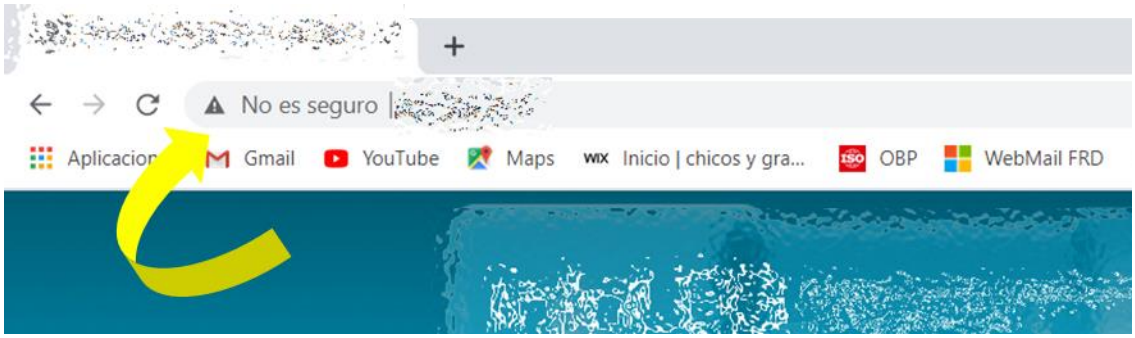
- Evitar abrir correos electrónicos de remitentes que no sean conocidos.
- Evitar la descarga o ejecución de archivos adjuntos inesperados o extraños.
- Evitar responder e-mails sospechosos y menos, enviar datos. No completar ningún pago.
- Si se sospecha de un engaño, seleccionar un nombre o parte del texto del email, copiar y pegar en un navegador de internet (como Google Chrome, por ejemplo), quizás se trate de un phishing conocido.
- Si se recibe correo en modo HTML[1] o texto enriquecido[2], convertir el mensaje a texto sin formato[3].

Precaución con los links de acceso en emails

- Evitar hacer clic en el enlace. Se sugiere acceder al sitio web desde el navegador: escribir la URL en el navegador (no copiar enlace). Puede ser un sitio web fraudulento.
- Comparar la URL del e-mail con la URL oficial.
- Revisar con mayor atención los enlaces acortados.
- ¿El celular no muestra detalles del enlace? Esperar a ver el correo desde la computadora.
- Acceder sólo a sitios seguros. Comienzan con https://...(el navegador muestra un candado cerrado) como en la siguiente figura:

- Evitar el acceso a sitios informados como no seguros por el navegador. Tal como aparece en la siguiente figura:

[1] Correo electrónico HTML: es diseñado como un sitio web con la ayuda de gráficos, colores, enlaces, etc.
[2] Correo con formato de texto enriquecido: permite la misma configuración que Microsoft Word.
[3] Correo electrónico sin formato: contiene sólo texto y no admite configuración de la letra sobre tamaño, color, estilo, etc.



Administrar el software

- Mantener actualizado el sistema operativo de la PC, notebook, celular, tabletas, etc.
- Mantener actualizadas todos los programas, incluso antivirus. La mayoría de los antivirus puede detectar enlaces o archivos engañosos.

Cuidar el patrimonio

- Renovar periódicamente las claves de acceso a la cuenta bancaria, tarjeta de crédito y sitios de compras.
- Evitar almacenar datos de tarjetas de crédito/débito en los sitios web de pagos.
- Revisar regularmente movimientos de cuentas bancarias y tarjetas de créditos.

Redes sociales

- Seleccionar qué se publica sobre sí mismo y del entorno, sobre quién tiene acceso a las publicaciones.
- Un estafador podría utilizar esta información para legitimar el mensaje que envíe.

Informados

- Atención a notas periodísticas o campañas de prevención que informen sobre estafas y metodologías más recientes.