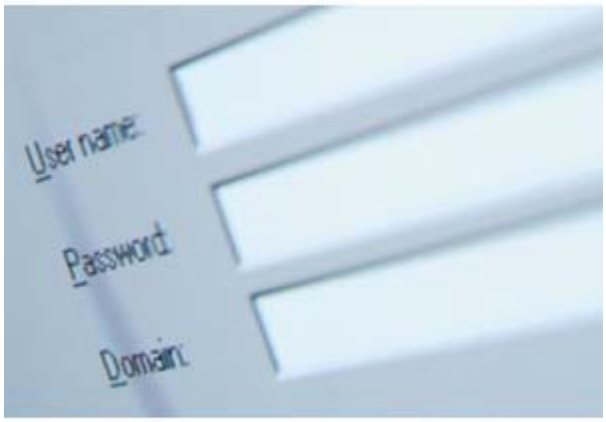
TIPS DE NAVEGACIÓN



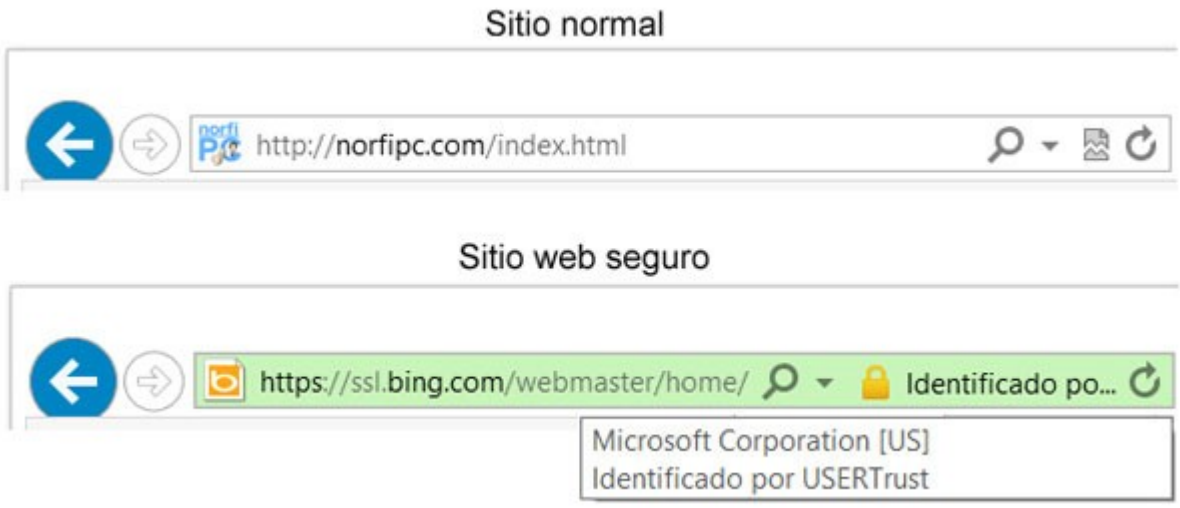
1. **Evitar los enlaces sospechosos**: uno de los medios más utilizados para direccionar a las víctimas a sitios maliciosos son los hipervínculos o enlaces. Evitar hacer clic en éstos previene el acceso a páginas web que posean amenazas capaces de infectar al usuario. Los enlaces pueden estar presentes en un correo electrónico, una ventana de chat o un mensaje en una red social: la clave está en analizar si son ofrecidos en alguna situación sospechosa (una invitación a ver una foto en un idioma distinto al propio, por ejemplo), provienen de un remitente desconocido o remiten a un sitio web poco confiable.

2. Ninguna empresa o entidad seria le solicitará información de carácter personal o contraseñas por correo electrónico. No debe responder a ninguna petición de información de estas características. Lo que se pretende con estas peticiones es conseguir acceso a sus datos personales o bancarios para usarlos de forma fraudulenta. No caiga en el engaño. Si tiene dudas llame a la entidad directamente.

3. **Evitar el ingreso de información personal en formularios dudosos:** cuando se enfrente a un formulario web que contenga campos con información sensible (por ejemplo, usuario y contraseña), es recomendable verificar la legitimidad del sitio. Una buena estrategia es corroborar el dominio y la utilización del protocolo HTTPS para garantizar la confidencialidad de la información. Tenga cuidado al momento de pagar facturas, movimientos bancarios, compras u otro tipo de negocio en línea. Evite hacerlo en computadores públicos, tabletas o smartphones prestados e incluso conectado desde redes inalámbricas libres y siempre digite la página a la cual desea ingresar siempre que vaya a realizar este tipo de movimientos.

¿Cómo saber cuándo un sitio web es seguro?

Los sitios web como bancos o cualquiera donde se vaya a efectuar una transacción financiera, usan el protocolo SSL de conexión segura. Puede saberlo fácilmente mirando la dirección del sitio en la barra de direcciones del navegador. La dirección URL comienza con HTTPS a diferencia de los sitios normales.Se muestra también un botón de identidad que debe ser de color azul o preferentemente verde con el nombre de la compañía.



4. **Utilizar contraseñas fuertes**: Se recomienda la utilización de contraseñas fuertes, con distintos tipos de caracteres y una longitud de al menos 8 caracteres, no compartirla y menos tener una sola contraseña para todos los sitios a los que ingresa, así como e-mails. Lo mejor es tener una contraseña diferente para cada cuenta y cambiarlas periódicamente.
5. **Tener cuidado frente a correos o sitios web poco confiables:** No entregar datos en los mensajes que pidan el ingreso de contraseñas y redirijan a páginas no seguras o que causen sospecha.
6. No responda a ofertas no solicitadas que le piden su información por correo, e-mail, teléfono o chat.
7. Cuide el tipo de información que publica y comparte en las redes sociales y chats.
8. Evite acceder a su banco o correo electrónico en computadores públicos, compartidos o de dudosa seguridad. En estos casos, lo recomendable es asegurarse de que tiene un antivirus comercial con protección de Internet e intentar no usar el teclado para introducir las contraseñas.
9. Cambie de vez en cuando sus contraseñas por otras completamente diferentes, especialmente las de accesos importantes como a bancos o a correo electrónico.

NOTA: Si presenta dificultades con el procedimiento descrito en este documento, por favor repórtelo a través de la plataforma **SUSI.**