PROTÉGETE DEL PHISHING

INSTITUTO DE PREVISIÓN MILITAR


SYSTEM HACKED


Phishing

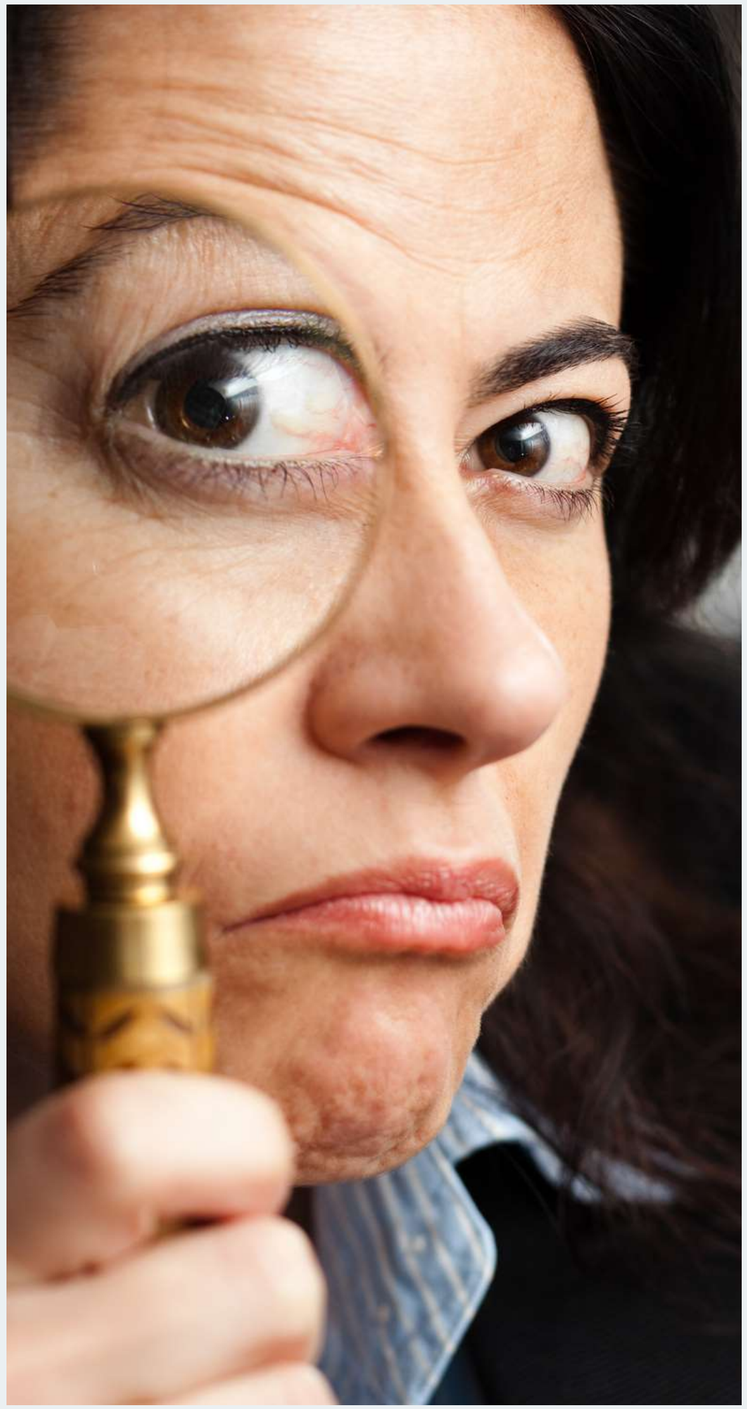

CREDIT CARD

¡ATENCIÓN!

El phishing es una táctica fraudulenta utilizada por delincuentes para engañarte y obtener información confidencial, como contraseñas y datos bancarios.

Estos estafadores suelen enviar correos electrónicos o mensajes de texto falsos que parecen legítimos, pero en realidad son trampas.

Recuerda, nunca debes proporcionar información personal o financiera a través de estos medios sin verificar su autenticidad primero. Mantente alerta y protege tu información.



¡CUIDADO CON LOS CORREOS ELECTRÓNICOS SOSPECHOSOS!

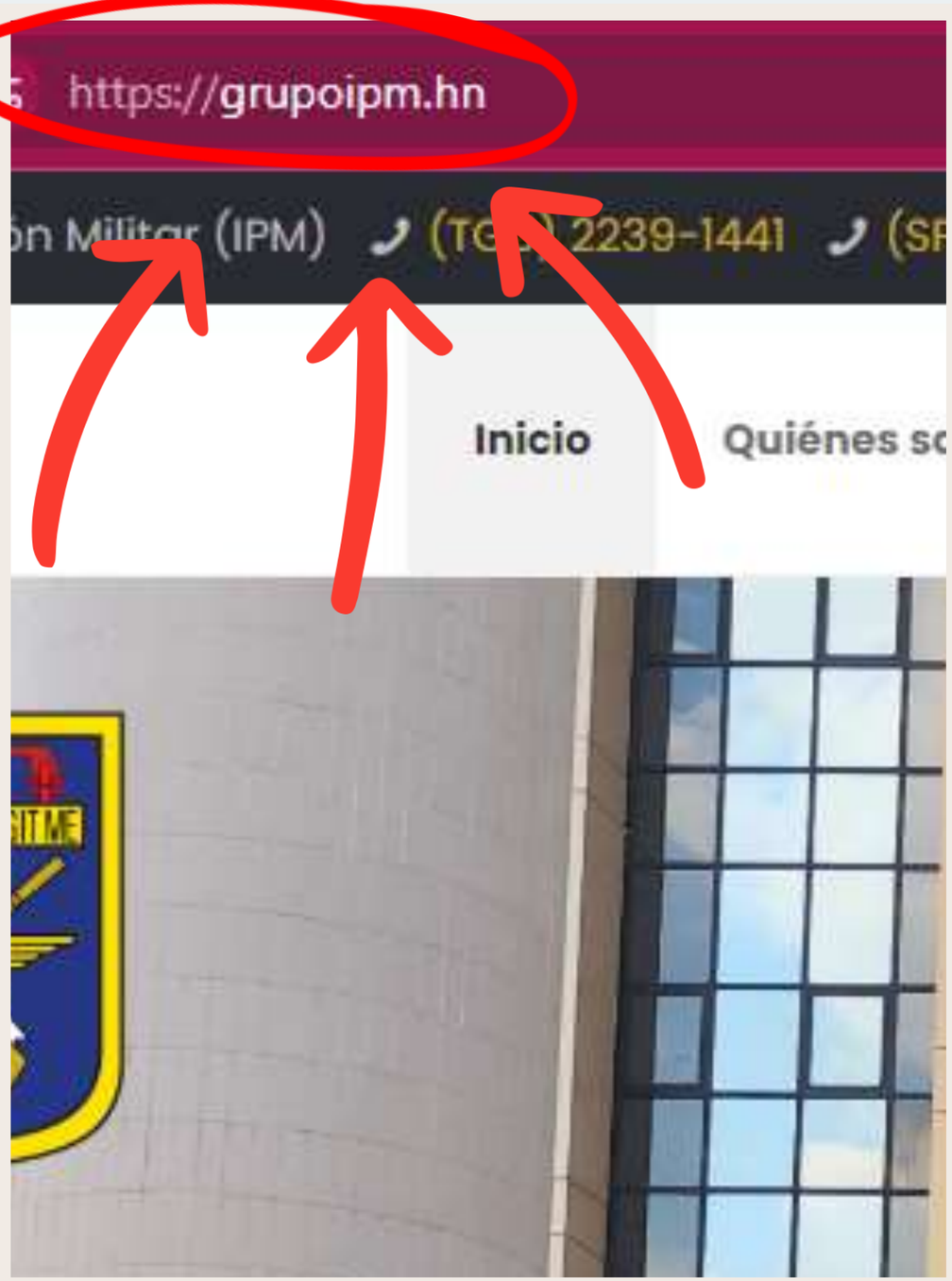
Los estafadores utilizan errores de ortografía, direcciones de correo electrónico extrañas y solicitudes de información personal para engañarte.

Si recibes un correo electrónico que parece sospechoso, no hagas clic en ningún enlace ni descargues archivos adjuntos.

En su lugar, verifica la autenticidad del remitente y comunícate directamente con el Instituto si tiene dudas.

¿COMO SABER SI UN SITIO WEB ES SEGURO?

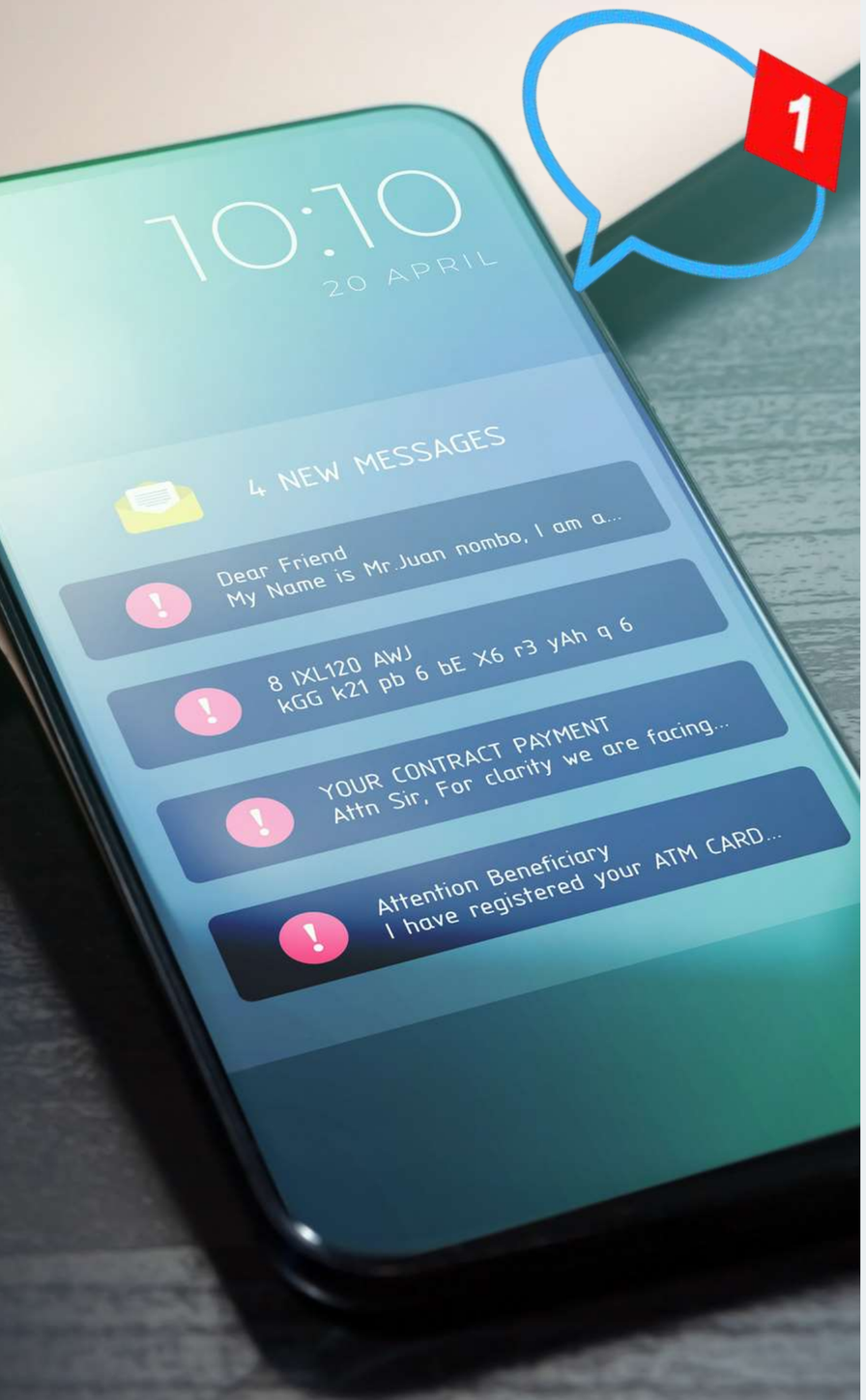
Busca el candado en la barra de direcciones y asegúrate de que la URL comience con "https". Estas son señales de que el sitio web utiliza una conexión segura. Nunca ingreses información personal o financiera en sitios web no seguros y evita hacer clic en enlaces sospechosos.



PROTEGE TU PRIVACIDAD EN LÍNEA

MANTÉN TUS CONTRASEÑAS SEGURAS

Usa contraseñas únicas y fuertes para cada cuenta y cámbialas regularmente. Evita compartir tus contraseñas con otras personas y considera utilizar un gestor de contraseñas para mantenerlas seguras. Tus contraseñas son la primera línea de defensa contra el phishing, así que asegúrate de protegerlas adecuadamente.



LOS DISPOSITIVOS MÓVILES TAMBIÉN SON VULNARABLES AL PHISHING

Ten cuidado con los mensajes de texto fraudulentos y las aplicaciones maliciosas. Descarga aplicaciones solo de fuentes confiables y mantén actualizado tu software de seguridad. No respondas a mensajes sospechosos y protege tu dispositivo móvil contra el phishing.

LA SEGURIDAD CIBERNETICA ES RESPONSABILIDAD DE TODOS

Tanto los usuarios como las instituciones financieras tienen un papel que desempeñar en la protección contra el phishing y otras amenazas en línea.

Mantente informado, educa a otros sobre los riesgos y trabaja en colaboración para mantener seguras tus cuentas y datos financieros.

Juntos, podemos hacer frente al phishing y proteger nuestra seguridad en línea.

Mantén tu software actualizado para protegerte contra vulnerabilidades de SEGURIDAD CONOCIDAS

Esto incluye sistemas operativos, navegadores web, aplicaciones y programas antivirus. Las actualizaciones periódicas pueden parchear posibles brechas de seguridad y ayudar a prevenir ataques de phishing y malware.

¿TE SOLICITAN UNA ACCIÓN URGENTE EN UN CORREO ELECTRÓNICO O MENSAJE?

Detente y evalúa la situación. Los estafadores a menudo intentan presionar a las personas para que actúen rápidamente sin pensar. Tómate tu tiempo para investigar y verificar la autenticidad de la solicitud antes de tomar cualquier medida.

¿Recibiste una oferta irresistible por correo electrónico o mensaje de texto?

Piénsalo dos veces antes de actuar. Los estafadores a menudo utilizan ofertas falsas para atraer a las víctimas y robar su información personal o financiera. Si suena demasiado bueno para ser verdad, es probable que sea una estafa.

¡CUIDADO CON LOS ENLACES ENGAÑOSOS!

Los estafadores pueden ocultar enlaces maliciosos detrás de palabras o imágenes aparentemente inofensivas. Antes de hacer clic en un enlace, pasa el cursor sobre él para ver la URL completa. Si parece sospechosa o no coincide con el sitio esperado, no hagas clic.