Ciudad de México, a 29 de noviembre de 2024

Comunicado 73

La SSPC advierte sobre páginas de comercio electrónicas y servicios de paquetería falsos

La Secretaría de Seguridad y Protección Ciudadana (SSPC), a través de la Dirección General de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico, alerta sobre páginas de comercio en línea fraudulentas, de servicios de mensajería y paquetería apócrifos; y brinda recomendaciones a la ciudadanía para evitar ser víctimas de ciberdelitos.

Derivado del aumento del comercio electrónico en internet, los ciberdelincuentes han ampliado su alcance, mediante la utilización de tácticas de ingeniería social para crear correos electrónicos o mensajes de texto semejantes a los de empresas de paquetería reconocidas. Estos mensajes suelen contener enlaces maliciosos o archivos adjuntos ocultos que, al ser abiertos, pueden comprometer la seguridad del usuario, con el robo de datos personales o financieros.

Entre las prácticas fraudulentas más comunes está el robo de cuentas de mensajería instantánea, donde los estafadores se hacen pasar por representantes de empresas de paquetería y afirman tener un paquete pendiente por entregar, por lo que solicitan confirmar la identidad mediante un código que supuestamente será enviado. Una vez que los usuarios comparten este código, los ciberdelincuentes obtienen acceso a las cuentas de mensajería.

De esta forma se cometen delitos como extorsión y otras prácticas, entre ellas:

• Phishing: Los ciberdelincuentes buscan obtener información confidencial, contraseñas y números de tarjetas de crédito, mediante la suplantación de identidad en correos electrónicos o mensajes falsos.

• Instalación de malware: Se infectan dispositivos con virus, ransomware o spyware, para comprometer la seguridad y privacidad del usuario.

• Fraude financiero: Se utilizan engaños para inducir a las personas a realizar pagos.

• Robo de identidad: Al obtener información personal, los delincuentes pueden usurpar la identidad de las víctimas, abrir cuentas bancarias falsas o realizar actividades fraudulentas en su nombre.

• Extorsión y chantaje: Se exige dinero a las víctimas para restaurar el acceso a sus datos o dispositivos.

Por lo anterior, la SSPC recomienda verificar la autenticidad de los mensajes recibidos de empresas de paquetería, examinar el remitente, sobre todo errores de ortografía o gramática, evitar hacer clic en enlaces o descargar archivos adjuntos de mensajes que no parezcan legítimos.

Además, acceder al sitio web oficial de la empresa sin hacer clic en enlaces de mensajes de correo electrónico o de texto, instalar y mantener actualizado un software antivirus y antimalware en los dispositivos, informar a la familia sobre estos riesgos y no proporcionar información personal o financiera en respuesta a mensajes no solicitados.

Cabe mencionar que las empresas legítimas de paquetería no suelen solicitar este tipo de información a través de mensajes de texto o correos electrónicos.

La SSPC invita a los usuarios a mantenerse atentos para reducir el riesgo de caer en incidentes relacionados con mensajes falsos de paquetería, así como proteger datos y dispositivos contra posibles amenazas en línea.

—oo0oo—