



Policía Cibernética alerta sobre incremento en suplantación de identidad en redes sociales

La dependencia alertó que se reciben aproximadamente 300 reportes de víctimas de suplantación de identidad a través de internet o llamadas telefónicas

Juan Hernández

Ante el aumento de reportes de suplantación de identidad en redes sociales, la Unidad de Policía Cibernética, de la Secretaría de Seguridad Ciudadana (SSC-CDMX), emite recomendaciones a la ciudadanía para evitar que su información personal sea utilizada por estafadores. La dependencia alertó sobre esta situación, pues cada mes, el personal especializado de la Policía Cibernética recibe aproximadamente 300 reportes de víctimas de suplantación de identidad, ocurridos principalmente

en distintas plataformas de redes sociales, sitios web, llamadas telefónicas o mensajes SMS. Se detalló que el modo de operar de los estafadores que ocupan las redes sociales para realizar esas prácticas ocurre cuando utilizan información personal de otra persona sin su consentimiento para crear un perfil falso o engañar a otros usuarios. Esto puede incluir el uso de fotos, nombres, información biográfica y cualquier otro detalle que les permita hacerse pasar por alguien más.

Este tipo de incidentes puede llevar a situaciones tanto de acoso, difamación, robo de información personal y financiera, así como daños a la reputación de la persona afectada y la suplantación de identidad, la cual también

puede estar relacionada con actividades fraudulentas, ya que implica engañar y obtener un beneficio económico ilícito.

Otra forma de operar de los estafadores es la suplantación de identidad de empresas bancarias, donde engañan a las personas para obtener información confidencial o dinero de forma fraudulenta, mediante llamadas telefónicas, sitios web o correos electrónicos falsos, haciéndose pasar por representantes legítimos de instituciones bancarias o financieras. Durante las llamadas telefónicas, los estafadores obtienen información confidencial, como números de cuenta bancaria, contraseñas y códigos de verificación, de igual forma piden descargar una aplicación en los dispositivos que funciona como un acceso para los estafadores. **M**