PDI Advierte Sobre El Peligro De Los Delitos Cibernéticos

21/10/2021

Producto de la pandemia, y el mayor tiempo en que la comunidad pasa conectada, los delitos cibernéticos han tenido una explosión a nivel mundial en el último periodo en el amplio ámbito de ilícitos que esta temática implica, se podría decir que la delincuencia se trasladó a la pantalla de un computador o de un teléfono movil.

En la Brigada Investigadora del Cibercrimen Metropolitana atribuyen esto a que tras la entrada del COVID-19 en el escenario mundial, muchas de las actividades que se realizaban en forma presencial ahora se llevan a cabo de manera virtual, lo que aumenta el riesgo de ser víctima de algún delito asociado al uso de la tecnología.

Según el reporte estadístico de la brigada especializada, la cantidad de denuncias recibidas en la PDI por estafas y otras defraudaciones, a través de Internet, aumentaron significativamente durante la pandemia: un 29% al comparar el

2019 con el 2020, y un 89% si se consideran los cinco primeros meses de 2021 con igual período del año anterior.

En lo que va del año, entre enero y agosto del 2021-a nivel nacional- se han levantado 10.728 denuncias asociadas a delitos del área de Cibercrimen y 2.997 órdenes de investigar, contemplando delitos como almacenamiento de pornografía infantil, amenazas, espionaje y sabotaje informático, estafas, extorsión, phishing, grooming y usurpación de nombre.

Junto a lo anterior, los investigadores especializados en delitos cibernéticos, también han notado que entre las estafas "on line", la más frecuente es el "Sim Swapping", conocido también como "secuestro de WhasApp".

¿Cómo opera este ilícito? Principalmente captan a sus víctimas entre personas que publican sus números personales en redes sociales con el fin de vender un producto. Con el objetivo de tomar el control de sus cuentas de WhatsApp contactan a estas personas simulando ser compradores. Es en este momento donde empieza a operar el engaño: Le dicen al vendedor que quieren ir a buscar el artículo, pero necesitan que les entreguen un "código de posicionamiento global" que le llegarán por mensaje de texto (SMS), que les permitiría llegar a la dirección correcta. Este código es, en realidad, el que genera la aplicación de mensajería instantánea cuando un usuario desea cambiar su cuenta a un nuevo teléfono.

Con esta fachada, luego de obtener el código, el delincuente hace traspaso de la cuenta de la víctima a su propio teléfono, haciéndose pasar por ella para solicitarle dinero a sus contactos, mediante un nuevo engaño.