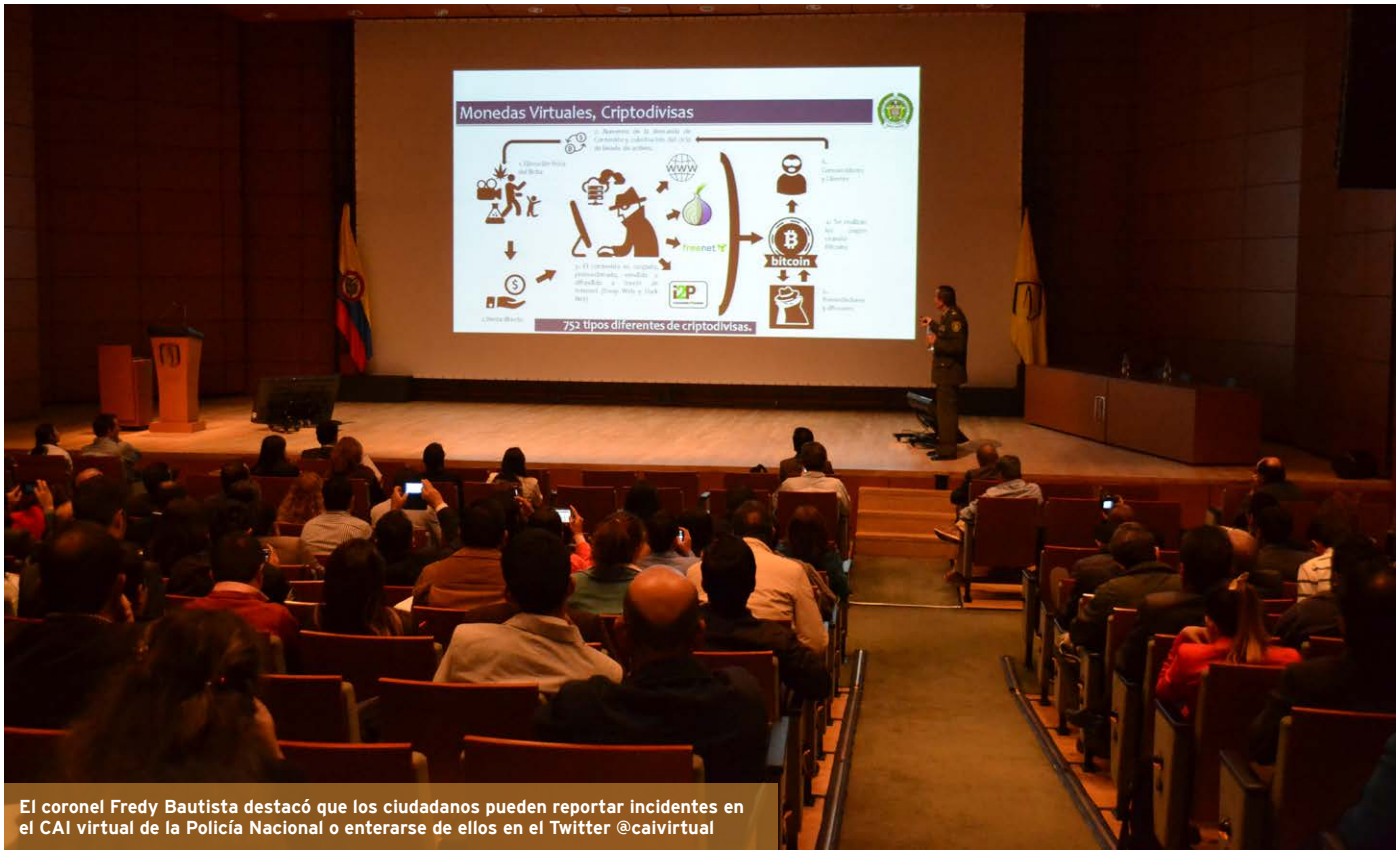
Las nuevas caras del ciberdelito

Al referirse a las modalidades más recientes de cibercrimen, el coronel Fredy Bautista, jefe de área del Centro Cibernético Policial, señaló que estamos en la era del secuestro de la información.



El coronel Fredy Bautista destacó que los ciudadanos pueden reportar incidentes en el CAI virtual de la Policía Nacional o enterarse de ellos en el Twitter @caivirtual

Foto: Natalia Fernanda Madrid Vidales

Todo lo que circula por el ciberespacio tiene un precio. Así lo han entendido los delincuentes que cada día inventan o perfeccionan formas de defraudar a las empresas y a las personas particulares.

A esas modalidades se refirió el coronel de la Policía Fredy Bautista, quien señaló que el incidente que más reportan los ciudadanos son los hurtos de sus productos de banca virtual por medios informáticos, no porque el sistema sea inseguro, sino porque seguimos cometiendo errores. Y resaltó que ahora los cibercriminales se enfocan en los teléfonos móviles, pues estos dispositivos están remplazando computadores y tabletas, y se han dado cuenta de que vulnerarlos es más productivo; en ellos aparecen ventanas emergentes que invitan a dar clic y así logran infectarlos. A menudo son correos que hablan de citaciones judiciales o de la DIAN, fotocomparendos o cobros a morosos.

El oficial insistió en la urgencia de generar hábitos de seguridad desde temprana edad y dijo que no se trata de proscribir o estigmatizar las redes sociales, sino de educar para que se usen con responsabilidad. También mencionó algunas de las estrategias de la Policía para combatir esos delitos (ver “La tecnología, gran aliada de la paz”, pág. 9).

Entre las modalidades más comunes de fraude cibernético están las siguientes:

- Secuestro de información. En todo el mundo crecen las extorsiones a empresas y personas debido a que los delincuentes utilizan *criptolockers* o *ransomwares* para cifrar determinados archivos o todo el disco duro de los computadores y piden rescate para recuperar los datos.
- Están surgiendo las criptodivisas y el ciberlavado y es difícil seguir la trazabilidad de los giros que se hacen mediante *bitcoins* o monedas digitales.
- Los datos como *commodity*, como mercancía o como producto son un desafío porque el objetivo de un ciberataque ya no es sustraer información valiosa de una empresa; un ciudadano común, cuyos datos tienen precio en los mercados ilegales, también puede ser atacado. Por ejemplo, los delincuentes pueden tomarle una fotografía a una persona

Para combatir el cibercrimen, la Policía colombiana trabaja con entidades como Europol, Interpol y el Innovation Global Complex en Singapur.

cuando está frente a una cámara web y venderla en la red profunda para que otros las usen en suplantaciones de identidad.

- Crimen como servicio o *crime as a service*. Ya no se trata de *hackers* que se presentaban como *robinhoods* que atacaban a las grandes corporaciones y desnudaban sus vulnerabilidades. Ahora son pirámides cuyos jefes tienen enlaces internacionales, en las que hay mercenarios informáticos vinculados a expertos lavadores de dinero y abogados para defender a los cabecillas. Esas redes desarrollan programas maliciosos o *malware* a la medida y los venden a criminales para que ataquen a las empresas, incluso a las pymes, y roben datos sensibles como números de cuentas bancarias. También se usan para la triangulación o difusión del dinero producto del cibercrimen.
- Compromiso de correos empresariales o *business e-mail compromise* (BEC). Los delincuentes generan correos electrónicos que enmascaran su origen real y convencen al usuario de que una empresa particular está solicitando una acción específica, como el envío de mercancía o datos.
- Servidores a prueba de balas o *bullet proof hosting*. Son servidores que mutan permanentemente de dirección IP o de sitio de *hosting,* de manera que resulte inocuo darlos de baja.
- *Darknet* o red profunda, una modalidad en la que se descarga un *software* que mantiene el anonimato y esconde la dirección IP. En ella operan sitios como Agora, Pandora y SilkRoad, donde se ofrecen droga y pornografía infantil.
- Ataques lógicos a los cajeros automáticos. La laminita metálica que insertaban en la ranura de la máquina para capturar los datos de la tarjeta ha sido remplazada por *software* malicioso que se le entrega a una persona que tiene contacto con la central encargada de administrar más de 400 cajeros de una entidad bancaria. El *software* infecta a los cajeros y con una sola tarjeta y una clave logran sustraer 60, 100 o 120 millones de pesos de una vez. Para ello usan programas como Dyre, Carbank, Timba y Corkon.
- Cadenas de voz en WhatsApp para generar pánico.
- *Phishing* asociado. Los delincuentes toman la información personal que los usuarios publican en las redes sociales y les envían correos que parecen reales para obtener los datos que les permiten acceder a sus computadores.
- Correos humanos o *money mules*. Son inmigrantes africanos, asiáticos o uno que otro latino, o personas de la tercera edad y jóvenes que se prestan para hacer o reclamar giros de dinero producto de actividades ilícitas y a cambio reciben un 10 % del valor total.
- *Bonus track*, una modalidad de fraude que infecta los dispositivos para vender drogas, pornografía infantil, armas o, incluso, servicios de sicariato. ■

> **"Es urgente generar hábitos de seguridad desde temprana edad. No se trata de proscribir o estigmatizar el uso de las redes sociales, sino de educar para que se usen con responsabilidad".**
>
> Coronel Fredy Bautista