

La Policía alerta del inminente 'boom' de las ciberestafas a través del móvil

El Grupo de Delitos Tecnológicos de la Jefatura Superior ha detectado ya casos de terminales que han sido pinchados con aplicaciones perniciosas

ZARAGOZA. Un teléfono móvil puede ser más peligroso que un bolsillo deshinchado. Con la diferencia de que por ese 'agujero' puede perder algo más que un puñado de monedas. Sin saberlo, y con un simple clic, podemos descargarnos una aplicación perniciosa y dar nuestro consentimiento a una ciberestafa. Cuando queramos darnos cuenta, nuestros ahorros se habrán ido por el desagüe de la red. Porque los 'malos' han aprendido a enmascararse en internet y están haciendo el agosto. La Policía advierte de que ahora han puesto sus ojos en los 'smartphone' (teléfonos inteligentes con línea de datos). Y no en el aparato en sí que, aunque tiene cierto valor, es cosa de 'raterillos'. Sino en las inmensas posibilidades para delinquir que ofrecen estos dispositivos, de los que ya hay 18 millones en España. Según el Grupo de Delitos Tecnológicos (GDT) de la Jefatura Superior de Aragón, el número de denuncias por móviles 'pinchados' es aquí todavía «testimonial». Sin embargo, aseguran que estas nuevas estafas van a experimentar un auténtico 'boom' a corto-medio plazo.

A lo largo de esta semana, por el campus Río Ebro –en un curso pionero organizado por la Universidad de Zaragoza y el Sindicato Unificado de Policía– han pasado todo tipo de especialistas en ciberdelincuencia: desde funcionarios del Cuerpo Nacional de Policía, a ingenieros informáticos, fiscales y magistrados. Y todos ellos han intentado quitarnos la venda de los ojos, para que veamos los riesgos que entrañan aparatos tan aparentemente inocentes y cotidianos como un teléfono móvil, un 'tablet' o un ordenador. «Todos ellos son tremendamente útiles, pero también peligrosos», asegura Diego Guerrero, funcionario del GDT y autor del libro 'Fraude en la red'. Y los números lo confirman, porque como se ha puesto de manifiesto en este curso, en las comisarías de la capital aragonesa se reciben a diario tres o cuatro denuncias por delitos perpetrados al amparo de las nuevas tecnologías. La tendencia es al alza y los ciberpolicías, aquí como en todos los sitios, empiezan a no dar abasto.

Pese a que son los casos de 'grooming' o ciberpederastía los que más alarma ciudadana provocan, estos, afortunadamente, representan un exiguo porcentaje de las denuncias que se tramitan en Aragón. «La inmensa mayoría



ALBERTO ARAGÓN

son estafas relacionadas con el uso fraudulento de tarjetas y portales de banca electrónica», explicaba en las jornadas Javier Marzo, otro de los especialistas adscrito al GDT. Lo primero que necesitan los delincuentes es conseguir nuestra clave y para ello utilizan varias fórmulas: los 'troyanos' (programas que se cuelan en el ordenador y recopilan todo tipo de datos), los capturadores de teclado (que roban las contraseñas recordando las teclas que pulsamos) y las microcámaras. Estas últimas se instalan en los propios cajeros automáticos y son muy difíciles de detectar.

Cuando ya tienen los números de las tarjetas y sus claves, los 'malos' las usan o las venden. Lo hacen también a través de la red, donde se puede adquirir un 'pack' de cien tarjetas pirateadas-robadas por entre 6 y 15 euros. Este material se usa para hacer todo tipo de compras en cibercomercios, causando un importante perjuicio al titular de la cuenta.

«Quien piratea, acaba estafado»

«Lo primero que hay que hacer para evitar infecciones es mantener actualizado el sistema operativo de nuestro ordenador. Pero también hay programas para detectar si ya se nos ha instalado algún troyano o capturador», advierte Javier Marzo, quien recuerda que «quien piratea, a la larga, acaba siendo estafado». Y según datos del último informe sobre piratería de la Business Software Alliance (BSA), un 48% de los aragoneses que usan internet piratean (los navarros, con un 28%, son los que menos lo hacen).

Las formas de estafar en la red son infinitas. Por ejemplo, con el llamado 'virus de la Policía', que bloquea el ordenador y aparece una pantalla que advierte al usuario de que ha sido cazado haciendo una descarga ilegal o consumiendo pornografía infantil. «Te pide que pagues 100 euros para desbloquearte, y más de 160 personas han picado en Zaragoza. Algunas, hasta dos veces», recuerdan los expertos de la Policía.

Pero volviendo a la estafa más generalizada y sabiendo que los ciberdelincuentes han empezado a echar sus redes en los 'smartphone', los especialistas dan algunos consejos. El primero, vincular nuestras cuentas 'online' a nuestro teléfono móvil. De esta forma, sabemos cada movimiento que se está haciendo en el banco y tenemos tiempo suficiente para ordenar que se paralice una operación. Caja Inmaculada cuenta ya con un servicio de alerta que funciona las 24 horas y avisa al titular cuando detecta que se están haciendo reintegros sospechosos con muy poco tiempo de diferencia y en lugares muy remotos.

Pero hay que estar alerta, porque los estafadores están intentando bloquear las alertas que el banco envía a los celulares. «Roban las claves bancarias 'online' con un troyano y haciéndose pasar por nuestra entidad nos piden el móvil, marca y modelo. Después, nos mandan un mensaje, supuestamente del banco, con una aplicación que infecta nuestro móvil. Con ella consiguen que los verdaderos mensajes del banco para confirmar transferencias solo les lleguen a ellos», explica Marzo. E insiste: la descarga de aplicaciones, solo en portales oficiales.

MIGUEL ÁNGEL COLOMA

«GROOMING» Y CIBERPEDÓFILOS

«COLARSE EN EL MAIL DE UN MENOR ES MUY SENCILLO»

'Grooming', 'sexting' o 'ciberbullying' son anglicismos con los que empiezan a familiarizarse muchos padres. Sobre todo, gracias a las charlas que está impartiendo el Grupo de Delitos Tecnológicos de la Policía en numerosos colegios. Se habla de 'grooming' cuando

un adulto se hace pasar por menor para conseguir material comprometedor de un adolescente. Y cuando lo consigue, empieza a extorsionarle para lograr más. Los expertos dicen que quienes lo practican son «pacientes e insaciables». En una de las últimas operaciones

se detectó un ciberpederasta que estaba en contacto con 150 menores en Zaragoza. Colarse en el mail de un menor es muy sencillo. Cuando el 'groomer' sabe la pregunta intuitiva de la cuenta, le saca la respuesta al niño chateando, alerta la Policía Nacional. **M. A. C.**

LOS JUECES NECESITAN PRUEBAS

«NOS MOVEMOS EN UN TERRENO RESBALADIZO»

Fiscales y magistrados han participado también en las jornadas sobre delitos tecnológicos celebradas esta semana en Zaragoza. Y lo han hecho para advertir de la dificultad que entraña perseguir este tipo de delincuencia por lo complicado que es conseguir pruebas. «Nos movemos en

un terreno resbaladizo, ya que cuando se interviene un teléfono móvil o un ordenador no solo se interviene una máquina. Dentro de ella puede haber fotos, archivos y material confidencial, por lo que hay que tener en cuenta el derecho a la intimidad», recordaba el titular del Juzgado de Instrucción

número 12 de Zaragoza, José Antonio Tello. Por ello, el magistrado pidió a los funcionarios de Policía que apliquen el principio de proporcionalidad y actúen «con precaución». «Ante la duda –dijo–, y para evitar que luego se invalide una prueba, lo mejor es pedir autorización judicial». **M. A. C.**