LA LUCHA CONTRA LA CIBERDELINCUENCIA

SERGIO GIMÉNEZ / FOCO SUR

Estafas online a empresas y particulares, pornografía infantil, ciberacoso y otros delitos cometidos a través de internet son cada vez más frecuentes y sofisticados, con el uso de herramientas como la IA para realizarlos.

MIGUEL BLANCO
FOTOS: VV.AA.

El auge de la tecnología y de herramientas y servicios como las redes sociales o la inteligencia artificial, además de modificar nuestros hábitos sociales y la forma de interactuar con el mundo, también está provocando un aumento de los delitos que se cometen a través de internet y el móvil. En 2024, según datos del Instituto Nacional de Ciberseguridad, Incibe, se produjeron 97.348 incidentes de este tipo, un 16,6% más que el año anterior.

'Phishing', 'man in the middle', 'ransomware', 'child grooming' o 'ciberbullying' son términos cada día más frecuentes en las noticias. Casi todos hemos recibido en alguna ocasión un correo electrónico pidiendo confirmar nuestro número de cuenta o cualquier otro dato personal para poder recibir un paquete de un servicio de mensajería que no estamos esperando. O hemos visto un aparentemente amistoso 'hola' en cualquier aplicación de mensajería o de red social procedente de alguien que no conocemos. O hemos descolgado el móvil y escuchado una voz robótica que te avisa de que has sido incluido en la selección de una oferta de trabajo de alguna conocida plataforma de búsqueda de empleo, a la que no te habías apuntado. Son algunas de las vías por las que los estafadores buscan conseguir datos personales de todo tipo, como copias del DNI, números de cuenta corriente o nóminas, con el objetivo de usarlos en sus actividades delictivas y, también, sacarte la mayor cantidad de dinero posible.

Las estafas y otros tipos de delitos online llevan años entre nosotros pero en los últimos cinco han aumentado con fuerza. El confinamiento provocado por la pandemia hizo que pasásemos más tiempo en internet y los ataques se multiplicaron. Por ello, las Fuerzas y Cuerpos de Seguridad del Estado tienen ya equipos especializados en la lucha contra la ciberdelincuencia, formados por expertos en rastrear el origen del delito por mucho que el autor haya ido borrando sus huellas en el medio digital.

El Grupo VI de Ciberdelincuencia de la Comisaría de Almería, uno de los más avanzados del país en la lucha contra este tipo de delitos y del que forman parte diez agentes, llevaba a cabo en marzo una operación que se saldaba con cinco detenidos en Roquetas de Mar. Eran cómplices de una estafa a una empresa de Mahón, que efectuó el pago de una factura en un número de cuenta proporcionado por los estafadores, en lugar de en el de la empresa que debía recibirlo. Los ciberdelincuentes habían conseguido interferir las comunicaciones por correo electrónico entre ambas compañías y habían enviado un email modificando el número de cuenta donde se debía enviar el pago, simulando ser la empresa que debía cobrarlo.

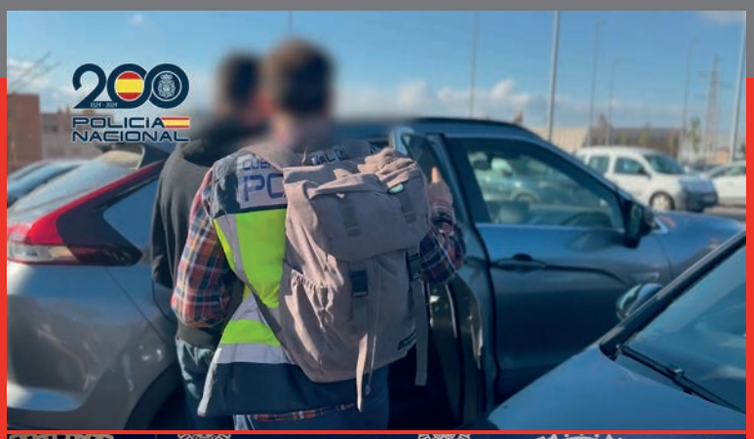
En abril, el Equipo @ de la Guardia Civil de Lorca, en Murcia, concluía la primera fase de una operación con la investigación de otros cinco personas en Roquetas de Mar por un caso similar contra dos empresas, una de Mazarrón, también en Murcia, a la que habían estafado 24.000 euros, y otra de Níjar, que había perdido 12.000.

Son ejemplos de estafas por el método 'man in the middle', una técnica por la que los estafadores, mediante técnicas de ingeniería social, consiguen vulnerar los servidores de correo electrónico de una empresa y, cuando detectan que esta va a recibir el pago de una factura, suplantan su correo electrónico y envían uno a la empresa deudora indicándoles un nuevo número de cuenta donde realizar el ingreso. Es el tipo de estafa online a empresas más frecuente.

EL FACTOR HUMANO

Los delitos online se pueden dividir entre los que se cometen contra el patrimonio, sea a empresas o particulares, o contra las personas, como el ciberacoso o la revelación de secretos. Dentro de los primeros, "las principales estafas que nos llegan son a grandes empresas, mediante 'man in the middle'", explica Juanfran Gómez, miembro del Grupo VI de la Comisaría de la Policía Nacional de Almería. En el caso de particulares, añade, cada vez se ven más "estafas en inversión en criptomonedas". Y en delitos contra las personas, "hemos visto un aumento de la pornografía infantil y también es importante el 'child grooming' y el acoso que se ejerce en los colegios entre compañeros".

En los casos de 'man in the middle', los autores de la estafa han estado haciendo un estudio previo y pormenorizado de las empresas, vigilando lo que publican en sus redes sociales, donde muchas veces particulares y empresas publican "más información de la que deberían". Una vez recogida toda esa información, "lo primero que hacen es una vulneración del servidor de correo de una de las empresas", explica el agente. A continuación, "cambian las reglas del correo de tal forma que si, por ejemplo, tienes que solo se pueden recibir correos de un determinado país, lo modi-



SERGIO GIMÉNEZ / FOCO SUR

SERGIO GIMÉNEZ / FOCO SUR

Arriba, Equipo @ de la Guardia Civil especializado en la lucha contra la ciberdelicuencia. A la izquierda, arriba, momento de la detención en Roquetas de Mar de uno de los acusados de estafar a una empresa de Mahón por el método 'man in the middle'; abajo, Juanfran Gómez, agente del Grupo VI de Ciberdelicuencia de la Comisaría de Policía Nacional de Almería.

fican". Durante un tiempo, los delincuentes hacen un seguimiento de la comunicación entre las empresas, hasta que ven que ya se va a realizar el pago y llevan a cabo "un ataque homógrafo, en el que cambian una letra del dominio". De esta manera, cambiando, por ejemplo, una ele por una i mayúscula, hacen pasar el correo electrónico falso por el original.

"Técnicamente, las empresas están muy bien protegidas pero el factor humano al final es el que falla", revela Gómez. El error habrá consistido, en muchas ocasiones, en haber pinchado ese enlace que te había llegado desde una dirección falsa. En algunas ocasiones, sí está "mal bastionado el servidor de correo" y los cibercriminales lo vulneran sin que exista ese error humano, pero es menos frecuente.

Cuando una empresa es víctima de este tipo de estafa, es fundamental que denuncie cuanto antes. "En cuanto se está produciendo la denuncia, nos avisan y nosotros llamamos a los bancos para que se produzca un bloqueo del capital", explica el agente. Si no hay denuncia o se hace al cabo de un tiempo, "no podemos hacer nada" y es prácticamente imposible recuperar el dinero.

En el caso de la estafa a la empresa de Mahón, sí lograron recuperar el dinero, pero no es fácil hacerlo. El dinero estafado, en ocasiones a varias personas o empresas, se acumula en una cuenta corriente. Desde esta, se distribuye a las cuentas de las llamadas 'mulas', como los cinco detenidos en la operación de la Policía Nacional en Roquetas de Mar. Y desde allí, el dinero viaja a otra cuenta, la del cabecilla, muchas veces en países del este de Europa, donde acaba en monederos de criptomonedas.

VOCES CLONADAS CON IA

Otro tipo de estafa es la del CEO. "El jefe de la empresa te llama y te dice que tienes que ingresarle 3.000 euros para que le den la licencia de Sanidad, por ejemplo", explica Gómez. "Tú no verificas que la llamada es de tu jefe real y haces el ingreso". Pero ni te ha llamado el jefe ni la cuenta es la de la empresa. El engaño lo consiguen porque clonan la voz del jefe mediante inteligencia artificial. "Parece muy ilógico que pase, pero pasa más de lo que creemos", asegura el agente.

"La IA se está utilizando cada vez más", asegura, y no solo para clonar la voz del jefe. Así, los casos de 'phishing' "cada día son más sofisticados por la utilización de IA". En la fase previa al ataque, "el escaneo de redes sociales para saber qué perfil de empresa es, lo hacen con IA, porque es muy rápida, muy concreta y muy limpia y eso garantiza que el ataque sea bueno". También se usa para clonar páginas web y para perfeccionar el lenguaje usado para comunicarse con la víctima.

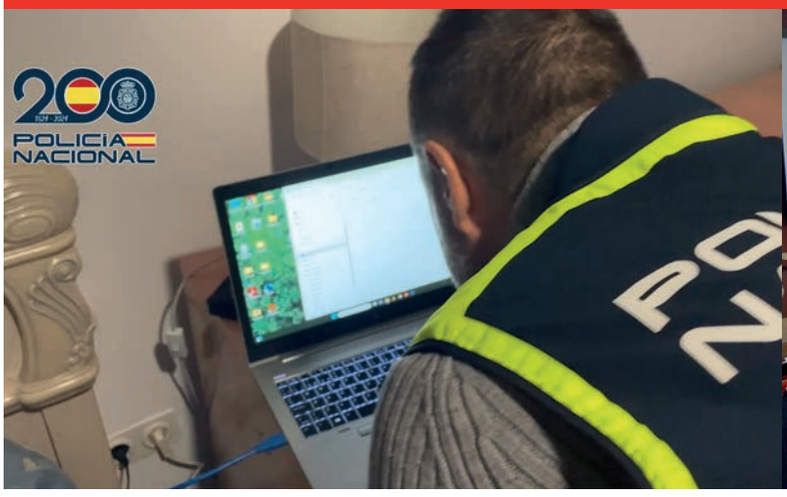
Otro tipo de delitos contra empresas son los 'ransomware'. Aquí, los ciberdelincuentes bloquean el acceso a los sistemas informáticos de la empresa, encriptando la información; los 'secuestran' a cambio de un rescate. En estos casos, "siempre aconsejamos no pagar el rescate, porque ha habido veces en los que sí se ha hecho y no se ha recuperado la información o solo en parte", porque ni los criminales logran desencriptar los discos duros. "En determinados países, además, pagar el rescate se considera financiación de grupo criminal e incluso terrorista", señala el agente.

Hay que tener en cuenta que, por lo general, cuando se comete un ciberdelito, el criminal y la víctima no están en la misma provincia y, muy a menudo, ni siquiera en el mismo país. La coordinación entre las fuerzas de seguridad a nivel nacional, europeo e internacional es clave para resolver los casos. Asimismo, se aplican legislaciones diferentes, dependiendo de dónde se esté centralizando la investigación judicial del crimen.

LA ESTAFA DE LAS CRIPTOMONEDAS

Es el caso de las estafas de inversión en criptomonedas, otro ciberdelito en auge en los últimos tiempos, que afecta a particulares. La víctima había visto en una red social a un famoso anunciando inversión en criptomonedas. Le llama la atención, pincha en el enlace y le contacta un 'broker' que le recomienda invertir, por ejemplo, 250 euros. "En un primer momento devuelve 300 y, poco a poco, le va embaucando y acaba ingresando 90.000 euros", cuenta el agente. Y el 'broker' desaparece del mapa.

A la hora de combatir estos delitos, las fuerzas de seguridad tienen que luchar, además, contra lo que llaman 'pitufeo'; en lugar de una estafa grande, realizan muchas estafas pequeñas, de mil euros o menos por persona. Solo al lograr identificar a un mismo autor o autores detrás de varias de ellas se consigue que el caso tenga entidad suficiente como para que prospere en los juzgados. Para ello, se valen de herramientas como el big data, con las que encuentran que "con estas características, este número de teléfono y esta dirección donde han ido a parar las criptomonedas tenemos tantas denuncias en toda España", cuenta Gómez. Gracias a esto, añade,



Agente del Grupo VI de la Policía Nacional de Almería, durante el operativo para detener a uno de los usuarios de una plataforma online de pornografía infantil. Jornadas de Ciberdefensa en la Universidad de Almería, celebradas a principios de año.

pueden conseguir una orden para investigar a nivel europeo, lo que sería imposible para cada caso por separado.

Otro tipo de estafa a particulares es la del amor, en la que la víctima cae en la red tejida por un famoso o un militar americano que se ha fijado en ella, pero que en realidad es, en la mayoría de ocasiones, un joven de algún país africano. En estos casos, logran estafar grandes cantidades, sumando pequeñas aportaciones a lo largo de bastante tiempo.

Una estafa también habitual es la del falso hijo en apuros, en la que alguien recibe un 'whatsapp' de un número que no tiene en la agenda de contactos diciendo que es su hijo, que ha perdido el móvil y la cartera y necesita que le envíe por Bizum cierta cantidad de dinero a ese número. Evidentemente, no es el hijo pero la urgencia muchas veces no deja reaccionar con lógica y la víctima acaba cayendo en la trampa.

El agente recuerda que incluso han tenido un caso de una falsa oferta de empleo para un conocido hotel de Almería. Pedían la vida laboral, una fotocopia del DNI, tres nóminas y la renta. "Tuvimos por lo menos cien denuncias", cuenta. Con esa información, "se iban al banco y abrían una cuenta corriente, que utilizaban luego para pivotar el dinero de estafas". Cuando se inicia una investigación, "lo primero que hace es identificar al titular de la cuenta, pero este no tiene ni idea de que se ha abierto esa cuenta a su nombre", explica el agente. Hasta que se aclara la situación, "les pueden llamar como investigados".

GOLPE A LA PORNOGRAFÍA INFANTIL

Uno de los últimos casos resueltos con éxito por el Grupo VI muestra la importancia de la comunicación que se lleva a cabo entre las policías de distintos países. Ha sido un caso de pornografía infantil investigado a nivel europeo, que se puso en marcha en Alemania y se ha desarrollado en 38 países, entre ellos España, donde hay 16 detenidos, uno de ellos en Almería. En la operación se ha conseguido desarticular una de las mayores plataformas mundiales de distribución de material pedófilo. En total, hay 79 detenidos y 1.393 identificados.

Los clientes pagaban con criptomonedas y accedían a la plataforma, donde veían el contenido en 'streaming', sin tenerlo que descargar. Rastrear la pista de los responsables de la red y de los consumidores hasta identificarlos implicaba un alto conocimiento técnico de diversas tecnologías.

Los agentes alemanes "accedieron al servidor donde se estaban volcando los vídeos", relata Gómez, que ha participado en la investigación. "A través de ese servidor, se ve que hay gente que accede al material pagando en criptomonedas, que es otro delito de financiación", continúa. La policía alemana contactó con la española para ayudarles a identificar, "a través de las direcciones de bitcoins", a los clientes. "Esta investigación incluye muchos tipos de delitos, pornografía infantil, producción, distribución, financiación, y se hace con medios técnicos muy buenos, con el volcado de un servidor donde está el contenido y la investigación de los blockchains", relata. Y añade que esto "requiere muchos conocimientos técnicos, pero el grupo de Almería es de los más potentes que hay".

Otros casos habituales de delitos contra las personas son los de revelación de secretos, la difusión de contenido sexual explícito grabado por una pareja. Cuando se termina la relación, a modo de venganza, el hombre lo distribuye y, en ocasiones, lo publica online, a veces incluso proporcionando datos de la chica, como su número de teléfono.

Asimismo, se dan casos de 'child grooming', adultos que, haciéndose pasar por menores, contactan con otros niños o niñas con el objetivo de acabar teniendo relaciones sexuales con ellos. En este sentido, el agente recomienda "tener cuidado con los chats de los videojuegos de los niños, porque los agresores los utilizan mucho para contactar con los niños"; primero para ofrecerles puntos o monedas del juego a cambio de fotos explícitas, que sería un delito de corrupción de menores, y después para quedar con ellos, que ya sería el 'child grooming'.

FORMACIÓN Y PREVENCIÓN

El trabajo policial resuelve buena parte de estos casos, pero muchos se podrían haber evitado. Por ello, el agente insiste en la necesidad de fomentar la formación a todos los niveles, desde los trabajadores de empresas a los particulares, incluso desde pequeños. En este sentido, desde hace años, Policía Nacional y Guardia Civil participan en el programa 'Ciberexpertos' del Plan Director para la Seguridad en los Centros Educativos.

Para minimizar las posibilidades de que una empresa sea víctima de una estafa online, recomienda medidas como "introducir un doble factor de identificación". Así, "en cuanto te emito un correo en el que te pongo el número de cuenta, tú me llamas y, a través de una contraseña, establecemos que ese correo es veraz y que te voy a pagar de forma inmediata", explica. Otra recomendación es "no dar privilegios a quien no los necesite en la red corporativa".

Desconfiar de los mensajes de un familiar desde un número distinto al suyo es otra práctica de prevención recomendada, así como llamarle para comprobar si ha perdido el móvil. "También hay que tener mucho cuidado con las aplicaciones que permiten el acceso remoto a tu ordenador, como Anydesk, que las utilizan mucho los estafadores de criptomonedas", para 'ayudarte' con las operaciones, ya que la víctima no tiene los conocimientos técnicos para llevarlas a cabo, "y lo aprovechan para robarte toda la información del ordenador".

Así, la formación y la prevención son claves para estar seguros en unos entornos digitales en los que cada vez es más sencillo que alguien intente estafarnos o utilizar nuestros datos para cometer otros delitos. Y cuando fallen, las fuerzas de seguridad han demostrado que, con tiempo y medios, acaban localizando y deteniendo a los ciberdelincuentes. ■

Colaboración institucional, clave para prevenir la ciberdelincuencia

A la hora de luchar contra la ciberdelincuencia, Juanfran Gómez destaca la necesidad de impulsar la colaboración entre las fuerzas de seguridad, las empresas, los ciudadanos y la universidad para aumentar la formación que se recibe en la materia y estar más seguros en nuestros entornos digitales. En este sentido, el pasado enero se celebraban en la Universidad de Almería las I Jornadas en Ciberdefensa y Seguridad Nacional, que contaron con la participación de expertos en la materia de empresas tecnológicas, Fiscalía y las Fuerzas y Cuerpos de Seguridad del Estado, entre estos el propio agente del Grupo VI de Almería.

El consejero de Universidad, Investigación e Innovación, José Carlos Gómez Villamandos, señalaba en la inauguración que en el último año, "ha habido un incremento de más de un 40% en ciberataques en Andalucía, más de 80.000 delitos financieros a través de este tipo de herramientas", lo que muestra la necesidad de invertir en formación.

El organizador de las Jornadas, el profesor José Antonio Álvarez Bermejo, explicaba que "muchas empresas, por no poner en compromiso su imagen institucional, no denuncian estos delitos y no contamos con un número real de los ataques, pero sí sabemos que crecen exponencialmente". Y añadía que "hoy en día, con un ordenador y un teclado se puede atacar a un Estado, bloquear un hospital o intervenir las comunicaciones en un aeropuerto".

José J. Céspedes, rector de la UAL, aseguró que "compartir conocimiento y divulgarlo permitirá identificar riesgos cibernéticos, plantear estrategias para atajarlos y diseñar herramientas que permitan a empresas, personas e instituciones prevenir, en la mayor medida posible, ser víctimas de ciberdelitos".

En marzo, Asempal, confederación empresarial de la provincia de Almería, acogía la jornada +Ciberseguridad, que contó con la presencia de la exministra Fátima Báñez, presidenta de la Fundación CEOE, que organizaba junto al Instituto Nacional de Ciberseguridad (Incibe) la jornada, y Antonio Hernando, secretario de Estado de Telecomunicaciones e Infraestructuras Digitales.

Cecilio Peregrín, presidente de Asempal, aseguró que "las empresas deben ser proactivas en su protección digital porque un ciberataque no solo genera pérdidas económicas, sino que también daña la confianza y la reputación de las empresas".

Báñez apuntó que "la barrera más importante contra un ciberataque es la formación de los trabajadores", para lo que destacó la colaboración entre administraciones, fuerzas de seguridad y empresas.

Hernando recalcó la importancia de dotar a las empresas, sobre todo a las pymes, de conocimientos y estrategias en ciberseguridad para garantizar su competitividad.

Jornada +Ciberseguridad, organizada por la Fundación CEOE y el Incibe en la sede de Asempal.