



DIGITAL

Los ciberdelitos se disparan en España

En 2019, la actividad criminal en el entorno virtual se incrementó en un 45% respecto al año anterior. Así lo recoge la Memoria Anual de la Fiscalía, que advierte del riesgo que los 'hackers' suponen en el contexto de la banca online.

Alejandro Galisteo, Madrid
Este lunes, Dolores Delgado, fiscal general del Estado, entregó la Memoria de la Fiscalía correspondiente al ejercicio 2019 a Juan Carlos Campo, ministro de Justicia. El acto llega una semana después de la presentación del informe. Y entre las más de 1.500 páginas que forman el documento destaca el incremento de la actividad cibercriminal. La Memoria destaca que en el último año se produjo una subida del 44,92% de las diligencias incoadas por delitos informáticos: "Los indicadores revelan el imparable crecimiento de la actividad delictiva en el ciberespacio", explica-

ba Delgado sobre un tipo de actividad criminal que el pasado año ocupó casi el 10% del trabajo de los fiscales y provocó que las investigaciones policiales para combatirla aumentaran en un 35,8%.
Aun así, el informe reconoce que son muchos los delitos de este tipo que no se denuncian o que no llegan a investigarse judicialmente, por haber sido imposible dar con los autores. Además, advierte del riesgo que supone el contexto creado por la pandemia, con un incremento de la actividad virtual de la población, el caldo de cultivo perfecto para la actuación de los hackers.
Entre los tipos de ciberdeli-

EL CRIMEN INFORMÁTICO EN CIFRAS

Tipo de delito	Número de procedimientos	Respecto al total (%)
Contra la libertad	1.381	10,51
Contra la integridad moral	87	0,66
Contra la libertad sexual	1.214	9,23
Contra la intimidad	677	2,89
Contra el honor	110	0,84
Contra el patrimonio y el orden socioeconómico	9.482	72,15
De falsedad	106	0,81
Contra la Constitución	83	0,63
Total	13.143	100

Fuente: Memoria Anual Fiscalía 2019

tos más habituales, la Memoria de la Fiscalía apunta a los que afectan al mundo de los negocios y las transacciones económicas. Así, en 2019, la actividad informática que dio lugar a un número más elevado de investigaciones judiciales fueron las estafas y fraudes, que sumaron 8.611 procedimientos judiciales, lo que supone un porcentaje del 65,51% del total del crimen online.
En el texto, los fiscales advierten tanto del imparable aumento de bandas criminales dedicadas a la estafa tradicional a través de webs y foros como de delitos económicos con un alto grado de sofisticación,

como los que duplican las tarjetas de crédito o los que son capaces de interceptar el código SMS de los usuarios como medida de seguridad en cualquier transacción.
La Fiscalía también señala el alto número de procedimientos incoados que atentan contra la libertad sexual, con un aumento del 12% de las agresiones de este tipo contra menores. En este sentido, la Memoria propone una reforma para la tipificación como delito de la suplantación de identidad en la red y medios más eficaces para el control de los sistemas de mensajería instantánea.

LAS CIBERESTAFAS MÁS HABITUALES



Inversión en criptomonedas

Estafas de inversiones en criptomonedas de alta rentabilidad con las que se logra captar la atención de los usuarios que transfieren importantes cantidades de dinero que posteriormente no pueden ser recuperadas.



Falsificación de webs institucionales

Los ciberdelincuentes pueden instalar un software en los dispositivos de los usuarios que falsifica webs de instituciones oficiales y de entidades bancarias con el objetivo de conseguir los datos de los estafados.



Estafa de soporte técnico

El atacante provoca que en el dispositivo de la víctima aparezca una advertencia de mal funcionamiento junto a un enlace de contacto con el equipo técnico que en realidad es un virus informático.



Fraude del CEO

Se trata de un delito dirigido contra trabajadores de cualquier empresa por la que los 'hackers' suplantán la identidad de algún directivo de la compañía, consiguiendo información privilegiada de la misma.



Duplicar tarjetas

Los ciberdelincuentes son capaces de duplicar y clonar las tarjetas bancarias de los usuarios utilizando un decodificador invisible en los cajeros automáticos para después usarlas sin que el propietario dé su permiso.



Captura de códigos SMS

Como medida de seguridad, los bancos envían un código SMS a los usuarios en cualquier operación. Ahora, los 'hackers' son capaces de interceptar esos códigos para introducirse y controlar el móvil de la víctima.