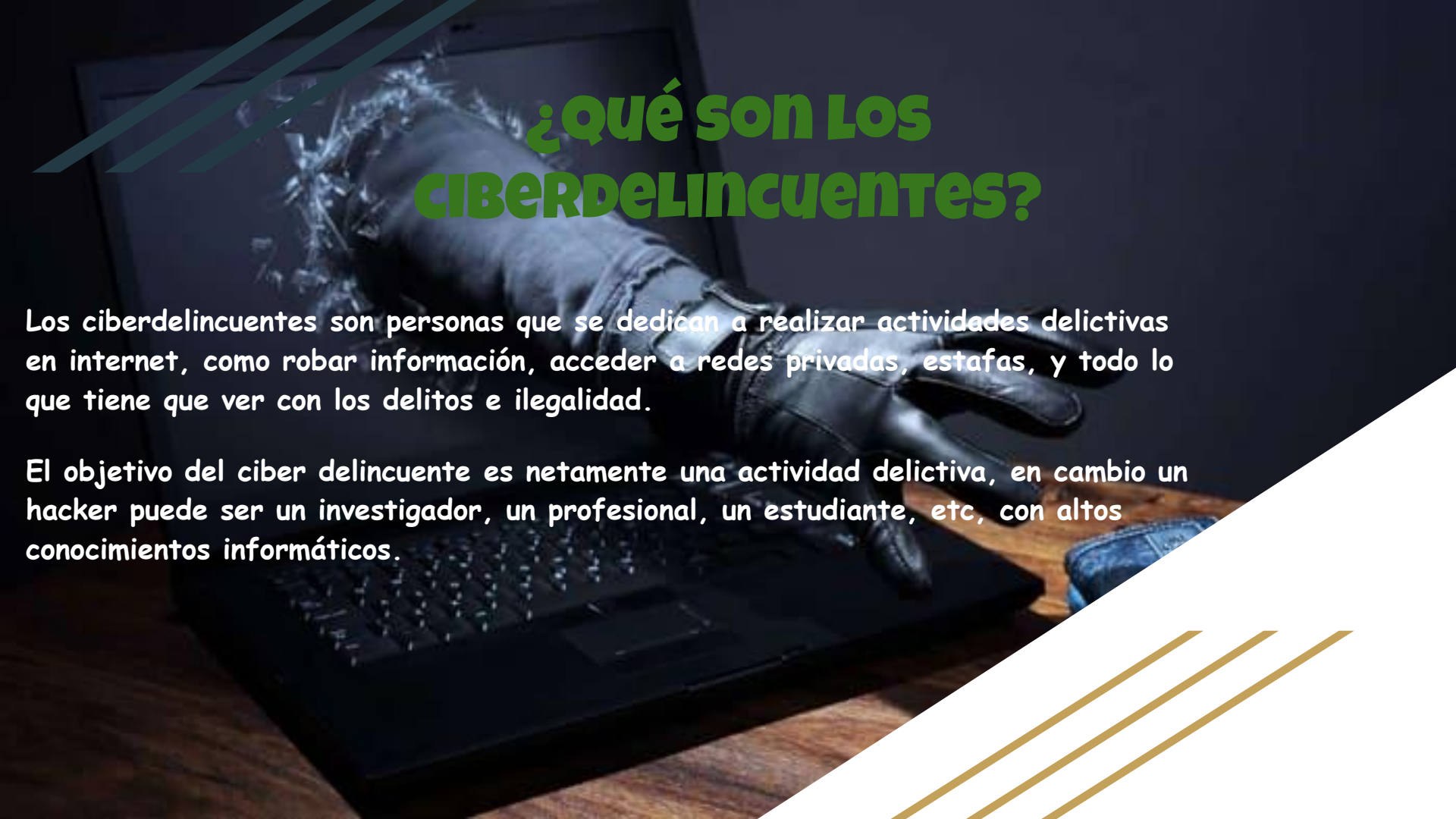
CIBERDELINCUENTES



¿Qué son los ciberdelincuentes?

Los ciberdelincuentes son personas que se dedican a realizar actividades delictivas en internet, como robar información, acceder a redes privadas, estafas, y todo lo que tiene que ver con los delitos e ilegalidad.

El objetivo del ciber delincuente es netamente una actividad delictiva, en cambio un hacker puede ser un investigador, un profesional, un estudiante, etc, con altos conocimientos informáticos.

LA POLICÍA Y LOS CIBERDELINCUENTES:

Actualmente los Estados Unidos y los países de Europa están constantemente luchando contra los ciberdelincuentes, creando normas, investigando y capturandolos. En los últimos años muchos de estos han sido sentenciados, aunque algunas de las penas han sido menores, se está mandando un mensaje claro.

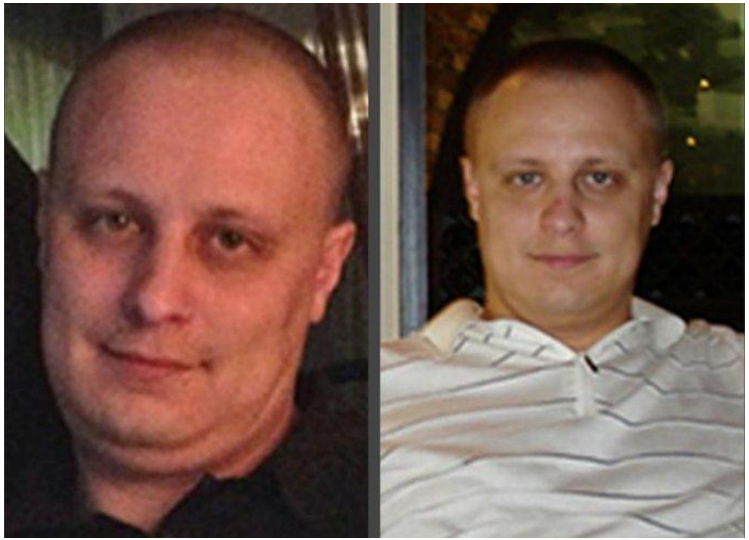
En otros países los vacíos legales y la falta de capacitación de la policía hacen que los ciberdelincuentes todavía tengan amplia ventaja y sigan haciendo de las suyas a plenitud.

Los ciberdelincuentes más buscados

Ciberdelincuentes más buscados por el FBI, están acusados de haber estado involucrados en robos de contraseñas, archivos clasificados, ataques masivos a servidores.

Evgeniy Mikhailovich Bogachev

También conocido como "lucky12345" y "slavik", es buscado por su supuesta participación en un mega engaño que implicó la instalación sin autorización de un software malicioso conocido como "Zeus" para robar números de cuentas bancarias y contraseñas.
En septiembre de 2011, el FBI comenzó a investigar una versión modificada del troyano Zeus, conocido como GameOver Zeus (GOZ) que fue utilizado para infectar a más de un millón de dispositivos, lo cual generó pérdidas por más de USD 100 millones.



GHOLAMREZA RAFATNEJAD

fundó Mabna, una compañía que está en la mira por haber accedido de manera ilegal a información clasificad de diferentes entidades. Más específicamente, Rafatnejad está acusado de haber participado en actividades delictivas, entre ellas el acceso no autorizado a computadoras para robar datos académicos y archivos protegidos en Estados Unidos y otros países para venderlos al gobierno iraní y universidades de ese país.

Shaileshkumar P. Jain y Bjorn Daniel Sundin

son buscados por su presunta participación en un cibercrimen internacional que hizo que usuarios de de 60 países compraran más de un millón de productos falsos de software, un engaño que derivó en pérdidas por USD 100 millones.

Se alega que desde diciembre de 2006 y hasta octubre de 2008, a través de anuncios falsos colocados en sitios web de compañías legítimas, Jain y sus cómplices engañaron a los usuarios para que creyeran que sus computadoras estaban infectadas con un malware para alentarlos a comprar software que supuestamente podía solucionar esos problemas. Pero en realidad no era así, era todo parte de un engaño.

Leyes de delitos informáticos en colombia

- ***Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.*** *El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*

- ***Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.*** *El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.*
- ***Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS.*** *El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.*
- ***Artículo 269D: DAÑO INFORMÁTICO.*** *El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
- ***Artículo 269E: USO DE SOFTWARE MALICIOSO.*** *El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
- ***Artículo 269F: VIOLACIÓN DE DATOS PERSONALES.*** *El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como "cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica". Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien "sustraiga" e "intercepte" dichos datos a pedir autorización al titular de los mismos.