Título Delitos Informáticos

Tipo de Producto Material Didáctico

Autores Galmarini, Luciano

Código del Proyecto y Título del Proyecto

A15S24 - Gestión de la ciberseguridad. Acceso no autorizado a sistemas informáticos

Responsable del Proyecto

Bertizzolo, Maria Eugenia Leila

Línea

Nuevas tecnologías y Derecho

Área Temática

Derecho

Fecha

2016

INSOD
Instituto de Ciencias Sociales y Disciplinas Proyectuales

UADE FUNDACIÓN UADE

Delitos Informáticos

Delito Informático

- Es aquel en el cual la comisión del delito (acción típica antijurídica y culpable) involucra a un sistema informático como medio (amenazas, instigación, incitación, apología) o como fin (hardware, software, información). (Téllez Valdes).
- Impensado para el legislador hasta no hace mucho tiempo.

Delito Informático

- **La situación antes de la Reforma al Código Penal**:
- Falta de compresión del fenómeno tecnológico por parte de los operadores del sistema (Jueces, auxiliares, abogados, Poder Ejecutivo, Congreso).
- Se carece de una cabal noción de los daños que se ocasionan por estos medios.

Derecho Penal

- El Derecho Penal es de « *última ratio* »
- Es una reacción del Estado frente a la vulneración de valores y bienes jurídicos fundamentales protegidos en la Constitución Nacional.
- No es una respuesta ante cualquier tipo de contingencias que se susciten en la vida en sociedad (lo cual hace al Derecho Civil).

Derecho Penal y Derecho Civil

- El Derecho Penal es « represivo » o « punitivo » ya que tiende a desalentar las conductas nocivas que estén tipificadas como delitos en una ley o Código, a través de una condena (reclusión, prisión, multa o inhabilitación).
- El Derecho Civil es resarcitorio y tiende a la reparación del daño de la víctima por parte del que cometió el ilícito a través de una indemnización.

Garantías Constitucionales

- **Principio de legalidad**: ningún habitante puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso (art. 18 CN).
- **Prohibición de la analogía**: si una conducta no se corresponde con el tipo, el Juez no puede aplicar lo previsto para una conducta similar. **Código Procesal Penal**: art. 2 “Las leyes penales no podrán aplicarse por analogía”.
- **Código Penal**: Es un catálogo cerrado de normas. (Numerus clausus).

Características de los Delitos Informáticos

- 1- Transnacionales
- 2- Mutables
- 3- White Collar Crime
- 4- Modernos
- 5- Cuantía

1) Transnacionalidad

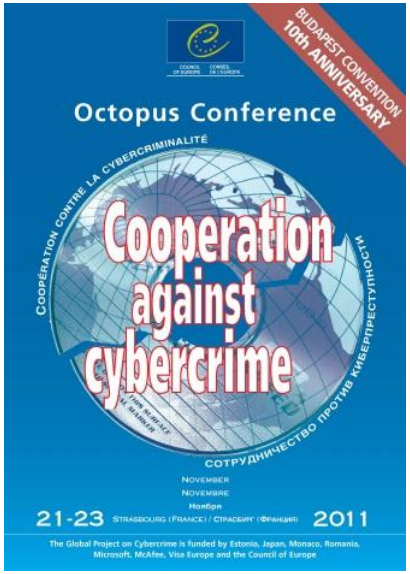
- Las maniobras delictivas no reconocen fronteras.
- Las conductas se realizan en un país y los resultados se producen en otro.
- Trascienden los límites de los países, que cuentan con sistemas jurídicos territoriales.

1) Transnacionalidad

- Conflictos:
- Ausencia de tipificación específica en la mayoría de las legislaciones.
- Falta de consenso internacional sobre el reproche de estas conductas.
- Dificultad en la persecución, detección de los delitos y localización de los autores.

1) Transnacionalidad

- A fin de que ningún ilícito quede impune, los Estados han recurrido a la cooperación internacional para prevenir y combatir este tipo de delitos.



Convenio de Budapest sobre Cibercriminalidad

- Firmado y celebrado por los Estados miembros del Consejo de Europa el 23/11/01. Está abierto a Estados no miembros mediante la Adhesión (Argentina adhirió).
- Objetivos: necesidad de llevar a cabo con prioridad una política penal común destinada a prevenir la criminalidad en el ciberespacio, mediante la adopción de una legislación apropiada (términos similares) y la mejora de la cooperación internacional.

Convenio de Budapest sobre Cibercriminalidad

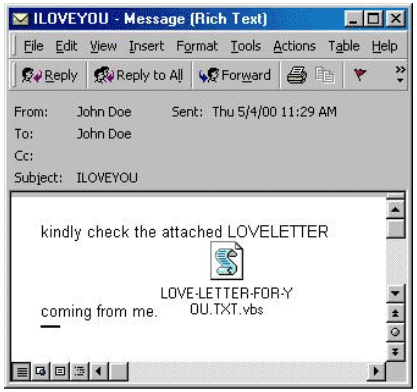
- Distingue cuatro grupos de delitos:
- Derechos de autor y afines
- Pornografía Infantil
- Confidencialidad, integridad y disponibilidad de los datos
- Crimen organizado: lavado de dinero, narcotráfico, terrorismo y trata de personas

1) Transnacionalidad

- Posturas: Competencia del país en el cual
- se encuentra el autor del delito (Love Bug). Caso de concurrencia de jurisdicciones: evita interpretar cual es la jurisdicción donde se produjo el mayor daño o seleccionar un pedido de extradición. Puede generar paraísos informáticos.
- se produjo el daño (Ivanov, Pasquantino). Requiere colaboración entre los Estados y un régimen de extradiciones.

1) Transnacionalidad

- **Love Bug**: virus que en el 2000 paralizó la actividad de varias compañías en todo el mundo, por el envío de millones de e-mails que hicieron colapsar los servidores. Como el envío se hizo desde Filipinas, el autor no fue condenado ya que dicha conducta no estaba configurada como delito.



Un e-mail con el virus ILOVEYOU en todo su esplendor.

1) Transnacionalidad

- USA v. Ivanov: Tribunal Federal de Connecticut.
- En 2000 Aleksey Ivanov hackeó el sistema de la Online Information Bureau y obtuvo las claves para controlar la red. Luego envió un email solicitando U$S 10.000 bajo amenaza de provocar la destrucción del sistema.
- Fue acusado por los delitos de conspiración, fraude informático, extorsión y posesión no autorizada de dispositivos de acceso (Hobbs Act).

1) Transnacionalidad

- Ivanov presentó excepción de incompetencia.
- Fallo: el tribunal norteamericano tiene competencia, a pesar de que Ivanov se encontraba en Rusia al momento de cometer los delitos, dado que había obtenido información en forma ilegal y había producido un daño de y en una computadora ubicada en Vernon, Estados Unidos.

1) Transnacionalidad

- Pasquantino, en 2004 la Corte Suprema de Estados Unidos sentó el principio del "*Wire Fraud*".
- Los tribunales norteamericanos tendrán competencia para juzgar cualquier delito de índole económica que utilice una comunicación por cable (teléfono, Internet, transferencias bancarias electrónicas, e-mail, WiFi) que atraviese los Estados Unidos.

2) Mutabilidad

- Adaptan sus acciones conforme a las circunstancias de modo, tiempo y lugar.
- Las permanentes innovaciones tecnológicas avanzan a paso más veloz que las soluciones legislativas.
- Desvío de dinero por medios virtuales, extorsión mediante encriptación de archivos, pharming, robo de identidad.

3) White Collar Crime

- Delitos de “cuello blanco” o “guante blanco”: aquellos cometidos por personas con cierta formación, instrucción y status socioeconómico.
- Grado de Sofistificación:
- “*Script kiddies*”: programas diseñados para atacar sistemas remotos de computadoras y redes.
- Agencias de inteligencia que se dedican al espionaje electrónico y ruptura de claves.

3) *White Collar Crime*

- Tiene acceso a la red y nociones de informática: *tablets*, *smartphones*, *laptops*, computadoras, dispositivos móviles, en su mayoría costosos.
- No siente remordimiento: por cuanto no hace un daño “visible” a personas. Cree que lo que hace no está mal, aún cuando sea ilegal.
- Síndrome del “Alpinista”: sensación de impunidad, particularmente por falta de legislación adecuada.

4) Moderno

- Los delitos informáticos provocan una **expansión** del Derecho Penal, que implica:
- a- delitos de tipo culposo: imprudentes (violación de elementos de prueba);
- b- delitos de peligro abstracto: no es necesario que se produzca un daño; alcanza con el acto preparatorio o tentativa (hacer circular un virus);

4) Moderno

- c- bien jurídico protegido pluriofensivo: una sola acción puede provocar múltiples daños en todo el planeta con solo atacar la red.
- d- delitos de « tipo abierto »: Son tipificados siguiendo el Principio de Neutralidad Tecnológica, evitando fijar una tecnología actual para que en el futuro se pueda aplicar el delito a la tecnología que la reemplace (el que acceda a una comunicación electrónica o de « *otra naturaleza* »).

5) Cuantía

- Estos delitos provocan un daño significativo.
- Afectan sistemas informáticos, dañando no solo el hardware y software, sino la información (datos) contenida en ellos, que es el principal valor económico de las empresas y uno de los bienes más valiosos y preciados de las personas.

Leyes de Delitos Informáticos

- Ley 24.766: de confidencialidad, introduce el delito de « *insider trading* ».
- Ley 26.388: de reforma al Código Penal en el 2008.
- Ley 26.904: introduce el delito de Grooming.
- Ley 25.036: modifica la Ley 11.723 (incluye al Software en los delitos del art. 72).
- Ley 25.891: de clonación de celulares.

Tipos Penales del Código Penal

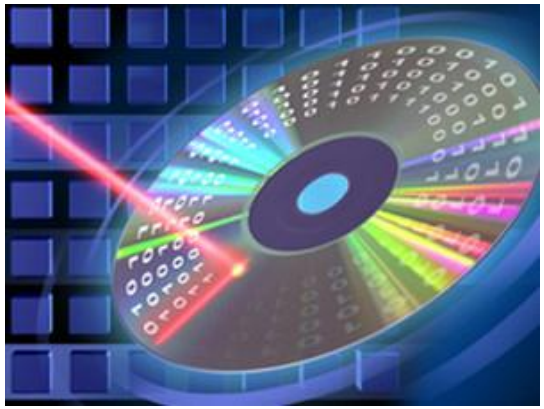
- **Antes de la reforma los jueces tenían que interpretar forzadamente los delitos incurriendo en "analogía".**
- **Hurto art. 162**: "será reprimido con prisión o reclusión de 1 mes a 2 años el que se apoderare ilegítimamente de una **cosa mueble**, total o parcialmente ajena. **¿Es la "información" una cosa?**
- **Estafa art. 172**: "será reprimido con prisión o reclusión de 1 mes a 6 años el que defraudare a **otro**...valiéndose de cualquier ardid o engaño". **¿Se puede inducir a error a una máquina?**
- **Daño, art. 183**: Será reprimido con prisión o reclusión de 15 días a 1 año el que destruyere, inutilizare, hiciere desaparecer, o de cualquier modo dañare una **cosa mueble**..." **¿Es el software una cosa?**

Ley 24.766: Insider Trading

- Toda persona que con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios,
- tenga acceso a una información sobre cuya confidencialidad se le haya prevenido,
- use y revele la misma sin causa justificada o sin consentimiento de la persona que guarda dicha información o de su usuario autorizado.

Ley 24.766: Insider Trading

- Comprende la información que conste en documentos, medios electrónicos y magnéticos, discos ópticos, microfilmes, películas u otros elementos similares.



Reforma del Código Penal

- La **Ley 26.388** termina con la incertidumbre:
- Suple lagunas legales.
- Hace frente a las amenazas del ciberespacio.
- Desalienta conductas nocivas.
- Penaliza las conductas disvaliosas que hasta 2008 no podían perseguirse debido a su atipicidad.

Reforma del Código Penal

- Subsana deficiencias normativas en forma armónica e integral, abarcando la casi totalidad de los ilícitos relacionados con las nuevas tecnologías, adaptándolos al medio informático, respetando los tipos penales tradicionales y la estructura del Código Penal.

Reforma del Código Penal

- La Ley 26.388 introduce solamente dos nuevos tipos penales
- Delito de "*Hacking*" (art. 153 bis)
- Delito de "*Virus Maker*" (art. 183, 2ª parte)
- La Ley 26.904 introduce el Delito de "*Grooming*".

Documento Electrónico

- **Artículo 1°.-** Incorpóranse como últimos párrafos del artículo 77 del Código Penal, los siguientes:
- "El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
- Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
- Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente."

- **Distribución y Tenencia con fines de distribución de Pornografía Infantil**
  - Art. 128 Código Penal

Bien Jurídico Protegido:
Integridad Sexual del Menor

Distribución de Pornografía Infantil

- **Art. 2°.-** Sustitúyese el artículo 128, por el siguiente:
- "Art. 128.- Será reprimido con prisión de 6 meses a 4 años el que **produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere**, **por cualquier medio**, toda **representación** de **un menor de 18 años** dedicado a **actividades sexuales explícitas** o toda **representación de sus partes genitales con fines predominantemente sexuales**, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores."

Distribución de Pornografía Infantil

- **Ampliación a toda la cadena**: a **produjere, publicare o distribuyere**, se agregan **financiare, ofreciere, comerciare, facilitare, divulgare**
- **Por cualquier medio**: comprende la red de Internet y todo dispositivo móvil o electrónico
- **Menor de 18 años**: problema de prueba (debió agregar "o que tengan apariencia física vinculada a esa edad")

“Representaciones”

- Se **cambia** “**imágenes**” por “**representación**”: lo que abarca Visuales, Auditivos y Escritos
- Cumple compromisos internacionales como el Protocolo de Venta de niños, Prostitución infantil y Utilización de niños en la pornografía (Complementario de la Convención de los Derechos del Niño de Naciones Unidas -ONU-), aprobado por Ley 25.763.

“Representaciones”

- Visuales: fotos, imágenes, diapositivas, videos, caricaturas, animaciones; Auditivos: grabaciones de audio con voces simuladas o reales de menores de edad y conversaciones telefónicas; Escritos: todo tipo de textos, cuentos, cartas, que relaten las experiencias de la vida real del autor, describiendo escenas pornográficas con menores.
- *Lolikon*, subespecie *Hentai* del *Anime* (Astroboy, Sailor Moon, Kum Kum).

Tenencia de Pornografía Infantil con fines de distribución. Acceso.

- **Art. 128, 2º y 3º párr.** "Será reprimido con prisión de 4 meses a 2 años **el que tuviere en su poder representaciones** de las descriptas en el párrafo anterior con **fines inequívocos de distribución o comercialización**.
- Será reprimido con prisión de 1 mes a 3 años el que **facilitare el acceso** a espectáculos pornográficos o **suministrare** material pornográfico a menores de 14 años."

Tenencia con fines de Distribución

- La tenencia es delito cuando se tenga con fines inequívocos de comercialización o distribución.
- La representación debe ser de un menor de 18 años.

Pornografía Infantil

- Organizaciones criminales conectadas a través de redes internacionales, que emplean Internet como medio para intercambiar archivos con material pornográfico infantil.
- Se apoyan en una *parafilia*: a la vez que

  Satisfacen los desvíos sexuales de los usuarios de este tipo de material (pedófilos y pederastas),

  Producen un negocio altamente lucrativo: 1 millón de niños es fotografiado y filmado por año para satisfacer una demanda que genera entre U$S 2.000 / 3.000 millones al año (Informe UNICEF)

Ley 26.904: Delito de Grooming y Sexting

- **Art. 131**: "Será penado con prisión de 6 meses a 4 años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".

TRIBUNAL EN LO CRIMINAL Nº 1 de NECOCHEA

- Corrupción de menores - Grooming. Condena a un joven que mediante el engaño de utilizar la apariencia de una niña, contactó vía internet a una menor de ocho años de edad, a quien le envió mensajes de contenido sexual y lenguaje obsceno, con evidentes fines corruptivos a su cuenta de correo, al mismo tiempo que enviaba mails con cantidad de fotografías con contenido de menores de edad desnudos y manteniendo relaciones sexuales entre sí.

TRIBUNAL EN LO CRIMINAL Nº 1 de NECOCHEA

- El Tribunal entendió que el accionar doloso del imputado emerge de las circunstancias de organizar una identidad falsa simulando ser una niña, crear una cuenta de mail coincidente, tapar el lente de su cámara web para ocultar su verdadera fisonomía de hombre adulto, encriptar con claves el material pornográfico infantil y simultáneamente mantener una cuenta de mail y de red social con su verdadera identidad, correspondiente a un buen hombre, con vida familiar, afectiva y laboral acorde su edad y circunstancias.

Ciberpolicía

- Existencia de la Ciberpolicía (Alemania), y ONGs: Internet Watch Foundation de UK, Protegeles.com de España, y software como Cyber Nanny (USA) y NLIP (Holanda).
- Bloquean las direcciones IP de sitios de pornografía infantil.

Cambio de Título

- **Art. 3°.-** Sustitúyese el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente:
- 'Violación de Secretos *y* ***de la Privacidad****."*

Violación de correo electrónico

- **Art. 4.-** Sustitúyese el artículo 153 por el siguiente: "Art. 153.- Será reprimido con prisión de 15 días a 6 meses el que abriere o accediere **indebidamente** a una comunicación electrónica, (una carta, un pliego cerrado, un despacho telegráfico, telefónico) o de otra naturaleza, que no le esté dirigido; o se apoderare **indebidamente** de una comunicación electrónica, (una carta, un pliego, un despacho u otro papel privado aunque no esté cerrado); o **indebidamente** suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

Violación de correo electrónico

- "En la misma pena incurrirá el que **indebidamente** interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier **sistema** de **carácter privado** o de **acceso restringido**.
- La pena será de prisión de 1 mes a 1 año, **si el autor además** comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena."

Publicación indebida de correo electrónico

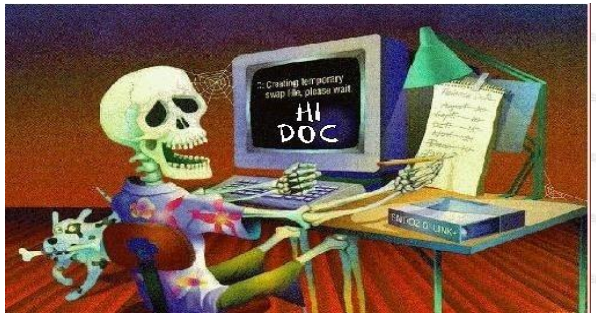
- **Art. 6°.-** Sustitúyese el artículo 155, por el siguiente:
- "Art. 155.- Será reprimido con multa de pesos UN MIL QUINIENTOS ($1.500) a PESOS CIEN MIL ($100.000), el que hallándose en posesión de una correspondencia, **una comunicación electrónica**, un pliego cerrado, **un despacho** telegráfico, telefónico o **de otra naturaleza**, no destinados a la publicidad, **los hiciere publicar indebidamente**, si el hecho causare o pudiere causar perjuicios a terceros.
- Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público."

Acceso ilegítimo a sistemas informáticos (Hackers)

- Los Hackers se dedican en forma incansable a encontrar algún fallo de sistema, que luego ellos mismos resuelven. **Objetivo**: alertan las vulnerabilidades en un software, sitio web, etc.

Acceso ilegítimo a sistemas informáticos (Hackers)

- **Art. 5°.-** Incorpórase como artículo 153 bis, el siguiente:
- "Art. 153 bis.- Será reprimido con prisión de 15 días a 6 meses, **si no resultare un delito más severamente penado**, el que **a sabiendas accediere por cualquier medio**, **sin la debida autorización o excediendo la que posea**, a un sistema o dato informático de acceso restringido.
- La pena será de 1 mes a 1 año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros."
- Es un delito residual.



Violación de Secretos: agravante al funcionario público

- **Art. 7°.-** Sustitúyese el artículo 157, por el siguiente:
- "Artículo 157.- Será reprimido con prisión de 1 mes a 2 años e inhabilitación especial de 1 a 4 años, el funcionario público que revelare hechos, actuaciones, ***documentos o datos***, que por ley deben ser secretos.″

Acceso ilegítimo a banco de datos personales

- **Art. 8°.-** Sustitúyese el artículo 157 bis, por el siguiente:
- "Artículo 157 Bis.- Será reprimido con la pena de prisión de 1 mes a 2 años el que:
- 1. A **sabiendas** e **ilegítimamente**, o **violando sistemas** de **confidencialidad** y **seguridad** de datos, **accediere**, de cualquier forma, a un **banco de datos personales**;
- 2. **Ilegítimamente proporcionare** o **revelare** a otro **información** registrada en un archivo o en un **banco de datos personales** cuyo **secreto** estuviere **obligado** a **preservar** por disposición de la ley.
- 3. **Ilegítimamente insertare** o **hiciere insertar** datos en un archivo de datos personales.
- Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años."

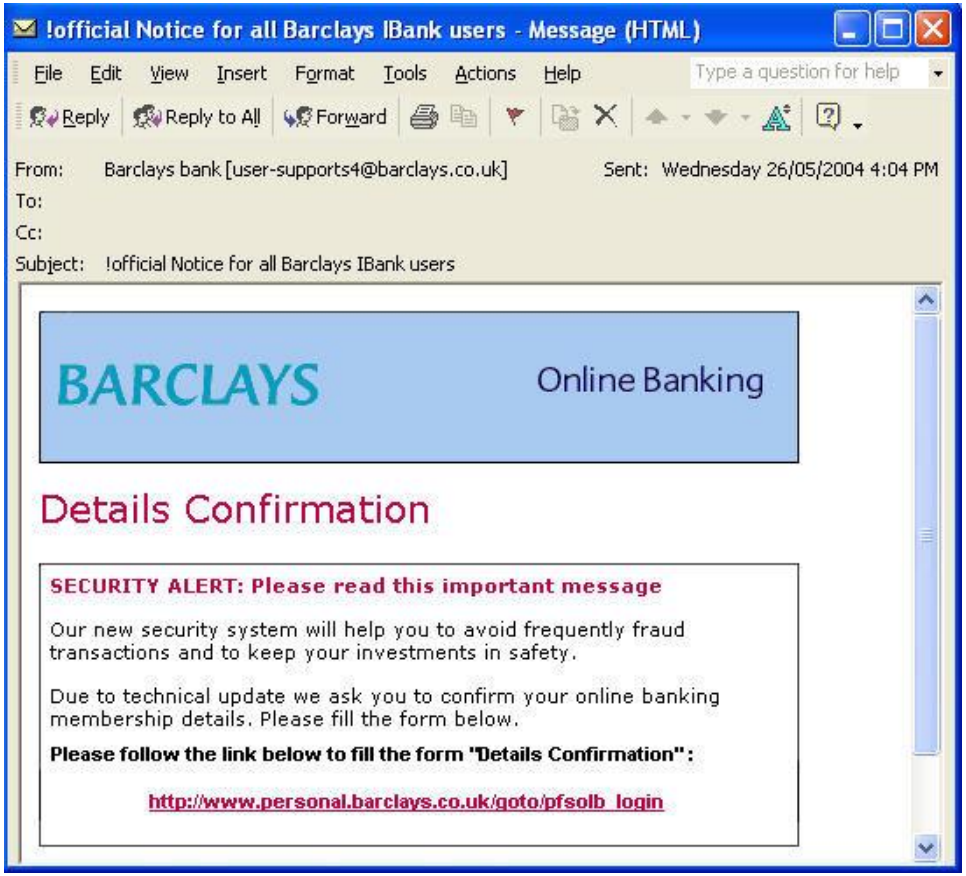
Defraudación

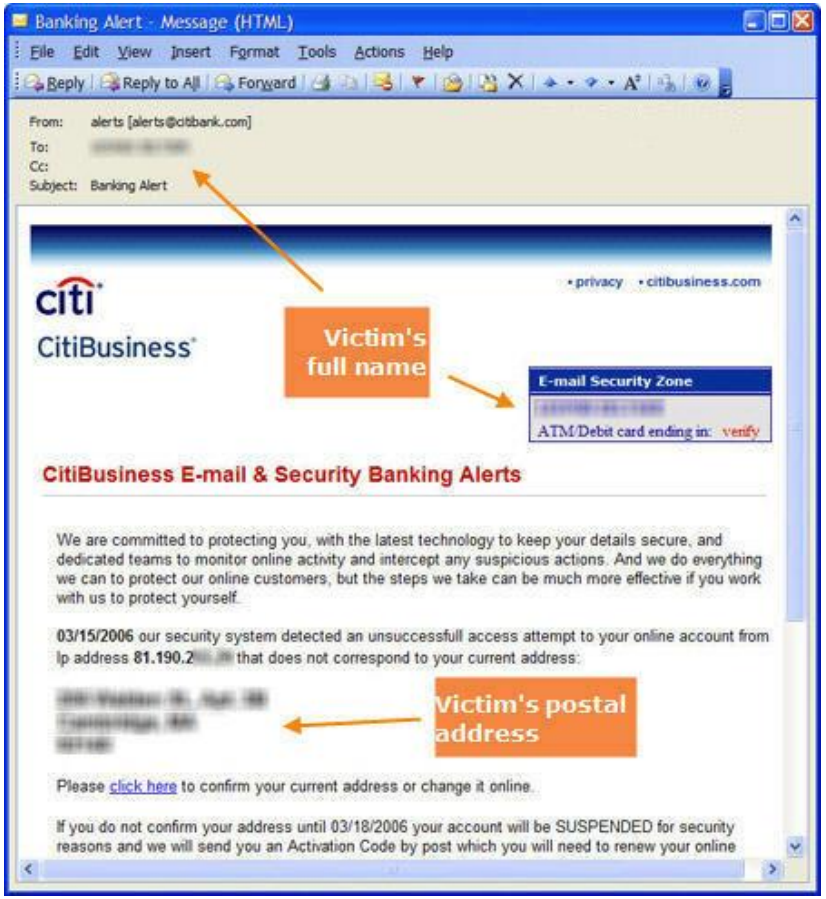
- **Art. 9°.-** Incorporase como inciso 16 del artículo 173, el siguiente: (1 mes a 6 años)
- "Inciso 16.- El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos."

Phishing

- **Engaño a una persona**: El caso mas común es el ***ph****ishing*. Neologismo que refiere a la acción de pescar donde "p" es *password* y "h" *hacker*.
- Llega un email con un link similar al de la entidad bancaria del usuario. Al hacer click sobre ese link se accede a una página web de un delincuente creyendo que es la de la entidad bancaria. Al ingresar los datos estos son captados por el delincuente. Y luego se produce el vaciamiento de la cuenta bancaria.
- Es necesario: un trabajo previo de inteligencia del delincuente; parasitar un hosting para albergar el sitio web falso; envío de spam.

Phishing: 1) Email con link





Phishing: 2) Sitio falso donde se comete el delito

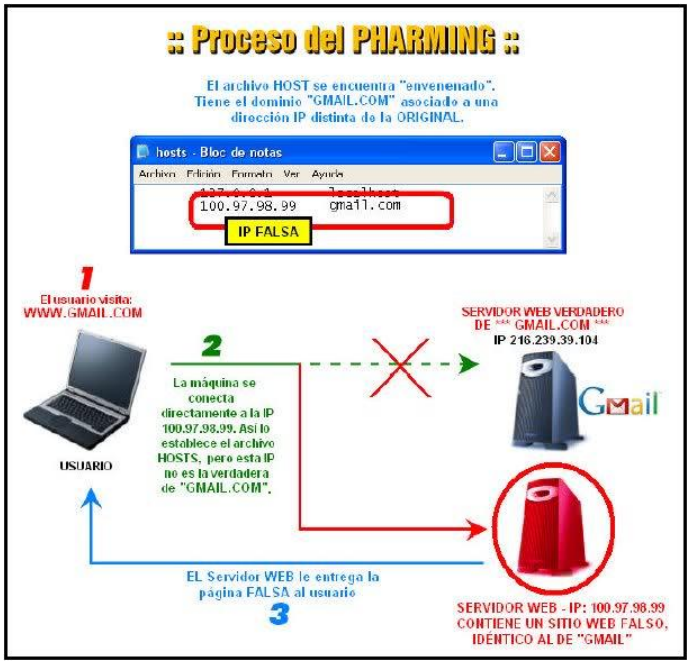
Pharming

- Manipulación informática: engaño a un sistema informático. El caso más típico es el *pharming*. Es una amenaza más sofisticada que el *phishing* y en este caso no hay engaño a una persona sino manipulación de un sistema informático: de las direcciones DNS que utiliza el usuario.
- Llega un email vacío y con solo abrirlo se instala en la computadora un programa que reescribe el archivo "hosts" (que todas las PCs tienen: una tabla con las direcciones IP de los sitios webs mas visitados por el usuario). Al reescribirse esas direcciones el usuario entrará a páginas webs falsas sin darse cuenta.

Pharming

- 1) Email vacío

- 2) Conexión a IP falsa



Keylogger

- Registrador de teclas: *key* (tecla) y *logger* (registrador)
- Es un software o dispositivo específico que registra los tipeos que se realizan en el teclado, para guardarlos en un archivo o memoria.
- Permite que otros usuarios tengan acceso a contraseñas, números de tarjetas de crédito, u otro tipo de información privada.

Skimming

- Consiste en sustraer información de las bandas magnéticas de las tarjetas de débito para luego extraer dinero de los cajeros automáticos.
- Combina un moderno dispositivo electrónico, con microcámaras de video o *keyloggers* colocados en cajeros automáticos.

Skimming

- Se instala un **falso lector** en la puerta de una sucursal, que **copia los datos** de la tarjeta, cada vez que alguien pasa la misma por la banda magnética.
- Asimismo se instala una microcámara camuflada cuyo lente apunta al teclado, para grabar el momento en que un cliente teclea su clave de seguridad.
- Luego se clona la tarjeta y se usan los datos para extraer dinero de los cajeros automáticos.

Cómo funciona el sistema

1 INSTALACIÓN FRAUDULENTA

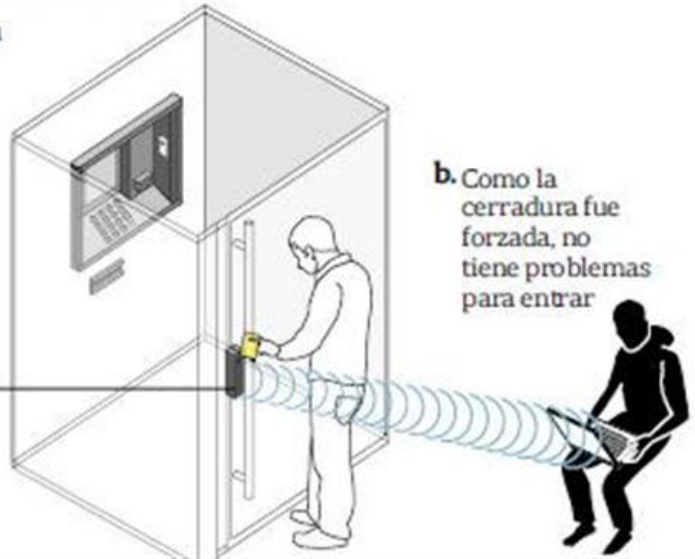
Los ladrones llegan al cajero y fuerzan la cerradura para que no sea necesaria la tarjeta para abrir

b. Colocación de una minicámara

a. Colocación de un lector de ingreso falso

2 INGRESO DEL CLIENTE

El usuario pasa su tarjeta por el lector falso de entrada del banco para ingresar.

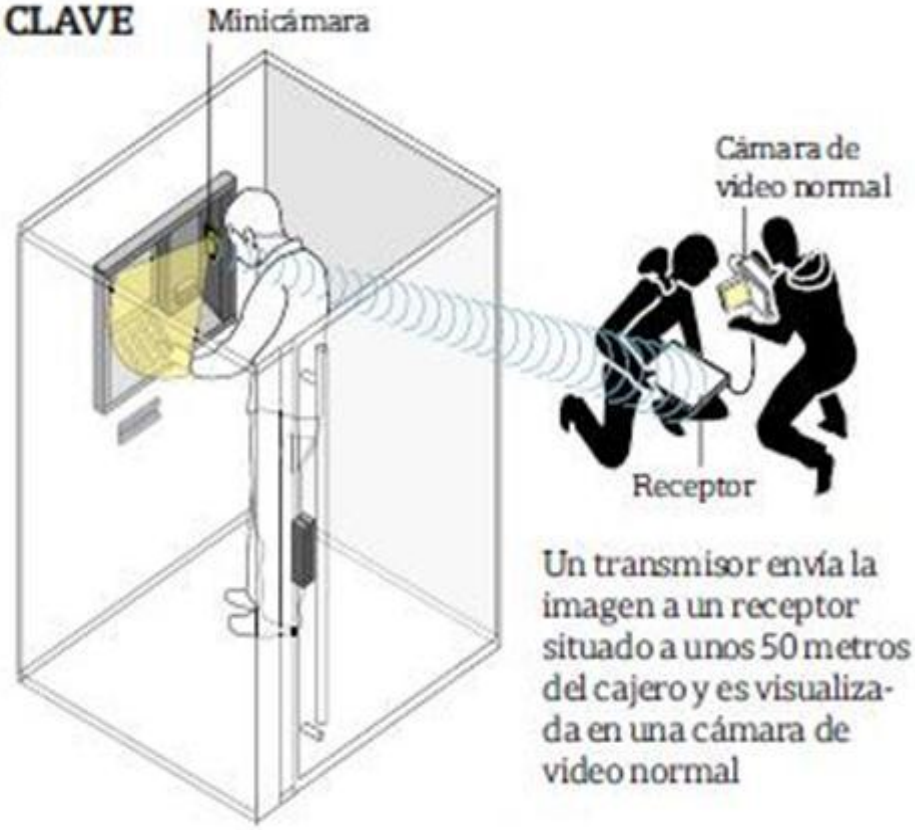


a. La banda magnética es copiada.

b. Como la cerradura fue forzada, no tiene problemas para entrar

3 COPIA DE LA CLAVE

El usuario coloca su clave para operar y es observado por la cámara colocada por los delincuentes.



Un transmisor envía la imagen a un receptor situado a unos 50 metros del cajero y es visualizada en una cámara de video normal

4 EL ROBO

Con la banda magnética y la clave de la tarjeta, los ladrones confeccionan una réplica del plástico y comienzan a saquear las cuentas del cliente.

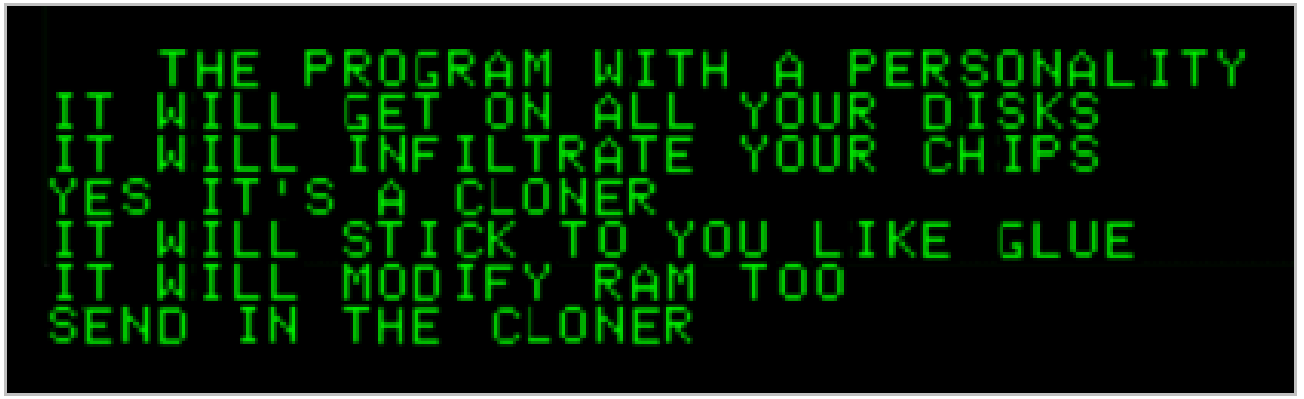
Fuente: Ministerio de Seguridad de la Nación / LA NACION

Daño informático y Distribución de virus

- **Art. 10.-** Incorpórase como segundo párrafo del artículo 183, el siguiente: (15 días a 1 año de prisión)
- "En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños."

Sabotaje Informático (Crackers)

- Los **Crackers** tienen grandes conocimientos de computación y su objetivo es bloquear sistemas de seguridad de los sitios web a los que acceden para causar daños.



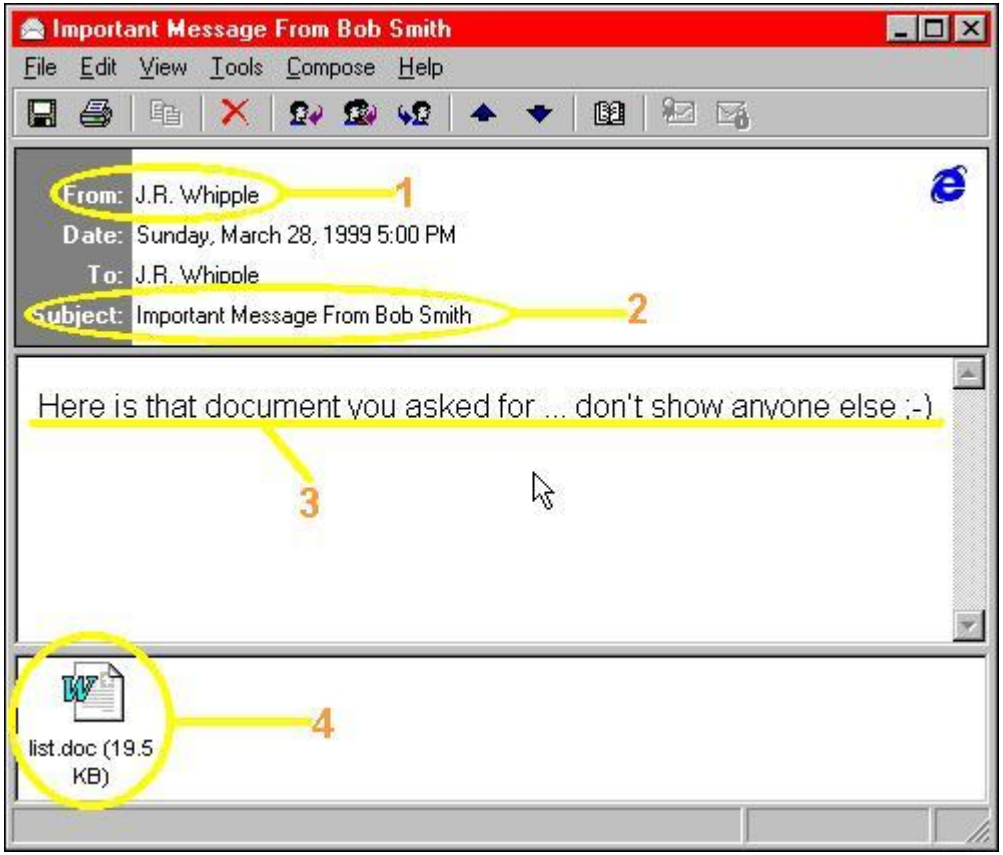
Sabotaje Informático

- La primer parte hace alusión al delito de daño informático mas conocido como sabotaje informático, y lo comete quien: altere, destruya o inutilice un dato, programa o sistema informático.
- Alterar: modificar un archivo de datos o programa sin destruirlo completamente.
- Destruir o Inutilizar: borrar
- definitivamente sin posibilidad
- de recuperación.

Virus Maker

- La segunda parte es el delito conocido como: “virus maker” y que pune la conducta de todo aquel que produce un virus y lo hace circular por cualquier forma (vende, distribuye o introduce).
- Es un delito de **peligro abstracto** ya que la persona comete el delito con solo hacer circular el virus aunque nunca se llegue a usar para el destino para el que fue creado.

Virus Melissa



Daño informático agravado

- **Art. 11.-** Sustitúyese el artículo 184, por el siguiente:
- "Artículo 184.- La pena será de 3 meses a 4 años de prisión, si mediare cualquiera de las circunstancias siguientes: (…)
- **5**. **Ejecutar el hecho en datos, documentos, programas o sistemas informáticos públicos;**
- **6. Ejecutar el hecho** en **sistemas informáticos destinados** a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u **otro servicio público**."

Interrupción de comunicaciones

- **Art. 12.-** Sustitúyese el artículo 197, por el siguiente:
- "Artículo 197.- Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica ***o de otra naturaleza*** o resistiere violentamente el restablecimiento de la comunicación interrumpida.”

Interrupción de comunicaciones

- El Juzgado Nacional en lo Criminal y Correccional Federal Nº 6 procesó a un ex empleado de Telefónica de Argentina, por el corte del servicio de telefonía celular de **Movistar** del 02/04/12 de abril, que provocó la interrupción del mismo en todo el país, entre las entre las 9 y 13 hs., impidiendo a los usuarios, abonados a dicha empresa, entablar cualquier tipo de comunicación telefónica.

Interrupción de comunicaciones

- Para llevar a cabo la maniobra, el imputado habría utilizado desde su domicilio, **dispositivos electrónicos**, como una antena “nanostation” que apuntaba hacia otra de iguales características ubicada en la localidad de Florencio Varela, a través de las cuales se logró el ingreso al Terminal Server de Movistar logrando la desconfiguración de los switches que provocaron la baja del servicio por el plazo mencionado.

Violación de elementos de prueba

- **Art. 13.-** Sustitúyese el artículo 255, por el siguiente:
- "Artículo 255.- Será reprimido con prisión de 1 mes a 4 años, el que sustrajere, alterare, ocultare, destruyere o inutilizare **en todo o en parte** objetos destinados a servir de prueba ante la autoridad competente, registros o documentos (**cualquiera fuera el soporte en el que estén contenidos, art. 77**) confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.
- Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de SETECIENTOS CINCUENTA PESOS a DOCE MIL QUINIENTOS PESOS."

Ley 25.891 Clonación de celulares

- La maniobra se centra en el uso de líneas de teléfonos móviles clonadas para traficar sobre ellas comunicaciones entrantes internacionales que ingresan vía Internet. Se realiza usando una computadora que cuenta con el hardware y software necesarios para captar comunicaciones de voz en formato digital (VoIP) y transformándolas (mediante un router) en discado y voz.
- Esta comunicación se deriva hacia una cantidad de teléfonos clonados que dependerá de la característica del hardware mencionada.

Delito de Clonación de celulares

- Ley 25.891: El que alterare, reemplazare, duplicare o de cualquier modo modificare un número de línea, de serie electrónico o mecánico de un equipo terminal o de un Módulo de Identificación Removible del usuario o la tecnología que en el futuro la reemplace, en equipos terminales provistos con este dispositivo, de modo que pueda ocasionar perjuicio al titular o usuario del terminal celular o a terceros.