Victimología – Delitos Informáticos

ÍNDICE:

El Delito informático

Elementos integrantes

- El delito es un acto humano, **es una acción (acción u omisión)**
- Dicho acto humano **ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido**.
- **Debe corresponder a un tipo legal** (figura de delito), definido por La Ley, ha de ser un acto típico.
- El acto **ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia)**, y una acción es imputable cuando puede ponerse a cargo de una determinada persona
- La ejecución u omisión del acto **debe estar sancionada por una pena**.

Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena.

Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por La Ley, que se realiza en o mediante el entorno informático y está sancionado con una pena.

En nuestro país, el delito informático está tipificado en la Ley 26.288, que agregó y modificó tipos del Código Penal, y algunos tipos particulares se encuentran en la ley 25.326 (Habeas Data), y 25.036 (Ley de Softtware).

▪ El delito informático como medio

- Violación de la intimidad:
  - Publicación en Internet de fotos o videos personales y/o íntimos
  - Violación del correo electrónico o cualquier comunicación electrónica (por ejemplo, SMS).

- Estafa:
  - Scamming
  - Phising

- Amenazas, Acoso:
  - Por mail, redes sociales, o SMS.

- Hurto
  - Robo de las cuentas bancarias a través del Home Banking.

- Pornografía infantil:
  - Distribución (o tenencia con fines inequívocos de distribución) de imágenes pornográficas de menores de la edad definida por el código penal (18 años en Argentina)

- Calumnias, Injurias, Abuso
  - Cyberbulling: Abusos de tipo verbal, mediante el uso de medios electrónicos. Son principalmente manifestaciones de odio, burlas, fotomontajes, acosos, que también pueden incluir amenazas; y apuntan a a estudiantes, adolescentes e incluso a niñas y niños, trayendo consigo destrucción moral, daños psicológicos y deserción escolar.
  - Grooming: Es el engaño por parte de un delincuente adulto, el cual simula a través de medios electrónicos ser un niño o niña con el ánimo de contactar a menores de edad y adolescentes con diversos fines, como la agresión o el abuso sexual; utilizando las redes sociales a partir de las cuales genera una amistad, hasta que logra generar la confianza en la víctima quien bajo la presión, el chantaje y la manipulación accede a las pretensiones o abusos del agresor.
  - Suplantación Personal: Consiste en la creación de perfiles falsos en las redes sociales y cuentas de correo, utilizando datos personales y fotos de las víctimas sin su consentimiento, con el fin de atentar contra la integridad moral, la intimidad, el buen nombre o el honor de las personas; pudiendo desembocar también en otros delitos como la injuria y la calumnia mediante imputaciones deshonrosas.

▪ El delito informático como objeto

El ataque puede producirse contra:

a. Hardware
b. Software
c. Información almacenada

- Hurto
  - Hacking (acceso no autorizado a un sistema o dato informático)
  - Cracking (violación de las medidas de seguridad informáticas)
  - Phreaking (botnets en Android, acceso no autorizado a través de Bluethoot)

- Daño
  - Destrucción de archivos o sistemas informáticos

- Fraude Informático
  - Cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos

- Violación de la intimidad
  - Intercepción, apoderamiento, o desvío indebido, y publicación de una comunicación electrónica (E-Mail, SMS, etc.). Ingreso no autorizado a una cuenta de Hotmail, Facebook, u otro servicio similar.

- Violación del Habeas Data (Ley 25.326). Modificaciones al Código Penal:
  – Art. 117 bis
    a) Insertar o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.
    b) Proporcionar a un tercero a sabiendas información falsa contenida en un archivo de datos personales.
  – Art. 157 bis
    a) A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, acceder, de cualquier forma, a un banco de datos personales;
    b) Revelar a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

- Usurpación
  - Ciberocupación

- Violación de los derechos de autor. Ley 25.036.
  Esta ley, a la que se ha dado en llamar "Ley del Software", vino a llenar un importante vacío legislativo de su época, al incluir a los programas de computación dentro de los derechos de autor.

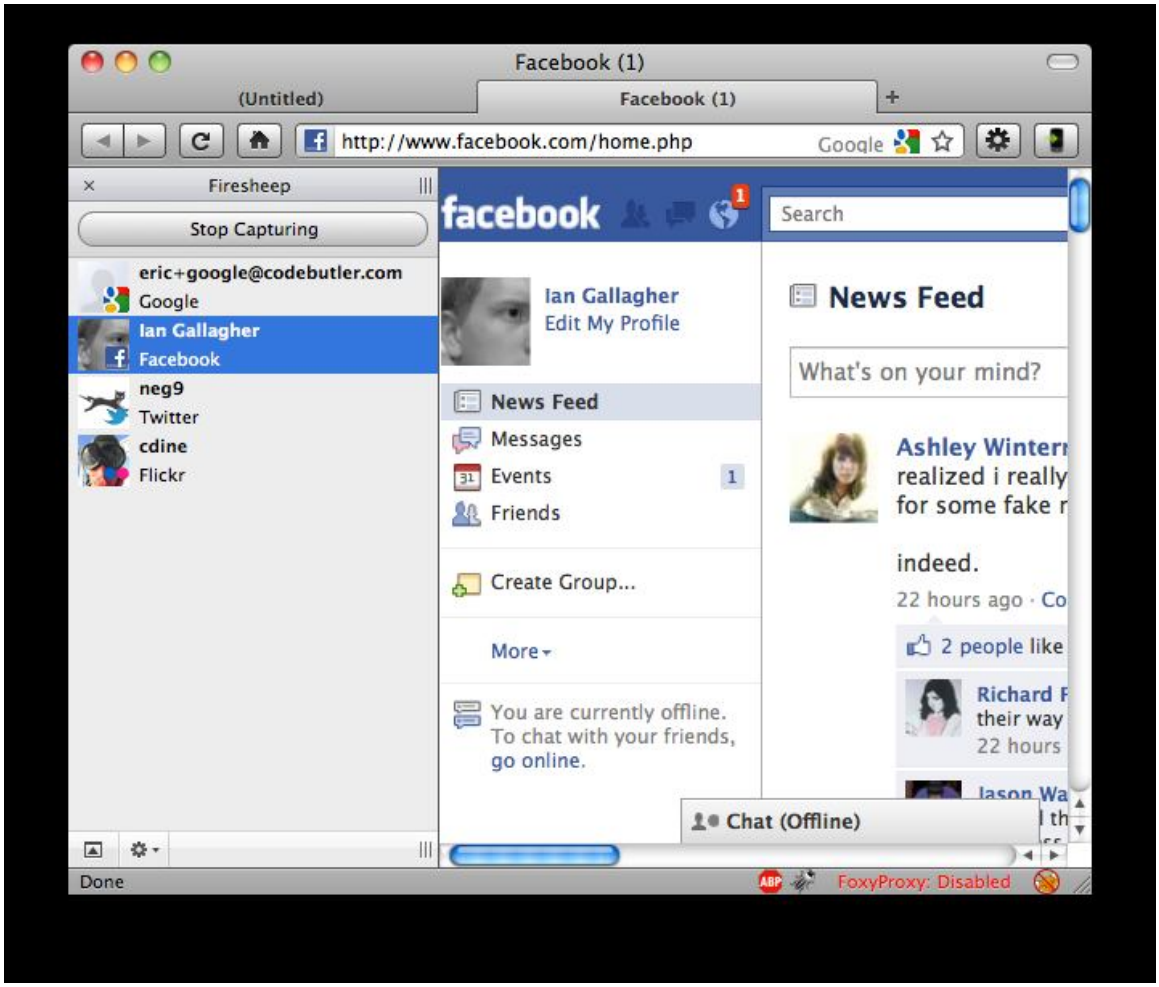
Según el art. 9º, se podrá producir una única copia de salvaguarda ("back up") de los ejemplares originales del software y añade que dicha copia debe estar debidamente identificada, con indicación del licenciado que la realizó y la fecha en que lo hizo.

¿Qué es lo que no sabemos acerca de la "realidad virtual" que llamamos Internet?

La respuesta es: infinidad de cosas. Internet constituye simplemente una red, pero una red muy grande. Para comprenderla cabalmente se deben tener conocimientos técnicos sobre infraestructura informática. A los efectos de estos apuntes, ejemplificaremos sólo algunos puntos que demuestren los peligros que en general el uso de Internet, sin conocimientos técnicos, podrían suscitarse:

Internet es una Red de Redes, es decir, no es más ni menos que una gran Red, de millones de computadoras. Cada computadora está conectada a una serie limitadas de computadoras, por lo cual la información que se transmite de una PC a otra en Internet suele atravesar en promedio 10 computadoras hasta llegar a destino. Esto implica que toda comunicación que enviemos o recibamos será susceptible de ser vista por otras personas; comenzando por los empleados de nuestros ISP (Proveedor de Acceso a Internet). Es por esto que deben encriptarse todas las comunicaciones de carácter sensibles (por ejemplo, las de Home Banking).

Los usuarios y claves de correos electrónicos (cuando se usan los clientes de correo, como el Outlook) son enviados sin encriptar, y cualquier persona que acceda a nuestro mismo router (por ejemplo, en un café con WiFi) podría interceptarla. También, compartiendo router, puede una persona "capturar" nuestra sesión de GMail, Twitter o Facebook, y hacer todas las acciones como si poseyera la clave. Podría también cambiar la clave, y la respuesta a la pregunta secreta, con el fin de pedir dinero por la restitución del uso de la cuenta.



Aquí un ejemplo de una extensión del navegador Firefox, que permite tomar sesiones de otros usuarios en la misma WiFi.

Una dirección de Internet (URL) está compuesta de varias partes. Lo que la mayoría de las personas no sabe es cuáles son las partes, qué significan, y fundamentalmente que una URL se debe leer de derecha a izquierda.
Así, muchas personas creerían que están ingresando a Facebook si en la barra de navegación de su explorador figura: www.facebook.com ó www.server1.facebook.com ó www.facebook.server1.com; cuando en realidad, sólo los 2 primeros casos refieren al sitio Facebook, mientras que el último no.
De ese modo, una persona puede –por ejemplo- ser víctima del siguiente engaño: recibir un correo electrónico que lo lleve al sitio www.facebook.server1.com donde verá la página de ingreso de Facebook, ingresará su usuario y clave y será redirigido al sitio real de Facebook, no sin antes haber almacenado su usuario y clave en el servidor del victimario.

Una URL se divide en: Protocolo, subdominio, dominio de segundo nivel y dominio de primer nivel.

Como ejemplo, en http://www.facebook.com, el protocolo es “http”, que significa “Hyper Text Transfer Protocol”, que es un modo de transferencia de información sin codificar por Internet. Si el protocolo es “https”, implica que la información está codificada, o enctriptada, y es muy común ver que ese protocolo es el que utilizan los sitios bancarios. Luego del protocolo, hay un separador “://”, y luego del separador, comienza la URL en sí.
Es importante tener en cuenta que la URL se lee de derecha a izquierda, es decir, comenzando por el final (para los lectores occidentales). El final de una URL es donde comienza la primer “/” (no tomamos en cuenta el separador “://”, pues, como dijimos, no forma parte de la URL en sí). Por ejemplo, si la URL es www.facebook.com/index.php?user=1874982 debemos descartar el “/index.php?user=1874982”. Si la URL fuera www.yahoo.com.ar/mail.aspx, entonces debemos descartar el “/mail.aspx”.

Definida la URL, pongamos atención en los ejemplos anteriores, en los que vimos como dominio de primer nivel tanto “.com”, como “.com.ar”. Sin entrar en detalle del por qué, diremos que el “.com” (o “.org”, o “.biz”, etc) son dominios de primer nivel administrados por entidades internacionales; mientras que el “.ar” (o “.br”, o “.it”), son dominios de primer nivel administrados por países. Los países por lo general distribuyen sus dominios subdividiéndolos con la misma estructura que los internacionales, y por eso tenemos “.com.ar” (es decir, el .ar subdividido en .com. Recuérdese que debe leerse de derecha a izquierda), “.org.ar”, etc.

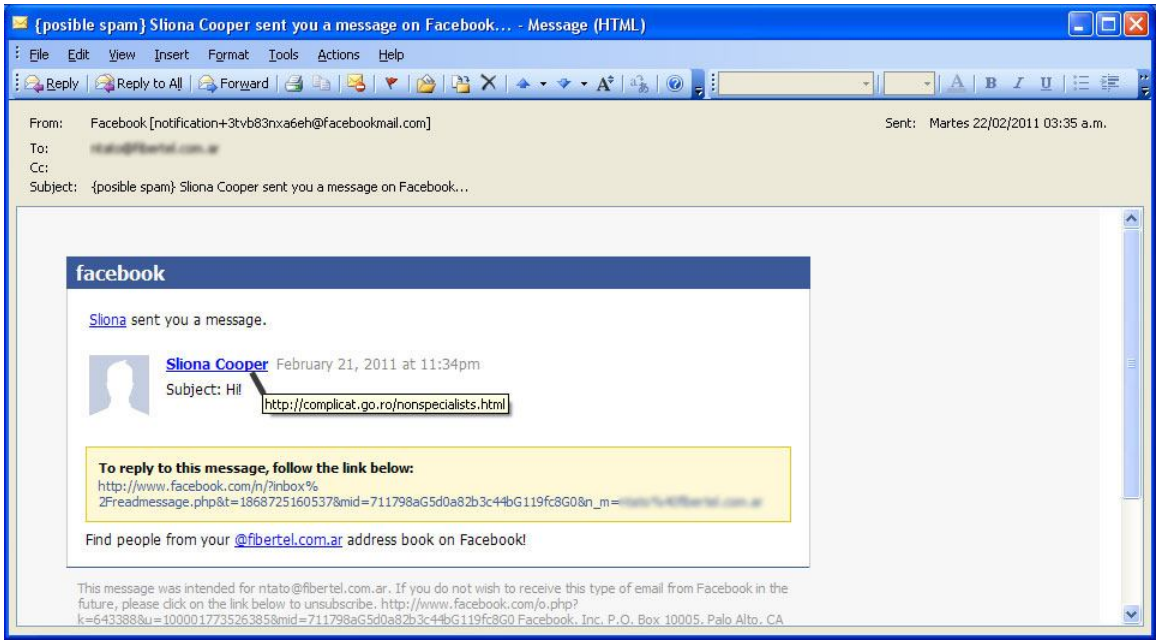
Se denomina a dominios de segundo nivel al nombre en sí. En los ejemplos, serían “facebook” y “yahoo”. Finalmente, lo que se encuentra a la izquierda del dominio de segundo nivel, es el subdominio (puede haber muchos) y no revisten mayor importancia a los efectos de estos apuntes. El más comúnmente utilizado es “www”, que significa “World Wide Web”. Generalmente se usa para identificar diferentes servidores o instancias en un dominio.

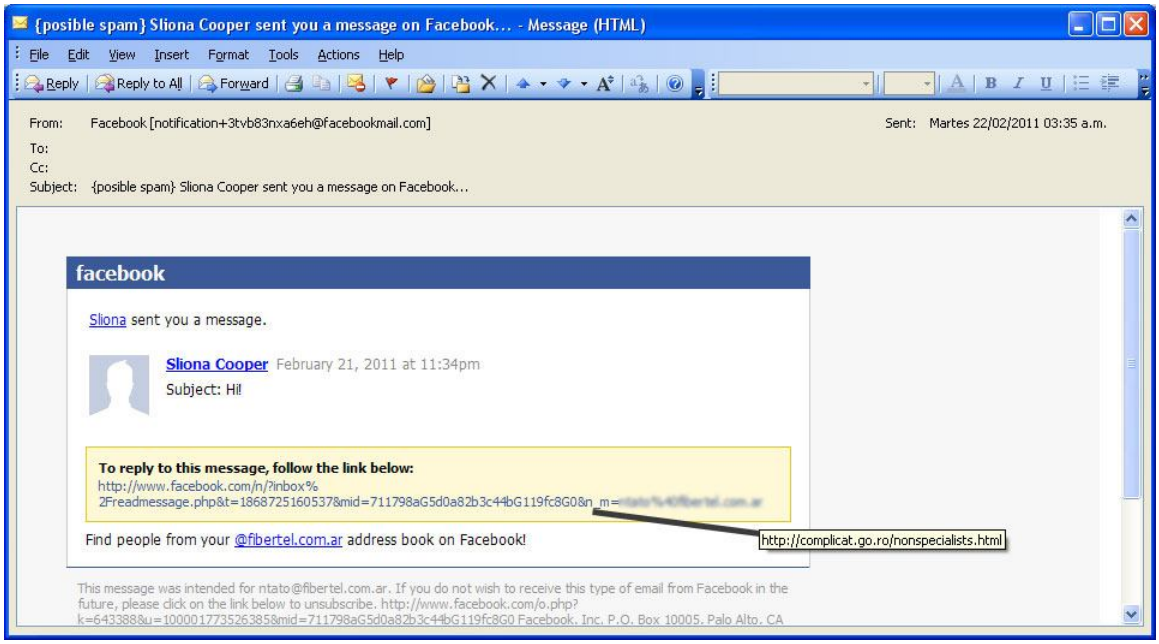
La conjunción de dominio de segundo nivel y dominio de primer nivel identifican a un sitio. Es decir, la empresa Facebook se identifica por el segundo nivel (Facebook) unido al primer nivel (.com). La URL www.facebook.com.ar no representa necesariamente al sitio www.facebook.com, porque difieren en el dominio de primer nivel.
Aunque generalmente las grandes empresas suelen adquirir los dominios tanto internacionales como locales (por ejemplo Yahoo posee tanto yahoo.com como yahoo.com.ar; lo mismo que Hotmail, Google, Bing y Facebook); pero empresas pequeñas o con poco conocimiento de estos temas, o sin presupuesto suficiente para adquirir dominios, o carentes de eficiencia para recuperarlos, no lo hacen. Por ejemplo, la agencia oficial de noticias Telam posee telam.com.ar, pero no telam.com. Por el contrario, el Colegio Público de Abogados de la Capital Federal (CPACF) recuperó tanto cpacf.com.ar como cpacf.com, este último luego de batallar en un tribunal arbitral internacional; y posee también cpacf.org.ar y cpacf.org. Todas esas URL llevan al mismo sitio.

Habiendo aclarado lo anterior, entonces surge evidente que www.facebook.com es el mismo sitio que www.server1.facebook.com, pero es un sitio diferente a www.facebook.server1.com.

Otro ejemplo del desconocimiento de Internet radica en los correos electrónicos. El remitente de un correo electrónico es muy fácilmente falsificable, incluso por alguien sin demasiados conocimientos informáticos. De hecho, los mails son casi anónimos realmente, y salvo que el sistema de envío de correo electrónico incluya la dirección IP del remitente (Hotmail lo hace, Gmail no), es muy difícil determinar el origen del mismo. Es por ello que si el contenido de un correo electrónico resulta al menos un poco sospechoso, se debe corroborar por otro medio el origen del mail, y bajo ningún aspecto abrir los archivos adjuntos.

A continuación hay un ejemplo que simula una notificación de Facebook. Pero el link, en lugar de llevar al sitio de Facebook, lleva a otro sitio (en el ejemplo, a http://complicat.go.ro/nonspecialists.html), tanto en el caso del nombre “Silona Cooper” como en el link inferior.





Nótese que si bien la URL en azul que indica un dominio de Facebook, en realidad está apuntando al dominio complicat.go.ro; desnudando que también una URL en un mail no necesariamente indica la URL real. El objetivo de estos tipos de mail puede ser tanto robar la clave del usuario como simplemente sumar su dirección de mail a una base de datos.

Para finalizar, pero sin profundizar en el tema, mencionaremos que los archivos adjuntos pueden contener virus o no, dependiendo del sistema operativo del usuario y el tipo de archivo (en los sistemas operativos de Microsoft, el tipo de archivo lo define su extensión, por ejemplo “.com”, “.doc”, etc) y no siempre el Antivirus lo puede interceptar.

Hay muchos otros temas a los que podríamos referirnos para intentar encuadrar esta realidad virtual que denominamos informática e Internet; pero lo dicho hasta ahora debería suficiente para que, extrapolando, el lector descubra que **la ignorancia de las víctimas sobre el tema es un factor esencial en el delito informático.**

Perfil del delincuente informático y la víctima

Si bien hace una década podían establecerse perfiles más o menos definidos tanto sobre el delincuente como sobre la víctima, el acceso generalizado a la informática y a Internet ha llevado a que cada vez más personas de diversas condiciones se encuentren en una u otra posición. Hoy en día, es tan fácil como habitual que una persona viole derechos de autor, o utilice alguna técnica de cracking para instalar un software (aunque más no sea la introducción de una clave que no ha adquirido legalmente), como que una computadora hogareña se vea infectada por virus o troyanos con diversas intenciones.

En primer lugar, veremos los perfiles de los delincuentes y víctimas para los casos más específicos, relacionados principalmente con los delitos informáticos como objeto, principalmente el Hacking y el Fraude Informático.

▪ Delitos informáticos "de guante blanco"

Las personas que cometen los «Delitos Informáticos» son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, **los *sujetos activos* tienen habilidades para el manejo de los sistemas informáticos y/o generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible**, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.
Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, **la persona que «ingresa» en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.**
El nivel típico de aptitudes del delincuente informático es tema de controversia ya que **para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico**, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.
Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los «delitos informáticos», **los estudiosos en la materia los han catalogado como «delitos de cuello blanco» término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943**.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como **«delitos de cuello blanco»**, aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las **«violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros»**.
Asimismo, este criminólogo estadounidense dice que **la definición** de los «delitos de cuello blanco» no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino **de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que:**

> ***«El sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional».***

Respecto al **Sujeto Pasivo** vamos a definirlo como el **sujeto sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo**.
Normalmente son grandes empresas, públicas o privadas, siendo los bancos de los más atractivos. La mayor parte de los delitos informáticos no son descubiertos o denunciados a las autoridades responsables, ya que los mismos tienen miedo de dejar al descubierto la falta de seguridad que poseen, generando una "invisibilidad" del delito informático.

Es difícil elaborar estadísticas sobre ambos tipos de delitos.
Sin embargo, **la cifra es muy alta; no es fácil descubrirlo y sancionarlo**, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; **existe una gran indiferencia de la opinión pública sobre los daños ocasionados** a la sociedad; **la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos «respetables»** otra coincidencia que tienen estos tipos de delitos es que, **generalmente, «son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad»**.
Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.
Por su parte, el «Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos» señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto **los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada**. Asimismo, **la ONU resume** de la siguiente manera a **los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:**

• **Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.**
• Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
• **Falta de especialización de las policías, fiscales y otros funcionarios judiciales** en el campo de los delitos informáticos.
• Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
• **Carácter transnacional de muchos delitos** cometidos mediante el uso de computadoras.
• **Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional**.

En síntesis, es destacable que **la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la**

interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

▪ Delitos informáticos en general

Si hace unos años sólo las grandes empresas y las instituciones u organismos públicos eran objeto de incidentes de acceso no autorizado por terceros (hackers), **ahora puede ser potencialmente víctima de los mismos cualquier familia o pequeña empresa que tenga una conexión más o menos permanente a Internet.**

Las víctimas suelen ostentar una o algunas de las siguientes características: ingenuidad, candidez, desconocimiento, falta de educación, desatención, necesidad, avaricia, búsqueda de venganza.

A modo de ejemplo, podemos mencionar aquellas personas que quieren acceder a cuentas de correo de otras personas (parejas, socios, o ex exposos), y googlean, es decir, ingresan en un buscador como Google, la siguiente frase: “como Hacker Hotmail”, lo cual remite a una serie de sitios cuya finalidad oculta es obtener información del internauta el cual, con tal de acceder a la cuenta de Hotmail de la otra persona, no escatima en brindar información propia, comenzando con su propia clave de correo electrónico.

También están aquellos sitios y correos que afirman identificar a aquellos contactos de Hotmail que “no te admiten”; con la misma finalidad de robar la contraseña.
Por otro lado, es muy fácil redactar un correo cuyo remitente no es quien figura; y adjuntarle un archivo “troyano”, que el destinatario abrirá ya que considera que el remitente es alguien conocido.

En estos casos, se produce también la denominada "invisibilidad" del delito informático, teniendo su razón de ser en el carácter anónimo de Internet, el cual provoca en la víctima la sensación, rayana con la certeza, de que la Justicia penal no podrá dar con el responsable del ataque en su contra. La víctima siente que se enfrenta a un ser "invisible" ante cuyos ataques sólo queda resignarse, por lo que pocas veces denuncian los hechos que se dan en su perjuicio.

Internet es un nuevo mundo, lo que podríamos llamar “una realidad paralela” o “realidad virtual”, en las cuales las personas se desenvuelven, con mayor o menor carga emocional. En esta nueva realidad, las personas se relacionan tanto emocional, como profesional y económicamente.
Pero resulta fundamental considerar que esta realidad tiene sus propias reglas, y dada la novedad de esta nueva realidad, muchas personas acceden a ella aplicando reglas de otros ámbitos, convirtiéndose en blanco fácil de los delitos.

Perfil de la victima de Scamming

Una práctica habitual en el scamming consiste en contratar gente para que intermedie en transacciones de dinero. Generalmente, dentro de los engañosos avisos que circulan, el perfil buscado del mulero oscila entre los 21 y 50 años. Entre los requisitos que suelen enumerar figuran que el potencial empleado debe ser comunicativo, cumplidor, despierto, capacitado para ir aprendiendo en el proceso de trabajo y responsable. No hace hincapié en el nivel educativo y prometen una paga de 1000 a 4000 euros mensuales. Una cifra atractiva para un trabajo de solamente dos horas diarias, fácilmente combinable con otras ocupaciones. En otros casos, el único requisito imprescindible, ser titular de una cuenta bancaria será suficiente para poder convertirse en intermediario de una persona de la cual no sabe su nombre y jamás le verá la cara.

El perfil de las víctimas de estafas por internet se corresponde con el de una persona -hombres y mujeres en igual medida- de entre 20 y 40 años y un nivel adquisitivo medio.

Perfil del agresor y la víctima de cyberbulling

Al igual que en el bullying convencional, el rango de edad tanto de los agresores como de víctimas se comprende entre los 11 y los 16 años, plena edad donde los niños están formándose como personas. Según el investigador Ferrán Barri, “los acosadores provienen de cualquier capa de la sociedad pero todos tienen unos rasgos en común. Todos han sido educados en valores como la sumisión y la prepotencia, no en la igualdad, y están acostumbrados a avasallar al otro”. Los adolescentes agredidos, por su parte, suelen ser niños muy sobreprotegidos, tímidos y con una severa dificultad en socializar y comunicarse.

Casos reales

- **Estafas (phishing y scamming)**

Mariano 7. Octubre 2007

A mi me estafaron con una oferta de trabajo de una supuesta inmobiliaria. Yo envié todos mis datos, porque supuestamente era para trabajar como agente de reserva inmobiliaria y un día sin avisarme me hicieron una transferencia de 3188 euros a mi cuenta bancaria. y me enviaron un mensaje al móvil donde decía que un cliente iba a hacer transferido la seña de una vivienda en mi cuenta y ese dinero debía enviar 3029 a una persona para la inversión de otro inmueble en Moscú y que lo debía hacer rápido porque el otro agente lo necesitaba para dentro de 1 una hora.

Yo le dije que ellos debían de pedirme permiso a mí ante de hacer transferencia en mi cuenta, pero me dijeron que yo era el único agente que estaba disponible y que lo debía hacer yo, y como me vieron con dudas me llamaron como 10 veces en cosas de 30 minutos y como me estaba molestando tanto yo que estaba en el trabajo y en una llamada me quisieron insinuar que si yo me quería quedar con ese dinero. y para que no me molestaran mas decidí hacer el envió por wester union a la persona que me dijeron en el sms, sin saber que estaba cometiendo un delito, pero como yo me quede con al duda, eso fue el 20/9/07 el 21/9/07 me pase por el banco pero como salí tarde del trabajo ya estaba, entonces lo deje para el lunes que lo tenia libre por ser de fiesta en al ciudad donde trabajo, y el lunes a 8:30 ya yo estaba al lado de la oficinas del banco porque a mi lo que me vino la mente fue que cuidad si esa gente lo que hacían era blanquear dinero y yo sin saberlo había participado de un delito de blanqueo de dinero.
Pero cuando llego al banco lo primero que el digo al administrativo es que iba a que diera información de la transferencia que me hicieron el 20/9/07 porque tenia duda de quien me había hecho la procedencia y la chica busco y me dijo que no había ningún problema que todos estaba bien y luego llego uno de los encargado y se cercioró del tema porque me conocía y me dijo que me había puesto una denuncia desde otra ciudad por transferencia fraudulenta yo me que de perplejo y me entro un miedo en el cuerpo, y le pregunte qué que debía hacer yo, y el me dijo que fuera a poner una denuncia la comisaría de policía.
Y Fue a comisaría y no quede detenido ahí mismo por suerte, y entonces le di toda la información que tenia y le dije que yo iba a buscar el dinero prestado y lo iba devolver y así lo hice. Y ahora todos so estaba en los tribunales de Cádiz, ya os infamaré con lo que se suceda.

Ricardo 20. Septiembre 2007

Hola que tal he recibido una oferta di donde me dicen que un familia se a muerto pero que tiene una gran suma de dinero y que escogieron correos al azar para ver quien iba a ser el afortunado de ganarse el 10%...-

Carolina. 12. Diciembre 2010

Me llegó un mail del trabajo, donde pedían que respondiera para evitar que la cuenta fuera eliminada. Sólo debía responder el mail.
Un día después, me llegó un mail de –supuestamente- un administrador de mails de yahoo.com; pidiéndome que respondiera con mis datos (incluyendo la clave) para no dar de baja la cuenta. En ese momento estaba con mucho trabajo, y no reflexioné realmente; por lo cual respondí con todos los datos que me pedían.
Al otro día, mis contactos recibieron un mail en el cual decía que yo restaba en Europa, varada, y necesitaba dinero.
Cuando yo traté de entrar a mi cuenta, la clave ya no funcionaba: me habían robado la cuenta de correo.
Tuve que realizar varios pasos para volver a recuperar mi cuenta de correo (en la cual tenía muchos correos importantes); pero finalmente lo logré, y no hubo daño considerable; ya que mis contactos reconocieron el mail como una estafa.

- ## Hurto

1º de Marzo de 2011.- Argentina.
La víctima, un empresario industrial de Rosario, lo advirtió cuando fue a realizar una operación bancaria y le informaron que de su cuenta habían retirado más de 500 mil pesos . La maniobra fue cometida hace dos semanas y en apenas cinco días hábiles . Los delincuentes lograron apoderarse del botín luego de obtener nombre de usuario y contraseña del comerciante.
Una decena de giros desde la cuenta original, asentada en una de las sucursales del Nuevo Banco de Santa Fe, permitieron concretar la estafa. El delito se cometió a través del sistema home banking , que permite movilizar dinero desde cualquier computadora.
Allí le dijeron que el medio millón de pesos fue esfumándose mediante una decena de transferencias, algunas cercanas a los 100 mil pesos . El dinero era traspasado a entidades bancarias de Rosario y de otros puntos del país. Esa ruta es la que permitió dar con algunos de los involucrados en la estafa.
Por el caso están detenidos cuatro hombres, uno de ellos un ex empleado bancario a quien, pese a su experiencia, no se le atribuye un rol preponderante en el golpe.
Todos son de Rosario. **Ninguno tiene antecedentes delictivos ni relación personal o comercial con el empresario. Fueron apresados en sus domicilios particulares luego de retirar la plata de los cajeros. Apenas logró recuperarse un porcentaje menor del dinero robado. "Tenemos que ver en qué carácter recibieron ese dinero. Porque también pudo ser de buena fe, como pago por algo**.
El entorno del empresario, capaz de obtener y filtrar a terceros sus datos bancarios, también estaba en la mira. Ayer no se descartaba que se produzcan más detenciones.

- ## Acoso

24 de Agosto de 2009.- Reino Unido. Ha sido condenada una joven de 18 años por acosar mediante Facebook a una compañera de colegio, incluso amenazándola de muerte. La joven tendrá que pasar tres meses en una institución penal por ciber-acoso, hostigación verbal e incluso física presentada durante varios años.
Un tribunal de Worcester le prohibió el contacto con sus conocidos y a difundir información sobre sí misma por Internet.
"Es la primera condena por esta modalidad virtual y se trata de un importante precedente", comentó Emma-Jane Cross, de la organización 'antimobbing' Beatbullying.
El acoso en Internet se extiende con cada vez mayor rapidez y podría resultar "más dañino que el típico 'mobbing' en la escuela", considera la experta.

- ## Pedofilia y Grooming

2009.- Argentina. "Se contactó con la chica por el chat, pero nunca le confesó su edad. Él, de 23 años, dijo que era como ella, de 12. Con el tiempo entró en confianza, la sedujo y le propuso que se encontraran personalmente. La tarde que la pasó a buscar por su escuela, ella se sorprendió: su amigo tenía 10 años más. Pero ya se había ganado su

confianza. Conversaron y caminaron unos metros hasta la plaza Alberdi, en Mataderos. Después de 20 minutos de charla, volvió a sorprenderla: la llevó hasta una zona poco transitada dentro del parque, la violó y se fue. Ella volvió a su casa y trató de disimular la angustia. Unos días después se quebró, le contó a su madre e hicieron la denuncia. El fue detenido el 30 de julio, después de más de 20 días de búsqueda, mientras chateaba en un locutorio de Morón."

Grooming. El grooming de niños por Internet (o simplemente grooming) es un nuevo tipo de problema relativo a la seguridad de los menores en Internet, consistente en acciones deliberadas por parte de un/a adulto/a de cara a establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual, posiblemente por medio de abusos. "A veces, se hacen pasar por nenas de 15 años para que los chicos le manden información vital: dónde viven y a qué colegio van", explica Inda Klein, investigadora especializada en niñez y nuevas tecnologías. "Los seducen, entran en confianza con ellos, y después les piden filmarlos con la web cam o que se saquen fotos", dice. Y agrega: "Si se niegan, empiezan las intimidaciones: desde hackear la computadora hasta amenazas contra miembros de su familia". Este acoso fue definido como grooming, y lo aplican con menores de entre 9 y 13 años.

También aprovechan el anonimato de la red para intercambiar material. El 15 de mayo de 2009, un organizador de viajes de egresados, un coordinador de grupos Boy Scouts y un comerciante del norte del conurbano bonaerense fueron arrestados, acusados de integrar una banda de pedófilos. Los sospechosos habrían iniciado los contactos en la calle: se acercaban a niños de bajos recursos y les ofrecían comida, alojamiento, y hasta los llevaban de vacaciones para poder fotografiarlos y filmarlos desnudos. Luego, habrían compartido ese material por correo electrónico y por chats.