



The image is a slide titled 'Temas a tratar' (Topics to be discussed) from the PDI (Policía de Investigaciones de Chile). The PDI logo is on the left. The slide lists the following topics:

- Estructura BRICIB
- Estadísticas de uso de la red a nivel mundial, latinoamericano y chileno.
- Estadísticas crecimiento de delitos
- Realidad nacional
- Tipos delitos que afectan al país

On the right side of the slide, there is a small image of a person's hands typing on a keyboard.

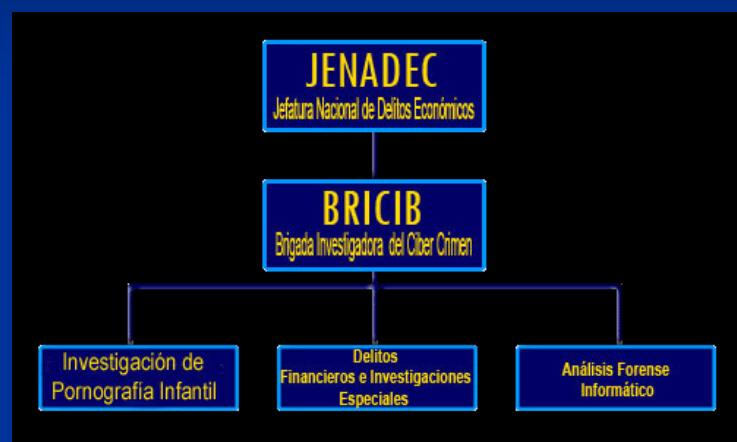


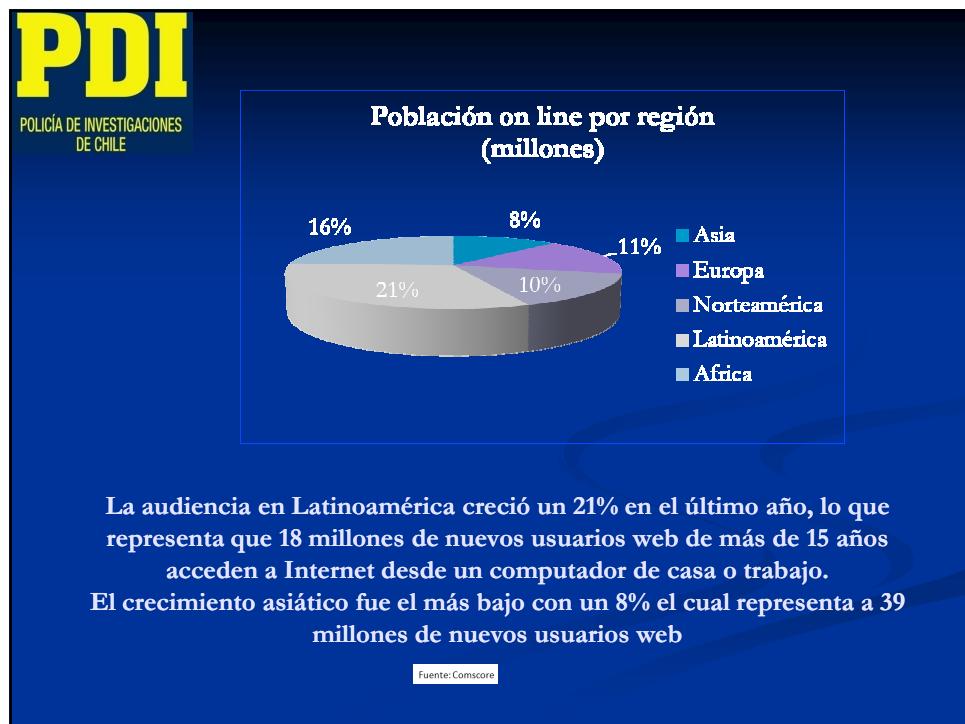
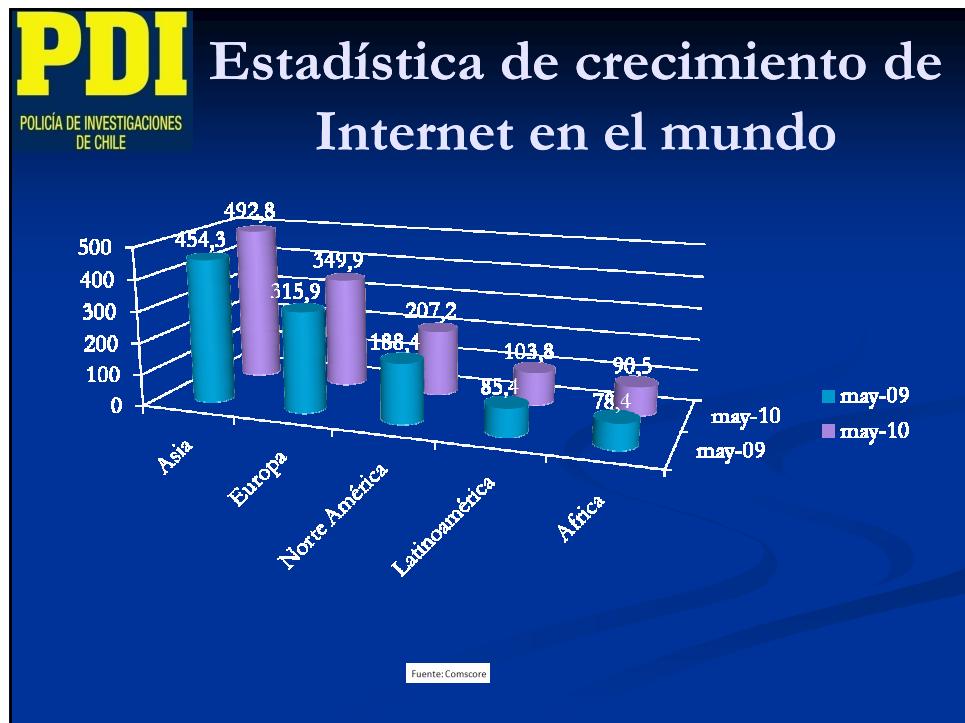
Historia

- La BRICIB se creó el 16 de octubre del año 2000.
- Su misión, apoyar a las demás Unidades en la investigación de los delitos informáticos y/o tecnológicos.
- Al comenzar a operar, se abrió una brecha investigativa no explotada en nuestro país, siendo receptora de numerosas órdenes investigar remitidas por Tribunales.



Estructura Interna de BRICIB





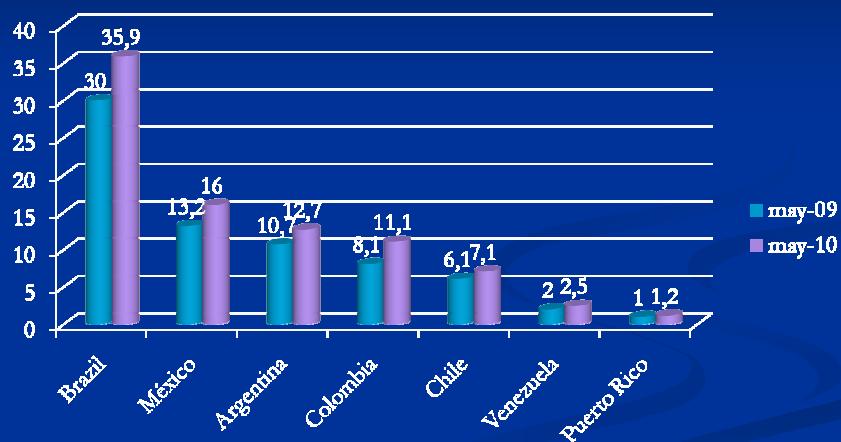


Factores influyentes en el crecimiento de Internet

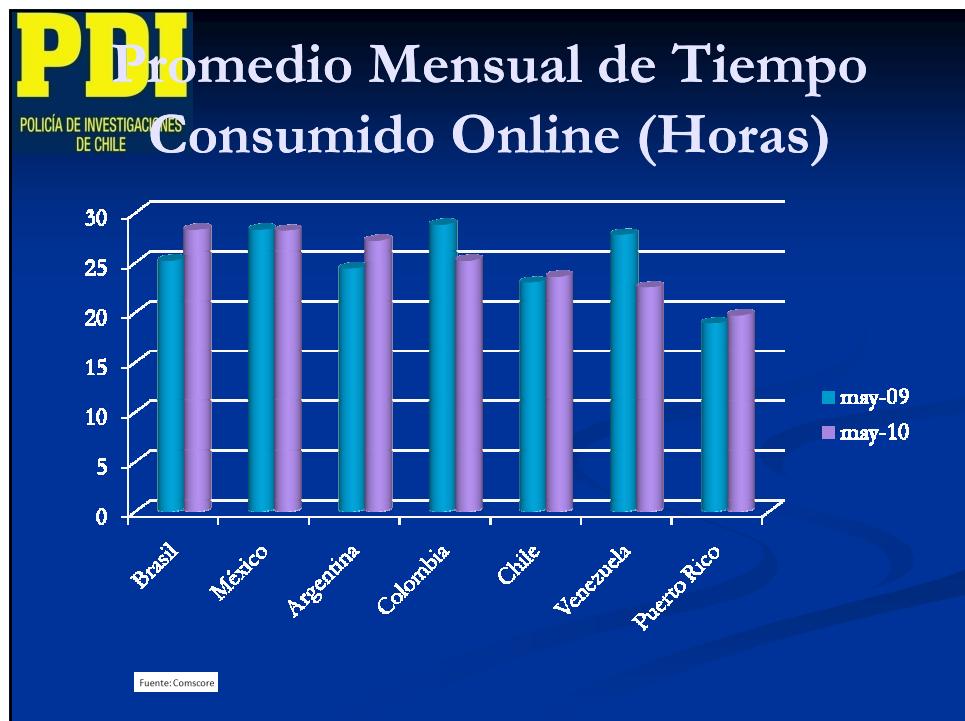
- Desarrollo de nuevas tecnologías.
- Variedad tecnológica y su bajo costo.
- Diversidad y bajo costo de acceso a la red (conexiones).
- Cantidad ilimitada de servicios que ofrece la red (pago de servicios, obtención de documentos, información variada, videos, música, mensajería instantánea, etc.).



Estadística de crecimiento de Internet en Sudamérica



Fuente: Comscore



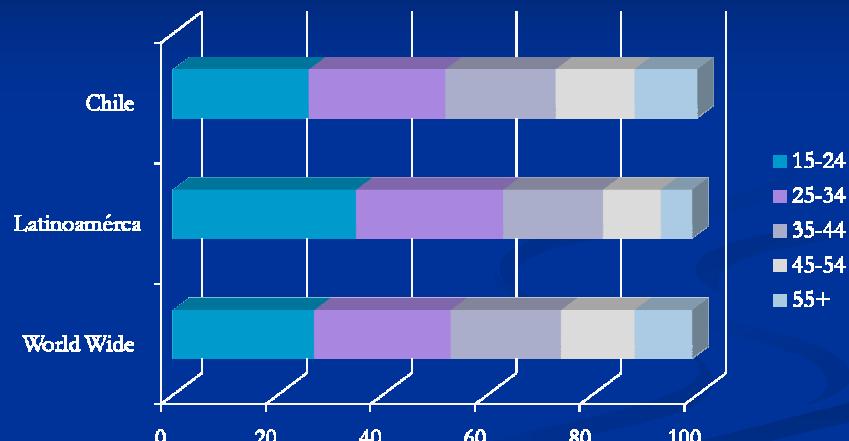


Los Usuarios Web Chilenos son en General Mayores que el Resto de los Latinoamericanos

- La distribución de edad en Chile es marcadamente similar al promedio Mundial, no así el resto de Latinoamérica y otros mercados en desarrollo, que se muestran muy jóvenes.
- La distribución de género en Chile es también la más igualitaria en Latinoamérica: el 50% de los usuarios de Internet son mujeres.



Edad de los Usuarios



Fuente: Comscore



Marcas Mundiales y Chilenas Representadas entre las Principales

- La ubicación de Google puede ser acreditada a la popularidad de su herramienta de búsqueda como también a YouTube (propiedad de Google).
- Facebook está arremetiendo dramáticamente, no sólo como un sitio de alto alcance sino que con muy alto uso.
- El alto alcance y uso de los sitios de Microsoft es dado por su aplicación de mensajería instantánea.
- Sitios chilenos tales como Terra, Empresa El Mercurio S.A.P, Grupo La Tercera, y Falabella se incluyen en los principales 25, como también un grupo de proveedores en idioma Español.

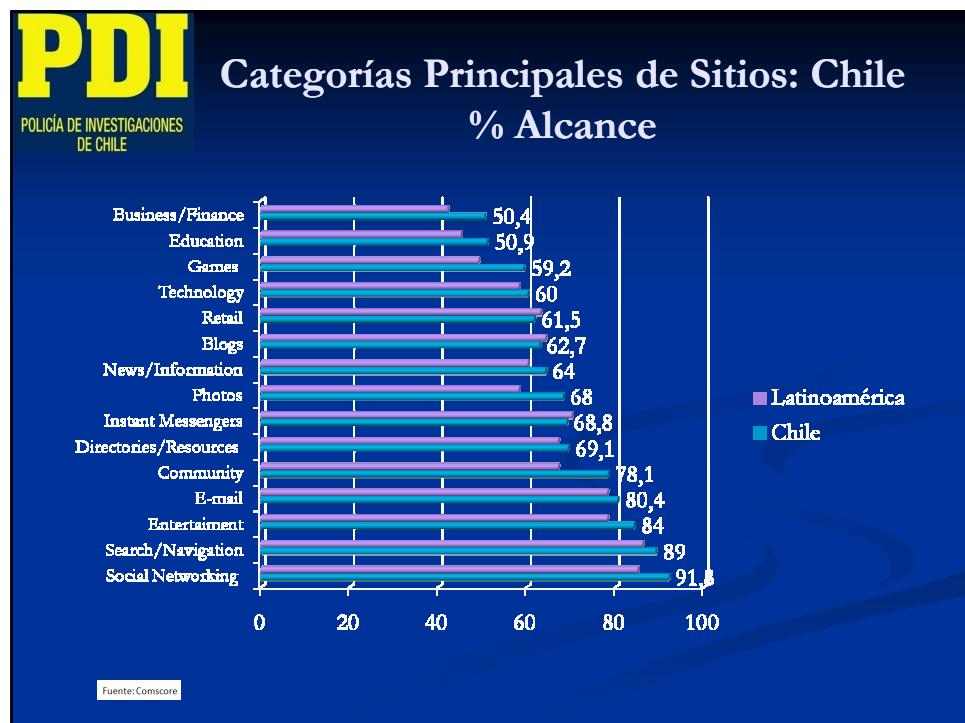
Principales "Properties" Audiencia Chilena			
	Total Visitantes Únicos (000)	Chile % Alcance	Promedio Minutos por Visitante
Google Sites	6,797	95.5	197.2
FACEBOOK.COM	6,219	87.4	274.0
Microsoft Sites	6,069	85.3	523.4
Terra - Telefónica	4,120	57.9	20.2
Yahoo! Sites	3,397	47.7	19.8
Wikimedia Foundation Sites	3,215	45.2	11.5
Empresa El Mercurio S.A.P.	2,888	40.6	46.3
TARINGA.NET	2,495	35.1	14.3
Grupo La Tercera	2,175	30.6	19.4
Hi-Media Group	2,114	29.7	50.7
Orange Sites	2,103	29.6	4.9
World Bank	2,079	29.2	4.1
MercadoLibre	2,056	28.9	21.4
NetShelter Technology Media	1,761	24.8	6.3
MEGAUPLOAD.COM	1,661	23.3	31.1
CONDUIT.COM	1,653	23.2	17.9
RapidShare AG	1,369	19.2	34.9
VEVO	1,358	19.1	8.9
AOL LLC	1,313	18.5	4.4
MUSICA.COM	1,280	18.0	7.8
OLX INC.	1,267	17.8	6.4
Grupo Falabella	1,150	16.2	14.0
BANCOESTADO.CL	1,105	15.5	18.5
Ponti.Univ. Católica de Chile	1,042	14.6	13.8
Hispavista Sites	1,041	14.6	6.4

¹³ Audiencia Chilena 15+ accediendo a Internet desde Hogar o Trabajo
Fuente: comScore Media Metrix, Abril 2010



¿Cómo utiliza Chile la Internet?

- Búsqueda/Navegación es la principal categoría en América Latina pero Redes Sociales es la principal en Chile. Los chilenos visitan sitios de entretenimiento (incluyendo música, películas, TV, multimedia, Noticias de Entretenimiento, humor) en una tasa que es mucho mayor al promedio regional.
- Sitios de Comunidad son más populares en Chile que el resto de América Latina.
- La mitad de todos los usuarios web Chilenos visitaron un sitio de Negocios/Finanzas, una tasa muy superior al promedio regional de 37.4 porciento.



PDI
POLICIA DE INVESTIGACIONES
DE CHILE

El Alto Alcance de las Redes Sociales en Chile es conducido por Facebook

Facebook es la red social más popular en Chile, con un 85% del total de la audiencia Chilena. Muchos sitios que se categorizan así mismos como "Redes Sociales" pueden en realidad operar paralelamente a sitios como Facebook ofreciendo funcionalidades extendidas: Fotolog, Badoo, Bligoo y Slideshare son todos ejemplos. Se espera que esta tendencia incremente, en la medida que los sitios traten de hacerse indispensables para sus usuarios, como lo hace Facebook.

Top Social Networks: Chile % Alcance

Sitio	% Alcance
FACEBOOK.COM	85.0
FOTOLOG.COM	30.3
Windows Live Profile	28.0
TWITTER.COM	9.8
BADOO.COM	7.7
BLIGOOG.COM	7.1
SLIDEShare.NET	6.4
MySpace	4.7
SONICO.COM	4.1
HI5.COM	3.6

Top Social Networks: Chile Minutos Promedio por Usuario

Sitio	Minutos Promedio por Usuario
FACEBOOK.COM	275.0
FOTOLOG.COM	52.1
Windows Live Profile	4.0
TWITTER.COM	19.3
BADOO.COM	124.9
BLIGOOG.COM	1.7
SLIDEShare.NET	1.8
MySpace	10.6
SONICO.COM	8.0
HI5.COM	16.1

comSCORE. © comScore, Inc. Proprietary and Confidential. 16 Audiencia Chilena 15+ accediendo a Internet desde Hogar o Trabajo. Fuente: comScore Media Metrix, Abril 2010.

PDI
POLICIA DE INVESTIGACIONES
DE CHILE

Delitos mas denunciados

Información reservada de la PDI CiberCrimen



Delitos mas denunciados

Información reservada
de la PDI
CiberCrimen



Cantidad de delitos denunciados e investigados por BRICIB

Información reservada
de la PDI
CiberCrimen



Delitos asociados a las tecnologías de la información y la comunicación

- Delitos informáticos contra sitios web (teams hackers).
- Delitos informáticos por accesos indebidos a cuentas de correo, facebook, blogs.
- Usurpaciones de nombre (en virtud a accesos indebidos o publicaciones a nombre de un tercero).
- Amenazas vía correo electrónico o mensajería instantánea.



Delitos asociados a las tecnologías de la información y la comunicación

- Almacenamiento y distribución de material pornográfico infantil (intercambio de material en redes p2p, salas de chat, mensajería instantánea y correos electrónicos).
- Ciber Bullying: definido como cualquier forma de maltrato psicológico, verbal o físico producido entre escolares de forma reiterada a lo largo de un tiempo determinado



Delitos asociados a las tecnologías de la información y la comunicación

- Gooming: podría definirse como acciones deliberadas por parte de un adulto cuyo fin es 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.
- Injurias y Calumnias (delitos de acción penal privada).



Fraudes por Internet y con uso de tecnologías

- Carta nigeriana
- Estafa y otras defraudaciones
- Infracción Ley N° 19.223 (Phishing, Pharming)
- Infracción a ley N° 20.009 (Medios de Pago)



Carta Nigeriana

- Fraude o engaño que se lleva a cabo principalmente por correo electrónico no deseado, adquiere su nombre del número de artículo del código penal de Nigeria que viola, ya que buena parte de estas estafas provienen de ese país.
- Esta estafa consiste en ilusionar a la víctima con una gran fortuna, que en realidad es inexistente, con objeto de persuadirla luego para que pague una suma de dinero por adelantado como condición para acceder a la supuesta fortuna

Estafas por Internet

- Estafas **on line**: Actividad mediante la cual un sujeto publica una o mas especies en Internet, ofreciéndolas por un valor menor al del mercado, por lo general son artefactos tecnológicos y de última generación, tales como notebooks, teléfonos celares (Iphone) y televisores LCD, por lo cual, los clientes al ver estas ofertas, son quienes generalmente contactan al imputado.





Clonación de tarjetas

- **Clonación de tarjetas:** Es toda actividad que implique la copia de la información contenida en la banda magnética de una tarjeta de crédito o débito.

para realizar esta actividad es preciso contar con ciertas herramientas, tales como las señaladas a continuación:



Clonación de Tarjetas

Para realizar esta actividad es preciso contar con ciertas herramientas, tales como las señaladas a continuación:





Clonación de tarjetas

- Métodos de ocultamiento de las herramientas que permiten la captura de la información de las bandas magnéticas.



Clonación de tarjetas



Dispositivo
sobrepuerto



Keylogger

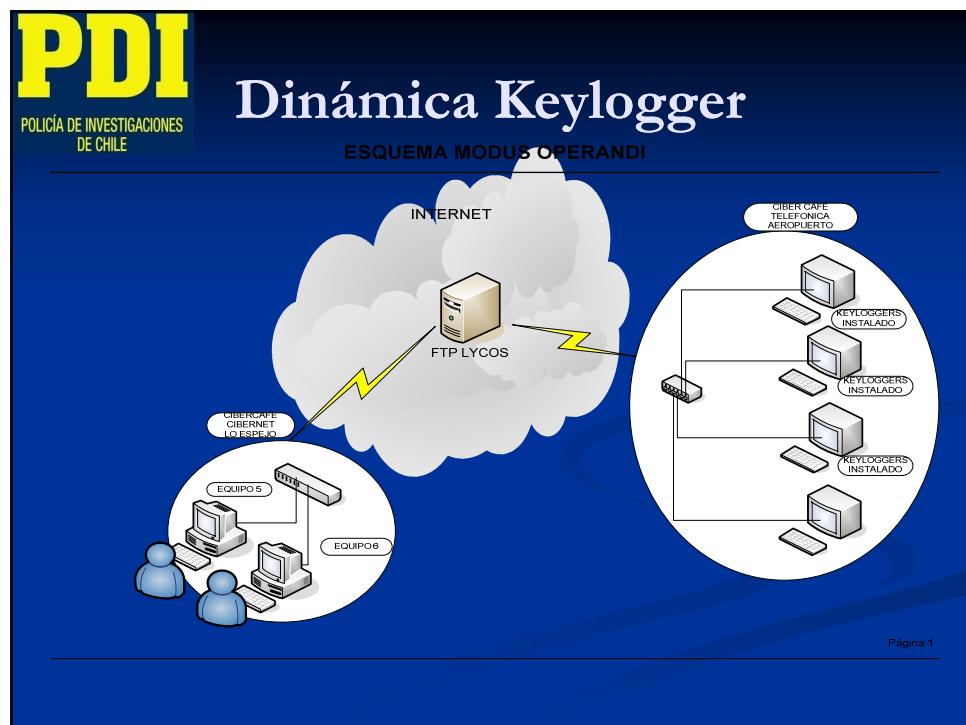
- Software que se encarga de registrar las pulsaciones que se realizan en el teclado, para memorizarlas en un fichero y/o enviarlas a través de internet a un servidor ftp o casilla electrónica, utilizado generalmente para capturar contraseñas de e-mail, bancarias u otras.



KEYLOGGER

- SOFTWARE.
- Obtención de datos.
- Fácil instalación.
- Lugares públicos.
- Fraudes internos.







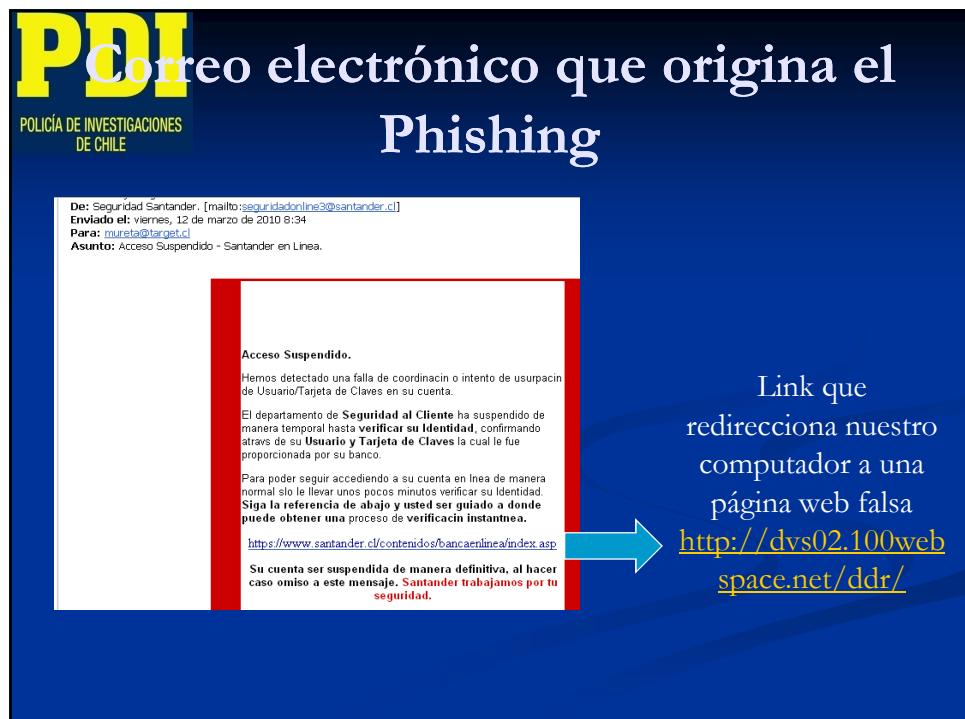
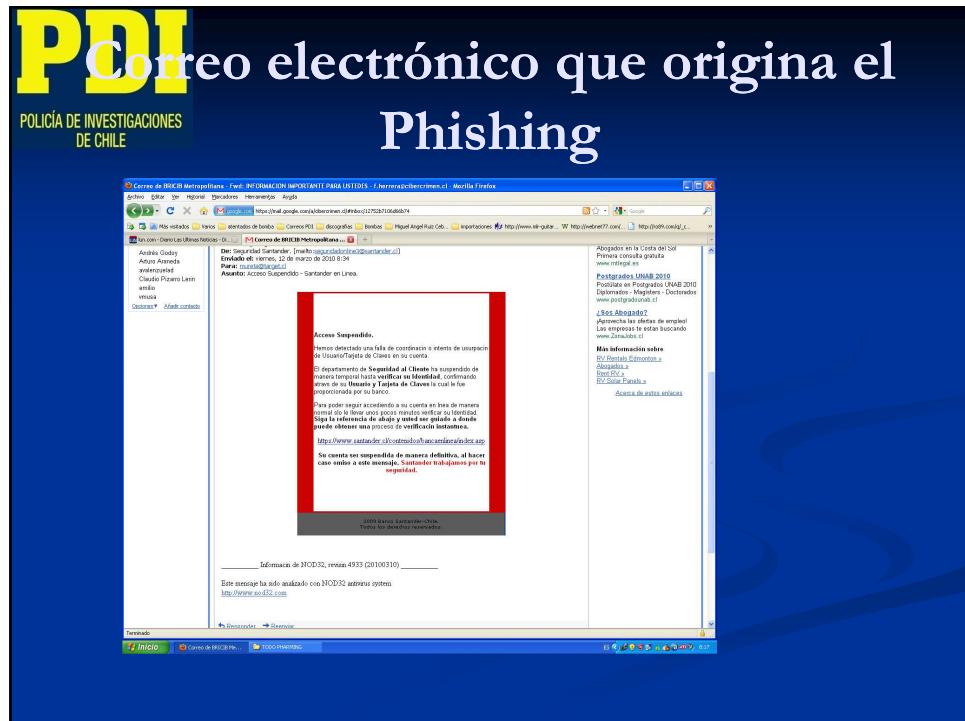
Phishing

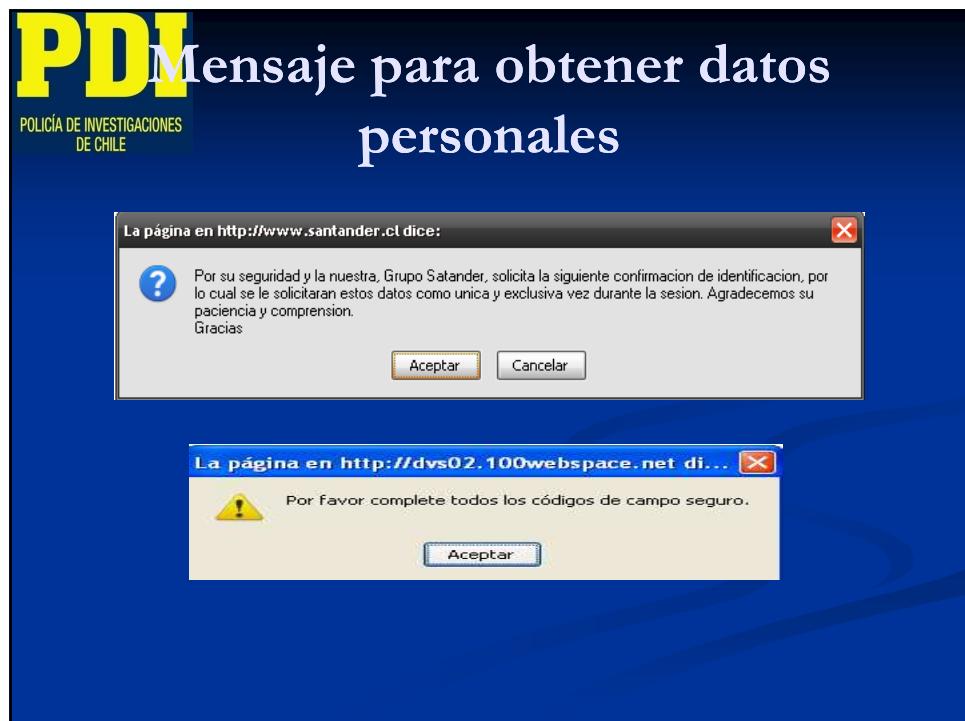
- El término Phishing proviene de la palabra inglesa "fishing" (pesca),^[1] haciendo alusión al intento de hacer que los usuarios "piquen en el anzuelo". A quien lo practica se le llama Phisher.
- Este delito se tipifica en nuestro país como sabotaje informático, infracc. a la ley 19.223 de delitos informáticos o bien como Estafas y otras defraudaciones.



Phishing

© Jefatura de Gabinete de Ministros - 2009. Todos los Derechos Reservados. Prohibida su edición, modificación y/o alteración y su reproducción, exhibición y/o distribución en forma total o parcial, con fines de lucro.





PDI Captación de datos de la tarjeta de coordenadas

POLICÍA DE INVESTIGACIONES DE CHILE

Seguridad en nuestros servicios en línea

Estimado cliente de Santander Santiago, con el fin de prevenir fraudes electrónicos estamos actualizando su información en nuestra base de datos bancaria. Complete la información solicitada. Obtén más información de la seguridad en línea y de cómo Santander Santiago protege tu información con una llave de 128 bits.

Digite la SuperClave Proporcionada.

A1	B1	C1	D1	E1	F1	G1	H1	I1	J1
A2	B2	C2	D2	E2	F2	G2	H2	I2	J2
A3	B3	C3	D3	E3	F3	G3	H3	I3	J3
A4	B4	C4	D4	E4	F4	G4	H4	I4	J4
A5	B5	C5	D5	E5	F5	G5	H5	I5	J5

©2009 Santander Santiago. Todos los derechos reservados.

PDI Evolución de Phishing

“Pharming”

POLICÍA DE INVESTIGACIONES DE CHILE

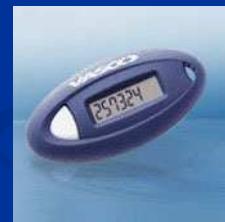
- Propagación mediante correo electrónico el cual lleva un código malicioso que infecta un computador.
- Suplanta una entidad bancaria y solicita datos críticos.
- Debido a la infección ocurre un redireccionamiento a sitio web fraudulento.
- Aparece solicitud para ingresar tarjeta de coordenadas.
- Finalmente, se efectúan traspasos de dineros a diversas cuentas, debido a que al entregar los datos bancarios los estafadores tiene control total de estas.



Métodos de prevención

- Verificación de link
- Habilitación de tarjeta coordenadas o digipass.
- Software detector de phishing o malware. (antivirus, ad-aware etc.)
- Capacitación constante del personal y para el personal.

	A	B	C	D	E	F	G	H
1	210	635	253	432	198	236	149	325
2	112	228	339	446	555	662	774	888
3	210	635	253	432	198	236	149	325
4	100	200	300	400	500	600	700	800
5	210	635	253	432	198	236	149	325
6	210	635	253	432	198	236	149	325
7	210	635	253	432	198	236	149	325
8	953	505	113	228	339	446	555	662
9	210	635	253	432	198	236	149	325
10	953	505	113	228	339	446	555	662
	582	365	689					



Evolución de Phishing Pharming

- Correo electrónico, que lleva un código malicioso que infecta un computador.
- Suplantando una entidad bancaria Solicita datos críticos.
- Debido a la infección ocurre un redireccionamiento a sitio web fraudulento.
- Aparece solicitud para ingresar tarjeta de coordenadas.
- Finalmente, se efectúan traspasos de dineros a diversas cuentas, debido a que al entregar los datos bancarios los estafadores tiene control total de estas.



- Una vez que el usuario digita en el explorador la URL del banco, el computador infectado redirecciona nuestra solicitud a una página web falsa, que tiene por objeto captar nuestros datos personales, como por ejemplo:

<http://www.santander.cl/>

Dirección IP **200.75.19.81**

Lo que realmente hace peligroso al Pharming es que realiza su ataque sobre estos datos siendo su principal objetivo el cambiar la correspondencia numérica de la dirección IP, por lo cual, los usuarios infectados no notarán que navegan en una URL falsa, debido a que el código malicioso se activa cada vez que se digita en el navegador www.bancoestado.cl.



Como modifica una persona mi computador?

**Información reservada
de la PDI
CiberCrimen**



Efectos de la infección

- El fichero **hosts** almacena una pequeña tabla con las direcciones de servidores y direcciones IP que más suele utilizar el usuario. Al modificar este fichero, por ejemplo, con falsas direcciones de bancos online, en el navegador se escribirá el nombre, pero nos enviará a una página que no corresponde con la real.

```

hosts - Bloc de notas
Archivo Edición Formato Ver Ayuda
189.236.245.182 bancoestado.cl
189.236.245.182 www.bancoestado.cl
189.236.245.182 www.santandersantiago.cl
189.236.245.182 santandersantiago.cl
189.236.245.182 santander.cl
189.236.245.182 www.santander.cl
189.236.245.182 www.bancosantander.cl

```



POLICÍA DE INVESTIGACIONES
DE CHILE



```

hosts - Bloc de notas
Archivo Edición Formato Ver Ayuda
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Este es un ejemplo de archivo HOSTS usado por
#
# Este archivo contiene las asignaciones de las
# host. Cada entrada debe permanecer en una lín
# debe ponerse en la primera columna, seguida d
# La dirección IP y el nombre de host deben sep
#
#
# También pueden insertarse comentarios (como é
# o a continuación del nombre de equipo indicán
#
# Por ejemplo:
#
#       102.54.94.97      rhino.acme.com
#       38.25.63.10      x.acme.com

```

```

hosts - Bloc de notas
Archivo Edición Formato Ver Ayuda
216.222.205.203 www.santander.cl
216.222.205.203 http://www.santander.cl
216.222.205.203 santander.cl
216.222.205.203 http://santander.cl
216.222.205.203 www.santandersantiago.cl
216.222.205.203 http://www.santandersantiago.cl
216.222.205.203 santandersantiago.cl
216.222.205.203 http://santandersantiago.cl

```



Formas de infección del Pharming

1. Postales Electrónicas (Es la más común y más usada).
2. Celular Gratis (Simula a la víctima haber ganado un teléfono celular)
3. Poemas de Amor (Simula recibir un poema especial)
4. Ábrete Sexo (Simula obtener una cuenta Premium de una página para adultos)
5. Facebook (Simula una invitación de amigos de facebook)
6. Video Youtube (Simula una recomendación de youtube para ver un video Gracioso)
7. Cuenta Desactivada (Simula que tu cuenta de correo está desactivada y que por favor verifiques tus datos para que no sea eliminada).



Virus identificados

- Algunos de los virus ya identificados son los siguientes

Información reservada
de la PDI
CiberCrimen

PDI
POLICÍA DE INVESTIGACIONES
DE CHILE

Ejemplo virus windll32.exe

- Si hacemos clic en el link de la supuesta postal, un archivo ejecutable se descarga desde la web del delincuente, en el momento en que ejecutemos dicho archivo, un código malicioso se instala en el equipo.



Malware /UNAM-CERT

PDI
POLICÍA DE INVESTIGACIONES
DE CHILE

Infección por postal

- Junto con la infección del virus en el equipo la que resulta imperceptible para el usuario se despliega una postal, de esta forma el usuario no sospechará que se infectó con un virus, para este en particular la postal que se despliega es la siguiente:



PDI
POLICÍA DE INVESTIGACIONES
DE CHILE



PHARMING

**Información reservada
de la PDI
CiberCrimen**

PDI
POLICÍA DE INVESTIGACIONES
DE CHILE

Métodos de prevención

- Verificación de link
- Habilitación de tarjeta coordenadas o digipass.
- Software detector de phishing o malware. (antivirus, ad-aware etc.)
- Capacitación constante del personal y para el personal.-

	A	B	C	D	E	F	G	H
1	212	635	253	432	198	236	149	325
2	112	339	446	198	236	774	884	325
3	212	635	253	432	198	236	149	325
4	953	565	113	228	339	446	555	662
5	212	635	253	432	198	236	149	325
6	953	565	113	228	339	446	555	662
7	212	635	253	432	198	236	149	325
8	112	339	446	198	236	774	884	325
9	212	635	253	432	198	236	149	325
10	953	565	113	228	339	446	555	662
	362	365	688					



