



INGENIERÍA SOCIAL PARA NO CREYENTES

Carlos A. Biscione

Technical Account Manager North of Latin America

Sun Microsystems



Contenido

- Ingeniería Social en Perspectiva:
 - > Definiciones.
 - > Objetivos.
- Técnicas y Herramientas de Ingeniería Social:
 - > Invasivas o Directas o Físicas.
 - > Seductivas y/o Inadvertidas.
- Como Defenderse:
 - > Tips Simples para Defenderse.
 - > Como Identificar al “Hacker Social”.
 - > Estrategias de Combate.
- Recursos para saber más.

Contenido

- **Ingeniería Social en Perspectiva:**
 - > **Definiciones.**
 - > Objetivos.
- **Técnicas y Herramientas de Ingeniería Social:**
 - > Invasivas o Directas o Físicas.
 - > Seductivas y/o Inadvertidas.
- **Como Defenderse:**
 - > Tips Simples para Defenderse.
 - > Como Identificar al “Hacker Social”.
 - > Estrategias de Combate.
- **Recursos para saber más.**

Una buena manera de esconder algo es mostrarlo.

Anónimo.

Si necesitas algo, solo pídelo. El secreto del éxito en obtenerlo está en la manera de pedirlo.

Anónimo.



Definiciones

- La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.
 - Carole Fennelly.
 - The human side of computer security.
 - SunWorld, Julio 1999.
- Término usado entre crackers y samurais para referirse a las técnicas de violación que se sustentan en las debilidades de las personas mas que en el software. El objetivo es engañar a la gente para que revele contraseñas u otra información que comprometa la seguridad del sistema objetivo.
 - Traducción moderada de THE COMPLETE SOCIAL ENGINEERING FAQ!
 - <http://packetstorm.linuxsecurity.com/docs/social-engineering/socialen.txt>



Contenido

- **Ingeniería Social en Perspectiva:**
 - > Definiciones.
 - > **Objetivos.**
- **Técnicas y Herramientas de Ingeniería Social:**
 - > Invasivas o Directas o Físicas.
 - > Seductivas y/o Inadvertidas.
- **Como Defenderse:**
 - > Tips Simples para Defenderse.
 - > Como Identificar al “Hacker Social”.
 - > Estrategias de Combate.
- **Recursos para saber más.**

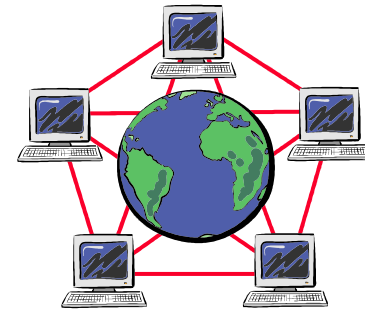
Objetivos (¿Qué Quieren Hacer?)*

- Los objetivos básicos de la Ingeniería Social son los mismos del “hacking” o “cracking” (dependiendo de quien lo haga) en general: ganar acceso no autorizado a los sistemas, redes o a la información para...
 - > Cometer Fraude,
 - > Entrometerse en las Redes,
 - > Espionaje Industrial,
 - > Robo de Identidad (de moda),
 - > Irrumpir en los Sistemas o Redes.



Objetivos (¿A Quien Van Dirigidos?)*

- Las víctimas típicas incluyen
 - > Empresas Telefónicas
 - > Servicios de Helpdesk y CRM
 - > Corporaciones Renombradas
 - > Agencias e Instituciones Gubernamentales y Militares
 - > Instituciones Financieras
 - > Hospitales.
- El boom de la internet tuvo su parte de culpa en la proliferación de ataques a pequeños “start-up’s”, pero en general, los ataques se centran en grandes compañías.



Contenido

- Ingeniería Social en Perspectiva:
 - > Definiciones.
 - > Objetivos.
- Técnicas y Herramientas de Ingeniería Social:
 - > **Invasivas o Directas o Físicas.**
 - > Seductivas y/o Inadvertidas.
- Como Defenderse:
 - > Tips Simples para Defenderse.
 - > Como Identificar al “Hacker Social”.
 - > Estrategias de Combate.
- Recursos para saber más.

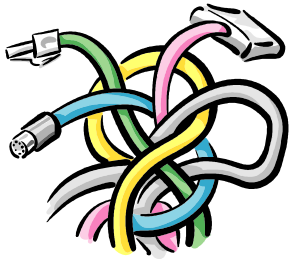
Técnicas y Herramientas de Ingeniería Social

Invasivas o Directas o Físicas



Técnicas de Ingeniería Social

(Invasivas o Directas o Físicas)



- **El Teléfono**
- **El Sitio de Trabajo**
- **La Basura**
- **La Internet-Intranet**
- **Fuera de la Oficina**



El Teléfono

- Personificación Falsa y Persuasión
 - > Tretas Engañosas: Amenazas, Confusiones Falsas.
 - > Falsos Reportes de Problemas.
- Personificación Falsa en llamadas a HelpDesks y Sistemas CRM
 - > Completación de Datos Personales
- Robo de Contraseñas o Claves de Acceso Telefónico:
 - > Consulta de buzones de voz.
 - > Uso fraudulento de líneas telefónicas.
 - > Uso de Sistemas Internacionales de Voz sobre IP.



El Sitio de Trabajo

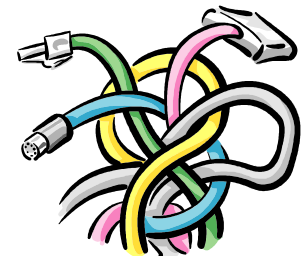
- Entrada a los sitios de trabajo

- > Acceso Físico no Autorizado
- > Tailgating



- Oficina

- > “Shoulder Surfing” (ver por encima del hombro), Leer al revés.
- > Robar, fotografiar o copiar documentos sensibles.
- > Pasearse por los pasillos buscando oficinas abiertas
- > Intentos de ganar acceso al cuarto de PBX y/o servidores para:
 - > Conseguir acceso a los sistemas,
 - > Instalar analizadores de protocolo escondidos, sniffers o,
 - > Remover o robar pequeños equipos con o sin datos.



La Basura

- “Dumpster Diving” o ¿Qué hay en nuestra basura?:
 - > Listados Telefónicos.
 - > Organigramas.
 - > Memorandos Internos.
 - > Manuales de Políticas de la Compañía.
 - > Agendas en Papel de Ejecutivos con Eventos y Vacaciones.
 - > Manuales de Sistemas.
 - > Impresiones de Datos Sensibles y Confidenciales.
 - > “Logins”, “Logons” y a veces... contraseñas.
 - > Listados de Programas (código fuente).
 - > Disquettes y Cintas.
 - > PapelMembretado y Formatos Varios.
 - > Hardware Obsoleto.



La Internet-Intranet

- Si en algo es consistente un usuario es en repetir passwords.
- “Password Guessing”
 - > Placa del Carro.
 - > Nombre de la HIJA + 2005.
 - > Fecha de nacimiento.
- Encuestas, Concursos, Falsas Actualizaciones de Datos.
- Anexos con Troyanos, Exploits, Spyware, Software de Navegación remota y Screen Rendering.



Todos los dias sale uno a la calle...

Dear Citibank Member,

This email was sent by the Citibank server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM. This is done for your protection -- because some of our members no longer have access to their email addresses and we must verify it.

To verify your e-mail address and access your bank account, click on the link below:

Fuera de la Oficina

- Almuerzos “De Negocios” de Viernes, que terminan en volada de oficina y “Happy Hours”, con potenciales consecuencias desastrosas:
 - > Sesiones de confesión de contraseñas, extensiones, direcciones de correo electrónico. Al otro día, la víctima no se acuerda.
- Conexiones “de oficina a Oficina”:
 - > ¿Puedo leer mi e-mail desde aqui?
 - > Eso está en la Intranet de la Empresa, pero (en tono jactancioso) yo puedo entrar desde aqui.
 - > Lo que no sabe la victima es de la existencia de “KeyGrabbers”
 - > Solución: One Time Passwords.



Contenido

- Ingeniería Social en Perspectiva:
 - > Definiciones.
 - > Objetivos.
- **Técnicas y Herramientas de Ingeniería Social:**
 - > Invasivas o Directas o Físicas.
 - > **Seductivas y/o Inadvertidas.**
- Como Defenderse:
 - > Tips Simples para Defenderse.
 - > Como Identificar al “Hacker Social”.
 - > Estrategias de Combate.
- Recursos para saber más.

Técnicas y Herramientas de Ingeniería Social

Seductivas y/o Inadvertidas.



Técnicas de Ingeniería Social

(Seductivas y/o Inadvertidas.)



- **Autoridad**
- **Carisma**
- **Reciprocidad**
- **Consistencia**
- **Validación Social**
- **Ingeniería Social Reversa**



Autoridad

- Pretender estar con la gente de TI o con un alto ejecutivo en la Empresa o Institución.
- Puede usar un tono de voz:
 - > Intimidante
 - > Amenazante
 - > Urgente



Carisma

- Se usan modales amistosos, agradables.
- Se conversa sobre intereses comunes.
- Puede usar la adulación para ganar información del contexto sobre una persona, grupo o producto.



Reciprocidad

- Se ofrece o promete ayuda, información u objetos que no necesariamente han sido requeridos.
- Esto construye confianza, dá la sensación de autenticidad y confiabilidad.



Consistencia

- Se usa el contacto repetido durante un cierto período de tiempo para establecer familiaridad con la “identidad” del atacante y probar su confiabilidad.



Validación Social

- Acecha el comportamiento normal de tratar de satisfacer un requerimiento.
- Se puede tomar ventaja de esta tendencia al actuar como un compañero de trabajo necesitando información, contraseñas o documentos para su trabajo.
- La víctima usualmente es una persona con cierto potencial de ser segregada dentro de su grupo, o que necesita “ser tomada en cuenta”.



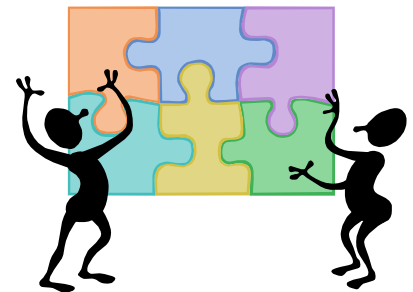
Ingeniería Social Reversa

- Ocurre cuando el Hacker crea una persona que parece estar en una posición de autoridad de tal modo que le pedirán información a él, en vez de que él la requiera.
- Las tres fases de los ataques de ISR:
 - > Sabotaje.
 - > Promoción.
 - > Asistencia.



Ingeniería Social Reversa

- ¿Como opera?
 - > El Hacker **sabotea** una red o sistema, ocasionando un problema.
 - > Este Hacker entonces **promueve** que él es el contacto apropiado par solucionar el problema, y entonces, cuando comienza a dar **asistencia** en el arreglo el problema, requiere pedacitos de información de los empleados y de esa manera obtiene lo que realmente quería cuando llegó.
 - > Los empleados nunca supieron que él era un hacker, porque su problema se desvaneció, él lo arreglo y todo el mundo está contento.



Contenido

- Ingeniería Social en Perspectiva:
 - > Definiciones.
 - > Objetivos.
- Técnicas y Herramientas de Ingeniería Social:
 - > Invasivas o Directas o Físicas.
 - > Seductivas y/o Inadvertidas.
- Como Defenderse:
 - > **Tips Simples para Defenderse.**
 - > Como Identificar al “Hacker Social”.
 - > Estratégias de Combate.
- Recursos para saber más.

Tips Simples para Defenderse



Tips Simples para Defenderse



- Mantenga una actitud cautelosa y revise constantemente sus tendencias de ayudar a personas que no conoce. **Ojo: No tiene que volverse una persona huraña y paranoica.**
- Verifique con quien habla, especialmente si le estan preguntando por contraseñas, datos de empleado u otra información sensitiva.





Tips Simples para Defenderse

- Al teléfono, obtenga nombres e identidades (Nro. De Empleado, por ejemplo). Corrobórelos y llámelos a su pretendida extensión.
- No se deje intimidar o adular para terminar ofreciendo información.
- No le permita a una persona desconocida “descrestarlo” con su aparente conocimiento.
 - > Ejemplo: Aquellos que conocen detalles técnicos o usan acrónimos o la jerga propia de la empresa o industria.



Tips Simples para Defenderse



- Muchos pueden sonar como parte de “la-cosa-real”, pero pueden ser parte de la conspiración.
- Sea cauteloso (de nuevo, no paranóico) en las encuestas, concursos y ofertas especiales via internet, teléfono y correo electrónico y convencional.
- Estas son formas comunes de cosechar direcciones de correo electrónico, contraseñas y otros datos personales.



...y...

¡Por Favor...!!!

**!!!NO
RESPONDA
MENSAJES EN
CADENA...!!!**

En un solo mensaje en cadena...

>From: "monica diaz"
 >To: yelitos96@latinmail.com, angelicamhm@hotmail.com, lilianabueno9@hotmail.com, man123@hotmail.com, sandrahdz@hotmail.com, wmm007@hotmail.com, chichodavid@starmedia.com, yasminalu@yahoo.com, y...@hotmail.com, yiyabarragan@hotmail.com, yogomez@ricarondo.com
 >Subject: FW: Fwd: Especialmente para ti!!!!
 >Date: Sat, 10 Jan 2004 19:52:31 +0000
 >

>From: "elizabeth lizcano"
 >To: menosalse@hotmail.com, zombie851@hotmail.com, eliza jael_volkova@yahoo.com.ar, mona1824@hotmail.com, ag wmm007@hotmail.com, ros
 >Subject: FW: Fwd: Especial
 >Date: Sat, 10 Jan 2004 11:21:21 -0500

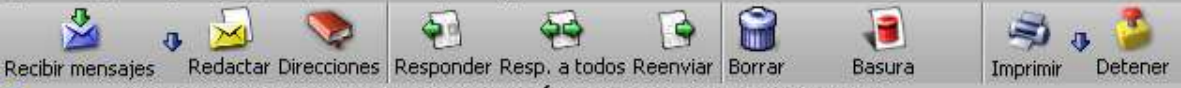
>From: "conceita mezzasalma"
 >To: la_bella1974@hotmail.com, eileen gatalok007@hotmail.com, el_nene_muckivas@hotmail.com, thebest109@mary_1977@hotmail.com, maurizio la_flaca_2003@hotmail.com, tml
 >Subject: FW: Fwd: Especialmer
 >Date: Thu, 08 Jan 2004 19:34:21 -0500

>From: "Andrea Eobadio Laskar"
 >To: missa_2811@hotmail.com, elaine_wenzels@hotmail.com, elzaha12c16@hotmail.com, kagayez30@hotmail.com, maria1612nav@hotmail.com, markaby76@hotmail.com, Pasyale13@hotmail.com, bobby_2323@hotmail.com
 >Subject: Fwd: Especialmente Para Ti!!!!
 >Date: Thu, 23 Oct 2003 19:06:15 -0400

>From: "paula andrea guerrero jurado"
 >To: aife@latinmail.com, elyerson@hotmail.com, >> dmsdaniel@latinmail.com, gaboar@hotmail.com, >> hector.j.gonzalez@ve.pwcglobal.com, jenniferhuzgy@yahoo.com, >> sustenas@arcivalores.com, lokoka@hotmail.com, >> jl_sualano@hotmail.com, adumith@rcnet.com.ve, >> manogutano@hotmail.com, marlonco@hotmail.com, >> silita23@hotmail.com, lady_marmelade@starmedia.com, >> vanessa_rivas80@hotmail.com, yamaleth511@hotmail.com, >> ymaury@latinmail.com, yekza@hotmail.com
 >> Subject: Especialmente para ti!!!!
 >> Date: Wed, 22 Oct 2003 13:53:28 -0400

@hotmail.com, deborahSexy707@hotmail.com, @hotmail.com, julianasanti_793@hotmail.com, @hotmail.com, mmolima39@hotmail.com, carema2004@hotmail.com, @hotmail.com, sandher30@hotmail.com, tina198320@msn.com,

er@hotmail.com, francie_ben@hotmail.com, andrea_5@hotmail.com, leo76_54@...@hotmail.com, mariaf_teran@...@hotmail.com, m, ptullones@hotmail.com, me007@hotmail.com, gadaladu@hotmail.com, logudice_cristina@hotmail.com, judithq@hotmail.com, com, silvana_mezzasalma@hotmail.com, snayana_italia@hotmail.com



Asunto: ACIS V JNSI - PROGRAMA ACADÉMICO DEFINIDO - 29 Abril/2005

De: [redacted]@uniandes.edu.co>

Fecha: 29/04/2005 07:43 p.m.

A: [redacted]@yahoo.com

CC: [redacted]@dijin.policia.gov.co, [redacted]@dijin.policia.gov.co, [redacted]@osi.cl, [redacted]@internet-solutions.com.co, [redacted]@ubiquando.com.co, [redacted]@santander.name, [redacted]@Sun.COM, [redacted]@fluidsignal.com, [redacted]@telecom.net.co, [redacted]@bog.br.com, [redacted]@newnetsa.com, [redacted]@digeware.com.co, [redacted]@highresults.net, [redacted]@etek.com.co, [redacted]@isagen.com.co, [redacted]@cisco.com

X-Mozilla-Status: 0001

X-Mozilla-Status2: 00000000

Return-path: <jcano@uniandes.edu.co>

Received: from tunja.Colombia.Sun.COM (esunmail [129.147.156.34]) by edgemail1.Central.Sun.COM (Planet Messaging Server 5.2 HotFix 2.02 (built Oct 21 2004)) with ESMTMP id <0IFQ004Q1T8B...>
Received: from sunmail3.sfbay.sun.com (sunmail3.SFBay.Sun.COM [129.149.247.180]) by tunja.Colombia.Sun.COM (8.12.10+Sun/8.12.10/ENSMail,v2.2) with ESMTMP id j3U4jQj3017955 for <[redacted]>
Received: from brmea-mail-1.sun.com (brmea-mail-1.Central.Sun.COM [129.147.5.31]) by sunmail3.sfbay.sun.com (8.11.7p1+Sun/8.11.7/ENSMail,v2.2) with ESMTMP id j3U4iru15158 for <carlos.bis...>
Received: from relay11.sun.com ([217.140.40.14]) by brmea-mail-1.sun.com (8.12.10/8.12.9) with ESMTMP id j3U4iqg027598 for <carlos.biscione@sun.com>; Fri, 29 Apr 2005 22:44:52 -0600 (MDT)
Received: from mms13es.sun.com (mms13es.sun.com [160.41.223.54]) by relay11i.sun.com with ESMTMP for carlos.biscione@sun.com; Sat, 30 Apr 2005 04:44:51 +0000 (Z)
Received: from mms12bas.mms.eu.btsyntegra.com (mms12bas.mms.eu.btsyntegra.com [217.140.40.30]) by mms13es.sun.com with ESMTMP for carlos.biscione@sun.com; Sat, 30 Apr 2005 04:44:51
Received: from oporapa.uniandes.edu.co (oporapa.uniandes.edu.co [157.253.50.55]) by relay12.sun.com with ESMTMP for carlos.biscione@sun.com; Sat, 30 Apr 2005 04:44:50 +0000 (Z)
Received: from oporapa.uniandes.edu.co (oporapa [157.253.50.55]) by oporapa.uniandes.edu.co (8.12.11/8.12.11) with SMTP id j3U4gFbn007957; Fri, 29 Apr 2005 23:43:24 -0500 (COT)
Received: from papalelo.uniandes.edu.co ([157.253.50.100]) by oporapa.uniandes.edu.co (SMSSMTP 4.1.4.30) with SMTP id M2005042919434605929; Fri, 29 Apr 2005 19:43:46 -0500
Received: from papalelo.uniandes.edu.co (localhost [127.0.0.1]) by papalelo.uniandes.edu.co (8.12.11/8.12.11) with ESMTMP id j3U0hKxm031422; Fri, 29 Apr 2005 19:43:46 -0500
Received: (from apache@localhost) by papalelo.uniandes.edu.co (8.12.11/8.12.11/Submit) id j3U0hcH3031410; Fri, 29 Apr 2005 19:43:38 -0500
Received: from 200.30.103.2 ([200.30.103.2]) by correo1.uniandes.edu.co (IMP) with HTTP for <jcano@correo.uniandes.edu.co>; Fri, 29 Apr 2005 19:43:37 -0500

Sender: jcano@uniandes.edu.co

Message-id: <1114821817.4272d4b9d721e@correo1.uniandes.edu.co>

MIME-version: 1.0

Content-type: text/plain; charset=ISO-8859-1

Content-transfer-encoding: 8BIT

User-Agent: Internet Messaging Program (IMP) 3.2.3

X-Authentication-warning: papalelo.uniandes.edu.co: apache set sender to jcano@uniandes.edu.co using -f

Original-recipient: rfc822;carlos.biscione@sun.com

Estimados conferencistas,

A la fecha hemos establecido el programa académico de las V Jornadas Nacionales de Seguridad Informática ACIS 2005, a realizarse los días 22, 23 y 24 de Junio del año en curso, cuya información de su charla, hora y día asignado se encuentra en <http://www.acis.org.co/index.php?id=332>. Favor revisar e indicar si es pertinente alguna actualización tanto del nombre, resumen de su charla como de su breve hoja de vida, con el fin de proceder de conformidad.

Contenido

- Ingeniería Social en Perspectiva:
 - > Definiciones.
 - > Objetivos.
- Técnicas y Herramientas de Ingeniería Social:
 - > Invasivas o Directas o Físicas.
 - > Seductivas y/o Inadvertidas.
- Como Defenderse:
 - > Tips Simples para Defenderse.
 - > **Como Identificar al “Hacker Social”.**
 - > Estrategias de Combate.
- Recursos para saber más.

Como Identificar al “Hacker Social”.

- Trata (y lo logra...) de ser creíble, luce como un profesional.
- Permanece en calma. Actúa como si perteneciera a la empresa.
- Conoce a sus víctimas y como reaccionarán.
- Reconoce al personaje alerta y lo evita.
- Sabe retirarse discretamente si algo comienza a fallar.



Como Identificar al “Hacker Social”.

- En los ataques telefónicos, se aprovechan del hecho de la mayor credibilidad de la mujer.
- Utilizan “marcas de agua” cuando usan correo convencional falso.
- Usan tarjetas de negocio y nombres (ambos) falsos. Verifíquelos antes de involucrarse.
- Tratan de manipular a las personas menos afortunadas, segregadas, a las menos agraciadas y en general a todos los que buscan validación social.
- Si el desafío es muy grande, trabajan en equipo.



Contenido

- Ingeniería Social en Perspectiva:
 - > Definiciones.
 - > Objetivos.
- Técnicas y Herramientas de Ingeniería Social:
 - > Invasivas o Directas o Físicas.
 - > Seductivas y/o Inadvertidas.
- Como Defenderse:
 - > Tips Simples para Defenderse.
 - > Como Identificar al “Hacker Social”.
 - > **Estrategias de Combate.**
- Recursos para saber más.

Estrategías de Combate:

- **Area de Riesgo**
 - > La Internet-Intranet
- **Tácticas del Hacker**
 - > “Password Guessing”
 - > Encuestas, Concursos, Falsas Actualizaciones de Datos.
 - > Anexos con Troyanos, Exploits, Spyware, Software de Navegación remota y Screen Rendering.
- **Estrategía de Combate**
 - > Refuerzo continuo del conocimiento de los cambios a los sistemas y redes.
 - > Entrenamiento en el uso de contraseñas
 - > Inducción en la creación de contraseñas “fuertes”

Estrategías de Combate:

- **Area de Riesgo**
 - > Teléfono (PBX)
- **Tácticas del Hacker**
- Personificación Falsa y Persuasión
- Personificación Falsa en llamadas a HelpDesks y CRM's.
- Robo de Contraseñas o Claves de Acceso Telefónico:
- **Estrategía de Combate**
 - > Entrenar a los empleados y helpdesk en el sentido de nunca dar passwords u otra información confidencial por teléfono
 - > Todos los empleados deben tener un PIN específico al HelpDesk
 - > Controlar llamadas larga distancia, seguir llamadas, rehusarse a transferencias sospechosas

Estrategías de Combate:

- **Area de Riesgo**

- > Sitio de Trabajo

- **Tácticas del Hacker**

- > Acceso Físico no Autorizado
- > Tailgating
- > “Shoulder Surfing”, Leer al revés.
- > Robar, fotografiar o copiar documentos sensibles.
- > Pasearse por los pasillos
- > Intentos de ganar acceso al cuarto de PBX y/o servidores

- **Estrategía de Combate**

- > Entrenamiento en uso del carnet de acceso. Presencia de Vigilantes.
- > No escriba contraseñas con alguien viendo
- > Restrinja uso de fotocopiadoras, escaners, cámaras digitales.
- > Requiera que las visitas sean escoltadas
- > Cierre y monitorée la oficina de correspondencia, cuartos de servidores y PBX.
- > Marque la información confidencial y manéjela apropiadamente

Estrategías de Combate:

- **Area de Riesgo**

- > La Basura

- **Tácticas del Hacker**

- > “Dumpster Diving” o “nadar en la basura”

- **Estrategía de Combate**

- > Mantenga toda la basura en áreas aseguradas y monitoreadas.

- > Destruya datos sensibles en papel,

- > Borre y destruya medios magnéticos (diskettes y cintas) y raye los medios ópticos (CD-ROMS, DVD´s).

- > Borre los discos de equipos obsoletos.

Estrategías de Combate:

- **Area de Riesgo**
 - > Fuera de la Oficina
- **Tácticas del Hacker**
 - > Reuniones fuera de la oficina con uso de bebidas alcoholicas.
 - > Conexiones “de oficina a Oficina”
- **Estrategía de Combate**
 - > Mantenga a los empleados alerta a través de entrenamientos continuos de conocimiento y reforzamiento de políticas de seguridad, tácticas y tretas de los Hackers sociales.

Contenido

- Ingeniería Social en Perspectiva:
 - > Definiciones.
 - > Objetivos.
- Técnicas y Herramientas de Ingeniería Social:
 - > Invasivas o Directas o Físicas.
 - > Seductivas y/o Inadvertidas.
- Como Defenderse:
 - > Tips Simples para Defenderse.
 - > Como Identificar al “Hacker Social”.
 - > Estrategias de Combate.
- Recursos para saber más.

Recursos para saber más.

- The human side of computer security.
 - Carole Fennelly.
 - SunWorld, Julio 1999.
 - Tambien se consigue en:
 - <http://sunsite.uakom.sk/sunworldonline/swol-07-1999/swol-07-security.html>
- El Hacker Social mas famoso: Kevin Mitnick
 - <http://www.kevinmitnick.com/>
 - <http://www.perantivirus.com/sosvirus/hackers/kevin.htm>
- Varios escritos famosos sobre Ingeniería Social.
 - <http://packetstorm.linuxsecurity.com/docs/social-engineering/>





INGENIERÍA SOCIAL PARA NO CREYENTES

Carlos A. Biscione

Technical Account Manager North of Latin America

Sun Microsystems

