Ingeniería Social

Engañando al eslabón más débil
en una cadena de seguridad.

Andreas Reichard
andreas.reichard@gmx.net
http://stud4.tuwien.ac.at/~e0126103/pub/bakkarbeit/social_engineering.pdf

Index de la presentación

1. Introducción

- Actividades de hackers afectan nuestra vida en sectores de economía, política y nuestra vida privada.
- Medidas técnicas para ampliar el nivel de seguridad no son suficientes.
- Existen formas de atacar que no se dirigen contra equipos, pero contra las personas operándolas.
- Esto se necesita que tomar en cuenta para poder implementar un eficiente programa de Seguridad.

2. El valor de la información 1/2

“Si conoces a los demás y te conoces a ti mismo, ni en cien batallas correrás peligro;
i no conoces a los demás, pero te conoces a ti mismo, perderás una batalla y ganarás otra;
i no conoces a los demás ni te conoces a ti mismo, correrás peligro en cada batalla.”

(Sun Tzu, “El arte de la guerra”)

2. El valor de la información 2/2

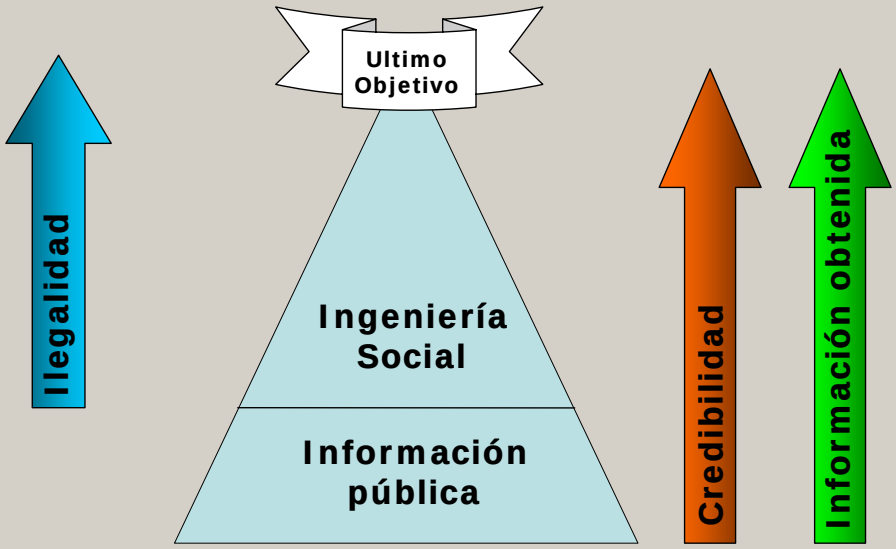
- No existe información “sin valor”, esto es solo una evaluación personal.
- Toda información puede ser útil de una manera o otra si uno sabe como usarla.
- No solo Ingenieros Sociales son especializados en extraer esta clase de información.
- Se necesita atención a que información se pasa a otra gente y si esta tiene derechos saberla.

3. ¿Que es Ingeniería Social? 1/5

- Siempre cuando dos personas se están comunicando, esta comunicación se puede explotar.
- Ingeniería Social es una manera de influir en personas para que ellos hagan cosas que, en circunstancias normales, no harían. Son técnicas de manipulación, usadas por teléfono o también en un contacto directo con la victima.
- Ingeniería Social empieza con la recogida de información para crear credibilidad.

3. ¿Que es Ingeniería Social? 2/5

El proceso de recogida de información:



3. ¿Que es Ingeniería Social? 3/5

- Herramientas para busqueda de información publica:
  - Internet (por ejemplo *www.google.com*)
  - Hot linees de telefóno
  - Listines telefónicos públicos
  - Colecciones de herramientas de búsqueda online (por ejemplo “Net detective”)

“Si hay información en un lugar puede estar muy bien protegida, pero seguro que existe en algún otro lugar también, donde cualquier persona puede cogerla.” (Carol Lane, “Naked in Cyberspace”)

3. ¿Que es Ingeniería Social? 4/5

- El objetivo de un Ingeniero Social de recoger lo más información posible es crear credibilidad y confiabilidad.
- Para crear simpatía un Ingeniero Social parece carismático, amable y atractivo a sus victimas (hay excepciones). Esto luego le ayuda para crear credibilidad, haciendo creer a otras personas que sabe información que, se supone, solo saben personas concretas (aunque no será confidencial).
- Una manera popular de atacar con Ingeniería Social es aparecer como “el colega nuevo en la empresa”.

3. ¿Que es Ingeniería Social? 5/5

- Un Ingeniero Social normalmente intenta crear un lazo social con su victima, por ejemplo demostrando simpatía por una situación desagradable de una victima - para después esperar por lo mismo, creando un sentimiento de mala conciencia y culpa en el caso de que la victima no le ayudara a su “colega”, que antes era tan compasivo.

4. Motivación y motivos 1/3

Motivación para el uso de Ingeniería Social

Q: ¿Por que se usan técnicas de Ingeniería Social?

A: Una persona que quiere cierta información, se pregunta de que manera la va a conseguir. Ingeniería Social en muchos casos es una manera más atractiva que otras más costosas. Funciona como una herramienta para los que saben como usarla.

- En muchas ocasiones, Ingeniería Social será la única manera para conseguir información que de otra manera no sea accesible.
- Aunque un ataque de Ingeniería Social puede parecer simple en su desarrollo, requiere mucha preparación y experiencia para tener éxito.

4. Motivación y motivos 2/3

Motivación para el uso de Ingeniería Social

- La motivación para un Ingeniero Social es usar una manera completamente diferente para conseguir información sensitiva, comparado con otros ataques (que se basan en la explotación de una vulnerabilidad en el software).

  "¿Para que crackear una contraseña utilizando fuerza bruta, esperando horas, si solo necesito hacer una llamada para conseguir la misma en un instante?"
  – Esto es la motivación para usar Ingeniería Social.

- Ingeniería Social se usa para de atacar los eslabones mas débiles en una cadena de seguridad: Las personas operando en ella.

4. Motivación y motivos 3/3

Motivos de Ingenieros Sociales

- ¿Por que hay personas que usan Ingeniería Social contra otras?

  Para dar respuesta a esta pregunta, solo tenemos que mirarnos a nosotros mismos de una manera honesta.

- La información que no podemos tener siempre será la que mas queremos conseguir.

- Motivos serán pura curiosidad, venganza, beneficio personal o económico, diversión, desafió y muchos más. Todos tienen en común, es que hay alguien que quiere presentar una imagen falsa de si mismo para ser capaz de acceder a información que no debe tener.

5. Características de un Ing. Soc. 1/7

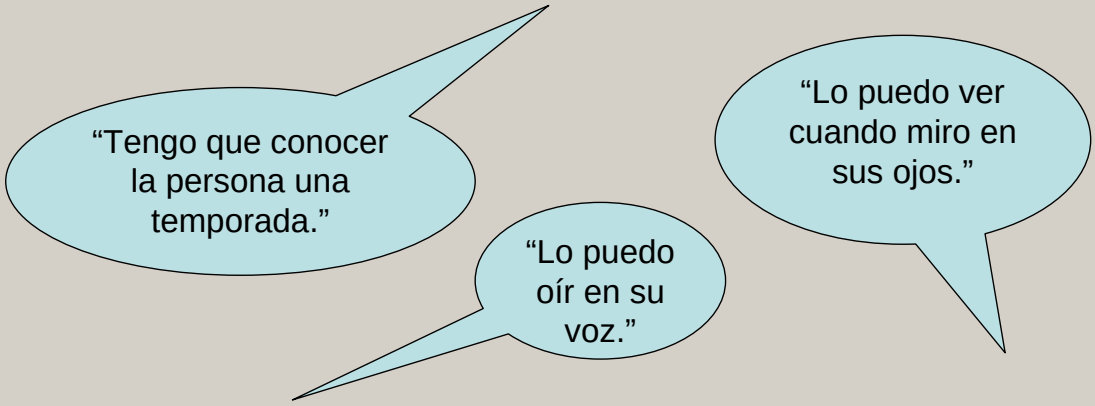
- Lo más importante para un Ingeniero Social es la impresión que produce en la gente que quiere que le ayude conseguir la información que quiere obtener.

- Esta información solo tiene valor para el si el Ing. Soc. sabe como usarla.
  ⇒ Será útil también tener suficiente conocimiento técnico.

5. Características de un Ing. Soc. 2/7

Disposiciones personales

Q: ¿Como se sabe si se puede confiar en alguien o no?



¿Son estos argumentos realmente *razones* para confiar en una persona?

5. Características de un Ing. Soc. 3/7

Disposiciones personales

- Las disposiciones personales necesarias para un Ingeniero Social son los que dan a las victimas la impresión que pueden confiar en el.
- Hay diferencias entre los sexos.
- Entran conceptos de Programación Neurolinguistica (NLP), Body Language (voz, fenotipo) y Habilidades sociales.

5. Características de un Ing. Soc. 4/7

11 12 13 14 15 16 17 18 19 20 21

Habilidades sociales

- Ingenieros Sociales en general son muy buenos actores y embusteros.
- En una conversación un Ingeniero Social cambia su actitud de forma que, mientras presenta de manera muy sutil la información que ha ganado hasta este punto para ganar confianza, aumenta la confiabilidad de sus victimas (esto a veces se llama “cold reading”) y avanzar con el desarrollo de la ataque.
- Definición de Habilidades Sociales: “el conocimiento de cómo manejar con personas y decisiones”

5. Características de un Ing. Soc. 5/7

11 12 13 14 15 16 17 18 19 20 21

Habilidades sociales

- Un Ing. Soc. tiene que ser atento por los sentimientos de otras personas y tiene que usar este conocimiento para adaptar su propia actitud.
- Es menos sobre IQ (intelligence quotient) y mas sobre EQ (emocional quotient).
- Ingenieros Sociales intentan perfeccionar el arte de leer lo mas posible sobre una persona solo con observarla o charlar con ella.
- Actúan espontáneamente y son muy flexibles, así se presentan en una manera simpática o por lo menos confiable.

5. Características de un Ing. Soc. 6/7

11 12 13 14 15 16 **17** 18 19 20 21

Habilidades sociales

- Ingenieros Sociales necesitan mucha confianza en si mismo para continuar con su escenario creado para los victimas.
- Siempre están en el peligro de ser descubiertos (para algunos esto es la razón para practicarlo, están buscando la excitación).
- La necesidad de estar preparado para todo lo que viene no significa que un atacante no tiene que preparase suficientemente *antes* del desarrollo de un ataque.

5. Características de un Ing. Soc. 7/7

11 12 13 14 15 16 17 **18** 19 20 21

Experiencia técnica

- Información solo tiene valor para un Ing. Soc. si esta sabe como usarla. En el contexto de un ataque esto será muy probablemente de una manera técnica.
- Muchos Ingenieros Sociales también tienen suficiente conocimiento sobre la materia técnica para usar la información obtenida directamente. Esta combinación de ataques psicológicos contra la gente y técnicos contra equipos hace que los Ingenieros Sociales sean bastante peligrosos.
- Kevin Mitnick dice que ha conseguido más en su “carrera” como un Hacker por su conocimiento sobre Ingeniería Social que sobre sus conocimientos técnicos.

6. Métodos de Ing. Social 1/32

- Existen varios métodos en la Ingeniería Social que se han repetido como muy típicos en el pasado.
- Sabiendo cuales son hace posible
  - evitar su éxito en el futuro,
  - y si no, entonces por lo menos disminuir el daño causad.
- Con el conocimiento sobre estos métodos se pueden crear políticas de seguridad adecuadas.
- Un Ing. Soc intenta predecir como una victima va a reaccionar cuando se pone en una situación especifica, creada por el atacante con sus métodos de ataque.

6. Métodos de Ing. Social 2/32

- Algunos Ingenieros Sociales tienen bases de datos con todas la información sobre sus victimas que podrían conseguir, recogidos durante meses antes del ataque.

  Estas bases de datos pueden contener información sobre
  - el tiempo de una persona empleada en una empresa
  - si es más cooperativa o más desconfiada al tomar una decisión
  - si es bien o mal informada sobre políticas de la empresa
  - que piensa sobre seguridad en general (importante o innecesario)
  - informacion muy personal como aficiones, los nombres y edades en la familia, deportivos favoritos, sitios de vacaciones preferidos etc.

6. Métodos de Ing. Social 3/32

11 12 13 14 15 16 17 18 19 20 21

Pidiendo ayuda

- La mayoría de la gente, cuando se le pide ayuda, no piensa mucho en cosas como seguridad, solo quiere ayudar. Es un instinto dentro de las personas que les hace creer que se puede confiar en cualquier persona que les pide ayuda que esta misma persona no les esta engañando.

- Todo lo que tiene que hacer un atacante es crear un escenario creíble para su victima para que esta pierda el pensamiento sobre seguridad (¡si es que existe!) sobre el instinto a ayudar a alguien que le pida ayuda.

6. Métodos de Ing. Social 4/32

22 23 24 25 26 27 28 29 30 31 32

Pidiendo ayuda

- In principio hay dos roles que un atacante puede coger cuando intenta a pedir ayuda de una victima.
  1. "Insider": Una persona del interior de una empresa u organización, apareciendo como un colega de la victima (algo que el atacante va presionar durante sus conversaciones con la victima, para que esta haga lo que el obligue).
  2. "Outsider": Una persona fuera de una empresa u organización (pero probablemente parte de otra que tiene una relación con la primera empresa).

- En los dos intenta el atacante que la gente crea que el es parte de algo que realmente no es. Depende del contexto de la ataque cual de las dos será la mas preferible para un atacante.

6. Métodos de Ing. Social 5/32

Pidiendo ayuda

- Un Ingeniero Social muchas veces tiene que cambiar la identidad durante un ataque.
- La manera de hacerlo es siempre la misma:
  Conseguir suficiente información sobre una persona para después presentarse como la misma de una manera creíble.
- Esto solo funciona en empresas tan grandes que no se conocen todos los empleados. En lugares donde todos se conocen, el atacante tiene que atacar de una manera indirecta.

6. Métodos de Ing. Social 6/32

Pidiendo ayuda – El “Insider”: Un colega preguntando por ayuda

- Dentro de una gran empresa es imposible que todos conozcan a todos. Las personas entran y salen, trabajadores temporales y visitantes dificultan el intento de saber quien es parte de la empresa y quien no, sin ofender a nadie.
- Durante una ataque un Ing. Soc. introduce mucho paja en la conversación y dentro de esto meten unas pocas preguntas que en realidad son la razón porque han venido a hablar con nosotros.
  La paja tapando toda la conversación solo es para que esto no se note.

6. Métodos de Ing. Social 7/32

Pidiendo ayuda – El “Insider”: Un colega preguntando por ayuda

- Pidiendo ayuda esta bien para coger y suplantar una identidad, pero combinando más técnicas (por ejemplo “name-dropping”) un atacante podrá crear presión a su victima para esforzar su deseo.
- Los Ingenieros Sociales saben como crear escenarios para poner a sus victimas en situaciones en que tendrán que omitir pensamientos sobre seguridad cuando tienen la suficiente presión (por ejemplo por miedo del Director de una empresa si se usa la autoridad de esta persona en el ataque).
- Con tanta presión las victimas reaccionan de una manera que fue prevista por el Ingeniero Social.

6. Métodos de Ing. Social 8/32

Pidiendo ayuda – El “Outsider”

- Aunque hay Ingenieros Sociales que tienen suficiente conocimiento sobre una empresa para coger un rol de “Insider”, muchas veces no es este el caso. Por lo que es mejor, coger un rol de “Outsider” (un obrero, un trabajador externo, un asociado de la empresa etc.) para conseguir suficiente conocimiento sobre una identidad dentro de la empresa para coger y explotarla en seguida.
- Aquí también un Ingeniero Social tiene que saber como presentar su rol de una manera creíble para la gente, para luego puede pasar a coger otra identidad.

6. Métodos de Ing. Social 8/32

Pidiendo ayuda – El “Outsider”

- Hay varias razones por que un atacante coge un rol de “Outsider” para atacar a una victima.
  1. No era capaz de conseguir suficiente información para aparecer creíble como un “Insider”.
  2. El atacante quiere mantener mas distancia a la empresa porque tiene miedo de que su ataque se descubra.
  3. En el escenario no es necesario coger un rol de “Insider”
- Hay unos roles bastante populares cuando un Ing. Soc. so pone de “Outsider”.
  1. El investigador
  2. El empleado de otra empresa
  3. El socio

6. Métodos de Ing. Social 9/32

Pidiendo ayuda – El “Outsider” como investigador

- El Ing. Soc. dice que esta investigando una temática relacionada con la empresa u organización que esta atacando. Así no parece sospechoso cuando pregunta cosas muy especificas (las mete en otras preguntas y paja para que no se da cuenta de la sensibilidad de la pregunta)
- La gente va a cooperar porque muchos de ellos han estado alguna vez en su vida en la misma situación y agradecieron mucho la cooperación de otra gente, ayudándoles con su investigación.
- La gente tiene mas confianza en escenarios conocidos que en otros. Por esto el atacante intenta crear un escenario familiar para su victima para crear compresión para su situación.

6. Métodos de Ing. Social 10/32

22 23 24 25 26 27 28 **29** 30 31 32

Pidiendo ayuda – El “Outsider” como empleado de otra empresa

- El atacante aparece como un empleado de otra empresa, ofreciendo un servicio para la empresa victima y necesitando una información para poder hacerlo.

- Se presenta como empleado de una empresa de
  - Telefonía
  - Redes informáticos
  - Equipos informáticos
  - Limpieza

  u otros servicios que se usan en casi todas las empresas.

6. Métodos de Ing. Social 11/32

22 23 24 25 26 27 28 29 **30** 31 32

Pidiendo ayuda – El “Outsider” como empleado de otra empresa

- Poniéndose como “el pobre, estresado empleado que solo quiere hacer su trabajo”, una persona que no le ayude cuando se lo esta pidiendo tiene que tener la sensación de que hace las cosas mas complicadas para un hombre que ya ha tenido un mal día de todas maneras.

  El uso de métodos como “name-dropping”, de autoridad o miedo puede ayudar bastante a un atacante.

6. Métodos de Ing. Social 12/32

22 23 24 25 26 27 28 29 30 31 32

Pidiendo ayuda – El “Outsider” como socio

- En este rol el atacante ejercite presión contra su victima que no sabe reaccionar de una manera adecuada porque le parecía probablemente ofensiva (aunque sería la forma correcta) y perjudicial para la actividad comercial.
- Nadie quiere tener la culpa de un error comercial porque uno de los socios se sentía maltratado por un empleado.
- El atacante sabe esto y lo usa para que su deseo no sea deniega.

6. Métodos de Ing. Social 13/32

22 23 24 25 26 27 28 29 30 31 32

Ofrecindo ayuda

- Una manera lista de atacar es causar un problema (o hacer que aparezca que hay uno) para luego ofrecer ayuda en resolverlo.
- Personas afectadas por un problema reaccionan aliviadas cuando hay alguien que les ofrece ayuda con el problema. No preguntan por aspectos de seguridad, derechos de acceso a datos sensitivos, si consiguen continuar con su trabajo lo mas pronto posible.
- Además, después de que el atacante “resolvió” el problema, victimas tienen un sentimiento de gratitud contra el que puede explotar en otro momento.

6. Métodos de Ing. Social 14/32

33 34 35 36 37 38 39 40 41 42 43

Ofreciendo ayuda

- Un ataque de esta forma consiste de dos ataques, una que causa el problema (si en realidad existe) y otra en que el atacante ofrece ayuda con resolverlo. Si el problema es real, un atacante puede usar uno de los métodos anteriores par causarlo.
- Después de haber causado el problema (o, si no existe en realidad, hacer a la victima creer que hay uno) un atacante llama a la victima y dice que es su responsabilidad que la gente afectada pueda continuar con su trabajo lo más antes posible.
- Como siempre hay poco tiempo para trabajar, las victimas quieren ayudar al atacante con todo lo que les pide, “para resolver el problema”.

6. Métodos de Ing. Social 15/32

33 34 35 36 37 38 39 40 41 42 43

Ofreciendo ayuda

- Otra vez podemos ver el típico procedimiento:
  La victima se enfrenta a presión (tiene que continuar con su trabajo, el atacante sabe esto y la a elegido por esta razón) y el atacante hace que la victima crea que el es lo que dice que es.
- Gracias a la presión, la victima está feliz de tener alguien que le ofrece una solución rápida al problema, entonces no pregunta cosas sobre seguridad etc. – solo esta pensando en continuar con su trabajo.

6. Métodos de Ing. Social 16/32

33 34 35 36 37 38 39 40 41 42 43

Name-dropping

- Para tener éxito con un ataque es esencial para un Ing. Soc. saber con que persona tiene que hablar como la “Chain of command” en una empresa.
- Name-dropping es una manera para asegurar a la victima que el atacante es en verdad quien dice quien es.
- No es lo mismo como engañar a la gente de la manera “… y si tu no haces lo que yo te digo, le voy a comentar al Señor VIP cual era la razón porque los sistemas no han funcionado a tiempo”. Esto (aunque es un poco exagerado) es otra técnica, el uso de autoridad, que vamos a ver en seguida, “name-dropping” es mas sutil.

6. Métodos de Ing. Social 17/32

33 34 35 36 37 38 39 40 41 42 43

Name-dropping

- Se trata de nombrar a personas importantes durante una conversación. Esto ayuda asegurar el rol del atacante a la victima y también puede dejarla realizar *por si misma* las consecuencias de no cooperar con el atacante.
- Name-dropping tambien ayuda el atacante con algunas personas que tienen una tendencia de hacer lo que hacen los demás, pensando “Que lo que es bueno para otros, seguro que también será bueno para mi”.
  Un Ing. Soc. sabe esto, entonces pueden intentar sugerir a una victima que otras personas que la victima respeta han cooperado con el atacante, así que la victima piensa “si ellos dicen que esta bien, supongo que es así.”

6. Métodos de Ing. Social 18/32

Usando autoridad y amenaza

- Si el name-dropping no resulta suficiente, un atacante puede aumentar la presión contra una victima, recordarle de forma directa la autoridad de una persona (o de si mismo, si se pone como esta persona) y consecuencias para la victima, sus colegas etc. de no cooperar con su demanda.

- El uso de autoridad y amenaza es una manera mas directa de name-dropping, que se podría llamar “the hardliner’s way”. Un Ing. Soc. intenta dejar esta posibilidad hasta el final porque después no hay muchas cosas que puede hacer.
  Si su victima todavía no coopera con su demanda, el atacante tiene que buscar otra manera de obtener los documentos o aceptar que no los va a conseguir de esta persona.

6. Métodos de Ing. Social 19/32

Ingeniería Social inversa

- Muy parecido a ofrecer ayuda, pero aquí la victima no es contactada por el atacante, sino al contrario.
- La victima pide ayuda con un problema causado antes por el atacante. Esto instantemente crea más credibilidad para el rol que tiene el atacante en el escenario porque el atacante se pone como persona que se debe llamar en el caso de que hay un problema.
- El Ingeniero Social contesta la llamada, diciendo que sabe exactamente lo que se tiene que hacer para resolver el problema, por ejemplo indicando a la victima instalar Malware en su ordenador.
- Otra posibilidad será que el atacante haga un rerouting de una llamada de una victima a un servicio legitimo, hablando en su lugar.

6. Métodos de Ing. Social 20/32

33 34 35 36 37 38 **39** 40 41 42 43

“Solo preguntar”

- En casos de Ingeniería Social había atacantes que simplemente preguntaron lo que querían saber, con poco más. ¿Como es posible?
- Una forma tan directa de Ingeniería Social no se puede usar en todos escenarios.
- El atacante tiene que aparentar que es normal que esté preguntando por información sensitiva. Lo que se necesita para esta manera de ataque es el arte de un buen actor con suficiente conocimiento sobre el área del escenario para poder expresarse bien (“lingo”), para crear una imagen totalmente congruente con el escenario.
- Por esto no hay muchos Ingenieros Sociales que se atreven a practicar Ingeniería Social de esta manera.

6. Métodos de Ing. Social 21/32

33 34 35 36 37 38 39 **40** 41 42 43

Peligrosas ofertas sobre E-mail

- La gente que manda estos mensajes intenta captar la atención de los recipientes de varias maneras. Se puede ofrecer algo, proclamando que hay un numero limitado (“Get it before it’s too late!”), de que hay gente compitiendo (“The first 500 to register will receive a free gift!”). Aunque las ofertas no tienen que ser maliciosos, los Ingenieros Sociales usan las mismas ideas para atacar a gente mediante el envío de E-mails.
- Intentan que la gente vaya a páginas Web preparados en que se bajan una aplicación o mandan esta aplicación como archivo adjunto en un E-mail con un contenido que causa que los recipientes al abrirlo instalen Malware en su ordenador.

6. Métodos de Ing. Social 22/32

33 34 35 36 37 38 39 40 **41** 42 43

Peligrosas ofertas sobre E-mail: E-mails persuasivos

- La gente ya más o menos debe saber que es Malware de los medios informativos. Nombres como “Anna Kournikova” o el famoso “Love letter” suenan a muchos.
  ¿Porque entonces hay todavía tanta gente que cree, cuando abre un archivos adjuntos en un E-mail o se baja una aplicación de una pagina Web, que no podría ser Malware?

- Los autores de E-mails persuasivos saben como piensa la gente, como llamar la atención para que alguien pulse el botón de su ratón para bajarse una ampliación de una pagina Web o abrir un archivos adjuntos de un E-mail.

6. Métodos de Ing. Social 23/32

33 34 35 36 37 38 39 40 41 **42** 43

Peligrosas ofertas sobre E-mail: E-mails persuasivos

- Muchos de estos peligrosos E-mails tienen asuntos como estos:
  “Re: aqui tienes la foto sexy que me pediste”
  “Re: Regalo gratuito”
  “Re: tengo lo que querías aunque me costo mucho”
  etc.

- El recipiente sabe que nunca ha mandado un E-mail para recibir tal respuesta. Pero como el asunto de la misma suena tan interesante, porque no mirar que hay dentro…

6. Métodos de Ing. Social 24/32

Peligrosas ofertas sobre E-mail: E-mails persuasivos

- Otros E-mails consiguen lo mismo, pero sin aparecer como respuestas
  “Mira esta herramienta hacker interesante”
  “Finalmente tengo acceso al portal-XXX, compruebalo”
  “Television por cable gratis – realmente sencillo”
  o simplemente
  “I love you”
  (que era el asunto de uno de los primeros E-mail Gusanos, el famoso “Love letter”)
- Los autores de estos E-mails saben que una oferta persuasiva evita que las personas intuyen el peligro que puede venir con abrir un archivo adjunto de un E-mail o bajarse una aplicación y ejecutarla. Pueden presuponer la reacción de los recipientes cuando reciben E-mails con un asunto como uno de los arriba.

6. Métodos de Ing. Social 24/32

Peligrosas ofertas sobre E-mail: E-mails de una persona conocida

- Cuando un E-mail viene de una persona conocida, la gente tiene más confianza en que no será nada malo que le han enviado.
- Un gusano es una especie de Virus que intenta divulgarse automáticamente realizando copias de si mismo.
  Lo más habitual es que usen el directorio de direcciones E-mail de Outlook u Outlook Express (que está instalado por defecto en cada instalación de Windows XP) y se manden una copia de si mismos a toda la gente conocida de la victima. Los recipientes de estos mensajes creen que su amigo les ha mandado un mensaje, abren el archivo adjunto – y el Gusano los infecta y hace lo mismo como con la victima anterior.

6. Métodos de Ing. Social 25/32

Peligrosas ofertas sobre E-mail: E-mails de una persona conocida

- De esta manera los gusanos se pueden divulgar muy rápido sobre todo el mundo. Como parecen ser mandados por gente conocida, mas gente abre los archivos adjuntos peligrosos e infecta su sistema.

  Hay mucha gente que no sospecha nada de que una pequeña aplicación que solo dice “¡Feliz navidad!” puede contener algo tan destructivo.

- El problema es que para mucha gente es suficiente conocer una persona para confiar en el contenido de un mensaje que viene de ellos. A veces algunos amigos solo nos hacen un forwarding de un mensaje, entonces el mensaje viene de ellos, si, ¡pero el mensaje original puede ser de cualquier persona, contener cualquier cosa!

6. Métodos de Ing. Social 26/32

Peligrosas ofertas sobre E-mail: E-mails falseados

- Hay otras formas de forjar E-mails para que parezca que vienen de un origen confiable, por ejemplo

  1. Robar una cuenta: - Envio es legitimo.
     - Para el usario casi indetectable si el atacante usa un programa de E-mail.

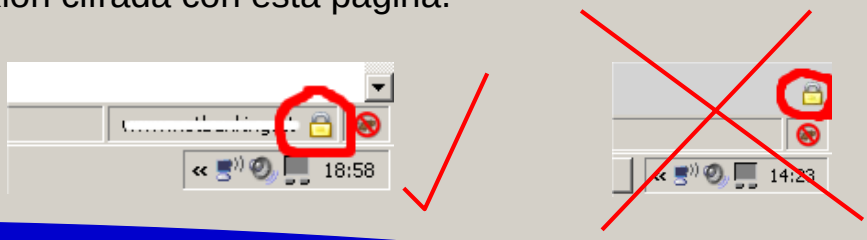
  2. Usando server-side scripts: - Existen servicios en la Web gratuitos y anónimos.
     - El header de un E-mail contiene detalles.

6. Métodos de Ing. Social 27/32

44
45
46
47
48
49
50
51
52
53
54

Paginas Web falseadas

- Muchas veces en E-mails falseados vienen enlaces a paginas Web falsas. Estas páginas Web intentan, en combinación con los E-mails, a engañar a una victima para que crea que esta en una pagina Web de, por ejemplo un banco o una compañía bien conocida (como eBay).
- Las páginas copian el diseño y gráficas de la página original, a veces también engañan a un visitador en hacerle creer que tiene una conexión cifrada con esta pagina.



6. Métodos de Ing. Social 28/32

44
45
46
47
48
49
50
51
52
53
54

Paginas Web falseadas

- De esta manera funciona el “Phishing”, que es un termino para esta forma bastante popular de conseguir información sobre cuentas de banco, E-mail providers, eBay etc.
- Los atacantes mandan una cantidad de “Phishing-mails” a todo el mundo, sabiendo que siempre hay gente que cree que estos E-mails y las páginas Web son autenticas. Y a veces es muy difícil distinguir entre una página real y una falseada.

6. Métodos de Ing. Social 29/32

Paginas Web falseadas: Como llegar allí

- La gente que no tiene mucha experiencia surfeando en Internet y por tanto se pueden engañar de manera muy sencilla para visitar una página Web falseada.

- URLs falseadas

```
http://www.paypa1.com
http://www.paypal.tripod.com
```

- Otra manera mas sofisticada de engañar a gente para visitar paginas forjadas era posible a causa de un Bug en unas versiones del navegador “Internet Explorer”.

```
http://www.myurl.com%01@badguys.com/stealpassword.asp
```


6. Métodos de Ing. Social 30/32

Paginas Web falseadas: Como llegar allí

- Además, una URL que contenía caracteres de tab podría ocultar una pagina Web del Taskbar de Windows:

```
http://www.myurl.com%01%09%09%09%09%09@
badguys.com/stealpassword.asp
```

  Antes de que Microsoft publicase unos parches para estos Bugs, mucha gente sufrió ataques de Phising basados en esto.

- No todas la confusiones con URLs son intencionadas. A veces una página Web tiene un nombre de domain que se puede confundir fácilmente con otro y en la pagina principal de la pagina dice que si un visitante quería irse al otro sitio, se ha equivocado. Algunos aun incluyen un enlace a la otra página.

6. Métodos de Ing. Social 31/32

Paginas Web falseadas: Como llegar allí

msg: dear eBay User,

It has become very noticeable that another party has been corrupting your eBay account and has violated our User Agreement policy listed:

4. Bidding and Buying

You are obligated to complete the transaction with the seller if you purchase an item through one of our fixed price formats or are the highest bidder as described below. If your are the highest bidder at the end of an auction (meeting the applicable minimum bid or reserve requirements) and your bid is accepted by the seller, you are obligated to complete the transaction with the seller, or the transaction is prohibited by law or by this Agreement.

You receive this notice from eBay because it has come to our attention that your current eBay account has caused interruptions with other eBay members. Therefore eBay requires immediate verification for your account. Please verify your account or the account may become disabled.
Click Here To Verify Your Account – http://error_ebay.tripod.com

****

Designated trademarks and brands are the property of their respective owners. eBay and the eBay logo are trademarks of eBay Inc.

6. Métodos de Ing. Social 32/32

Paginas Web falseadas: Como llegar allí

- Hay gente que no podría reconocer este mensaje por lo que es y visitara la pagina Web que se enseña en el.

  ¿Como se sabe que es falso?

  1. El uso de las palabras no es profesional. Un mensaje como este nunca sería publicado por una empresa como eBay.
  2. eBay nunca pregunta por verificación de cuentas de usarios.
  3. La URL es una de Tripod, que ya sabemos, es un proveedor de espacio Web libre.

- ¿Que pasará si una persona toma este mensaje en serio y va a la página Web indicada? Muy probablemente encontrará un formulario para introducir sus datos y después de pulsar un botón aparecería un mensaje diciendo algo como “Verificación satisfactoria. Gracias por su cooperación.”

7. Victimas de Ing. Social 1/4

Características típicas de personas vulnerables a ataques de Ingeniería Social

- Los Ingenieros Sociales hacen que personas hagan cosas que, en un contexto normal, no harán. Lo que tienen que hacer para poder desarrollar su ataque es cambiar la actitud de una victima.

- Hay personas que son más vulnerables a ataques de Ingeniería Social que otras. Esto depende de las siguientes características:
  - Seguridad en su mismo
  - La habilidad de pensar de forma lógica, también bajo presión.
  - La satisfacción en la propia situación actual (por ejemplo del trabajo).
  - Un sentimiento de desconfianza ante la gente desconocida.
  - Ingenuidad general ante la gente desconocida.

7. Victimas de Ing. Social 2/4

Características típicas de personas vulnerables a ataques de Ingeniería Social

- Los Ingenieros Sociales saben juzgar la personalidad de una persona de manera excelente. En una conversación normal y corta o solo con observar a una persona pueden decidir si esta será una buena victima para un ataque de Ingeniera Social o no.

- Basado en esta decisión usan diferentes métodos de atacar a la victima, unos más adecuados a una específica victima que otros

- Los Ingenieros Sociales eligen victimas que se puedan influir fácilmente para que luego muchas de ellas olviden sobre políticas de seguridad o no les den la importancia que deben tener.

7. Victimas de Ing. Social 3/4

Posiciones atractivas para un Ingeniero Social

- Recepcionista

- Departamento de recursos humanos (“Human resources”)
  - Informacion guardada:
    - Estado actual (trabajando, de vacaciones, enfermo, de momento trabajando en un proyecto fuera de la empresa etc.)
    - Departamento del empleado
    - Nombres de colegas
    - Superiores (esto es muy interesante si el Ingeniero Social quiere tomar la identidad de uno de ellos en una ataque)
    - Condición laboral
    - Informaciones sobre el contrato y el salario de un empleado
    - …

7. Victimas de Ing. Social 4/4

Posiciones atractivas para un Ingeniero Social

- Managers

- “Newbies”

- Temps, freelancers

- Help desk
  - Responsabilidades:
    - Cuentas de usarios (creación, eliminación, activación, desactivación, reactivación)
    - Cambiar contraseñas
    - Instalar software (por razones de seguridad los empleados no deben tener suficiente permisos para hacer esto)
    - Ofrecer ayuda con todo esto

- Departamento de Administración de la red

8. ¿Quién podrá ser un Ing. Soc.? 1/6

- Identificar un Ingeniero Social puede ser bastante difícil.
- Sin embargo hay personas que, al lado de Hackers y Crackers, tienen un buen potencial para desarrollar un ataque de Ingeniería Social por su experiencia de trabajo.
  - Ex policía
  - Ex detectives privados
  - Ex empleados
  - “Insiders”, empleados descontentos
  - Visitantes

8. ¿Quién podrá ser un Ing. Soc.? 2/6

Como identificar un Ingeniero Social

- Identificar un Ingeniero Social es muy complicado. No solo porque sabe como evitar ser descubierto, pero más porque sospechar de alguien de ser un Ingeniero Social es algo muy delicado porque la persona puede sentirse insultada.
  Esto es uno de los mayores problemas en medidas contra la Ingeniería Social.
- Los Ingenieros Sociales saben esto, para ellos es muy importante dar a los demás el sentido que estará bastante fuera de lugar preguntarles por derechos de seguridad, aunque se trata de una cosa bastante delicada donde esto se debe hacer.

8. ¿Quién podrá ser un Ing. Soc.? 3/6

Los siguientes puntos facilitan la identificación de un Ingeniero Social:

- Los Ingenieros Sociales intentan presionar a su victimas. Esta presión se puede crear de varias maneras como “name-dropping” o el uso de autoridad o amenaza.

  También pueden crear esta presión con aparecer bastante amable y cordial para crear un sentido de gratitud en una victima para que puedan esperar un favor de ellos después.

8. ¿Quién podrá ser un Ing. Soc.? 4/6

- Los Ing. Soc. hablan con mucha paja y preguntan muchas cosas. Esto no es más que una cubierta para crear el sentido de que ellos saben de lo que están hablando.
  Dentro de esto esconden unas pocas preguntas que es lo que quieren saber de verdad, pero de una manera tal que parece que no es nada especial, como lo demás.

  Una victima debe estar muy atenta a todo lo que se pregunta, independiente de lo que se dijo antes o después, sin tener miedo por preguntar a alguien por su derecho de saber una información delicada.

  Un Ing. Soc. intenta hacer sus victimas olvidar sobre estos pensamientos sobre derechos y seguridad para conseguir la información deseada.

8. ¿Quién podrá ser un Ing. Soc.? 5/6

- Mientras está preguntando, un Ingeniero Social quiere crear el sentido de que no es nada extraordinario que el pregunte estas cosas, es lo mas normal del mundo. Esto crea la ilusión de que ellos tienen todos los derechos necesarios para saber cierta información, sin que se ha comprobado esta suposición.

  Si otros no cooperan con esto, ellos usan técnicas como “name-dropping”, autoridad o amenazas para hacer a las victimas cooperar.

- Ingenieros Sociales siempre crean escenarios en que será necesario contravenir a políticas de seguridad. Son muy imaginativos en esto y nunca deben ser menospreciados porque esto es algo que cuentan ellos cuando están desarrollando su ataque.

8. ¿Quién podrá ser un Ing. Soc.? 6/6

- Ingenieros Sociales intentan aparecer confiables a otros. Lo consiguen con incluir informaciones dentro de conversaciones que han conseguido antes, mientras atacando a otra persona. Estas informaciones pueden ser aparentemente irrelevantes, pero hace creer a otras personas que el atacante es un “Insider” porque otras personas probablemente no sabrán esta información.

  Por esto es tan importante que todas las personas en una empresa entiendan el valor de la información en general. Saber cosas como el nombre de una persona simplemente no es suficiente para confiar en una persona. Solo la comprobación vale, nada más. Si no se puede conseguir en este momento, entonces se tiene que esperar hasta que se pueda conseguir. Antes no hay acceso a información.

9. Defensa contra la Ing. Soc. 1/30

Medidas técnicas

- Ingeniería Social es una manera de atacar a gente de manera psicológica.
  Sin embargo hay unas medidas técnicas que pueden asistir defenderse contra cual ataques.

- Es importante que las siguientes medidas se entiendan como solo *parte* de una infraestructura des seguridad completa.

9. Defensa contra la Ing. Soc. 2/30

Medidas técnicas

- Directorio electrónico de empleados
  - Disponible desde el Intranet
  - Contiene perfiles con una foto, teléfono, numero de móvil, dirección E-mail, posición dentro de la empresa
  - Permite busca de empleados
  - Temps y freelancers también se guardan en el directorio, pero así que se pueden distinguir de los demás
  - La información siempre tiene que ser actual
  - Usando un directorio electrónico de empleados, más importante será la atención por ataques de Ingeniería Social.

- E-mails con firmas digitales

9. Defensa contra la Ing. Soc. 3/30

55 56 57 58 59 60 61 62 63 64 65

Medidas técnicas

- Identificación de llamada
  - Cuidado con llamadas fuera de la empresa y a móviles (se pueden robar).
    Verificación de la identidad del llamante es necesaria, antes de pasarle información.
  - En caso que se recibe una llamada de un numero no verificado es lo mejor devolver la llamada a un numero verificado.
  - También es posible falsificar una identificación de llamada, pero se necesita acceso a un Switch de teléfono y conocimiento como configurarlo.

9. Defensa contra la Ing. Soc. 4/30

66 67 68 69 70 71 72 73 74 75 76

Medidas técnicas

- Contraseñas seguras
  - Restricciones en el diseño
    - No palabras que se pueden encontrar en un diccionario
    - No palabras que se pueden conseguir sobre adivinar (nombre del gato) o Ingeniería Social
    - Mínimo tamaño de una contraseña
    - No aceptar contraseñas que se pueden encontrar en un diccionario
    - Cambio de contraseña cada 2 meses sin repetir ninguna de las ultimas 3 contraseñas usadas
    - Desactivación de una cuenta después de 3 intentos fallidos de entrar con una contraseña incorrecta
    - No aceptar contraseñas que solo tienen letras.
  - La gente tiene que estar atento a nunca dar su contraseña a otra persona. Un mensaje prara recordarles esto puede aparecer cada vez que se cambia una contraseña.

9. Defensa contra la Ing. Soc. 5/30

Medidas técnicas

- Seguridad física en áreas sensitivas
  - Áreas sensitivas de una empresa tienen que tener puertas especiales con un pasillo de seguridad por los que solo pueda pasar una persona a la vez (contra “piggybacking”)
  - Por supuesto también tendrán que autenticarse a un guarda de seguridad o usando una Smartcard.
  - Mejor no solo poder verificar la autentificación de manera electrónica, sino también tener un guarda de seguridad, interviniendo en un intento como el de arriba.
  - Por lo menos se debe instalar una camara observando la entrada.
- Filtros E-mail
  - Configuración asi que E-mails conteniendo archivos adjuntos sospechosos (como ejecutables) no pueden pasar.
    ⇒ Responsabilidad de decisión se pasa de hombre a machina

9. Defensa contra la Ing. Soc. 6/30

Formación y entrenamiento

- Es la parte más importante en las defensa contra Ing. Soc.
- Programa de concienciación
  - La mejor manera de educar a gente para reaccionar de manera correcta cuando se enfrenta a un ataque de Ingeniera Social es mediante un programa de formación.
  - *Todos* empleados deben atender periódicamente. Se deben desarrollar programas para
    - Managers
    - Personas de IT
    - Usarios de ordenadores
    - Empleados no de IT
    - Asistentes administrativos
    - Recepcionistas
    - Guardias de seguridad
    - Empleados de limpieza
    - Temps y freelancers

9. Defensa contra la Ing. Soc. 7/30

66 67 68 **69** 70 71 72 73 74 75 76

Formación y entrenamiento

- Programa de concienciación
  - En caso de que un empleado cambia de posición dentro de la empresa, es necesario que se forme de nuevo para estar preparado para sus nuevas responsabilidades.
  - Un diseñador tiene que dejar suficiente tiempo a la gente para que piensen sobre la materia y las cosas que aprendan durante el programa de formación.
  - Un diseñador tiene que considerar los métodos de educación más eficientes.
  - Una compañía no tiene que inventarse un programa de educación, hay empresas especializadas en esto (a veces tambien en hacer tests de penetración de la seguridad de una compañía).
  - Existen certificados para gente que ha terminando con éxito un programa así, esto puede dar motivación extra para los empleados.

9. Defensa contra la Ing. Soc. 8/30

66 67 68 69 **70** 71 72 73 74 75 76

Formación y entrenamiento

- La falta de interés en la temática de seguridad
  - Uno de los problemas más grandes de la seguridad en general es convencer a la gente que hay necesidad para ella.
    Muchas personas piensan que la seguridad es algo que les complica la vida y el trabajo y mejor evitarlo porque es incomoda.
  - La gente tiene que entender que no solo equipos se pueden atacar, pero también personas, usando Ingeniería Social.
    Tienen que aprender sobre los métodos que se usan.
  - *"Esto nunca podría pasar a mi, ¿quien será tan tonto para dejarse influir de esta manera?"* – muchas personas piensan así si se enfrentan a la materia de Ingeniería Social.
  - Hasta que no se cambia esta manera de pensar, ataques de Ingeniería Social continúan tener éxito.
    Por esto existen programas de entrenamiento de concienciación.

9. Defensa contra la Ing. Soc. 9/30

66 67 68 69 70 **71** 72 73 74 75 76

Formación y entrenamiento

- La falta de interés en la temática de seguridad
  - Cuando la gente entiende que es la Ingeniería Social y en que peligro están mientras están trabajando, van a aceptar el entrenamiento de seguridad como parte de la protección en lo que todos están trabajando.
    Se entiende que la seguridad es responsabilidad de *todos* los empleados de una empresa, no solo de *un* departamento.
  - La importancia de seguridad y las consecuencias si falla tienen que ser conocidos por todos los empleados. Es un desafió para un entrenador de un programa de seguridad llegar a este punto los más pronto posible porque después de entender esto, en todas las sesiones del programa la gente va a participar con más atención.

9. Defensa contra la Ing. Soc. 10/30

66 67 68 69 70 71 **72** 73 74 75 76

Formación y entrenamiento

- La falta de interés en la temática de seguridad
  - El conocimiento solo no es suficiente.
    - El programa de entrenamiento tiene que animar a la gente a pensar por si misma en la materia porque la Ingeniería Social es dinámica y solo con políticas estáticas no se puede garantizar la mejor protección (la protección absoluta no existe).
  - Cuanto más personas piensen por si mismos en esto, menos éxito tendrá un Ingeniero Social al intentar atacar a una empresa donde la gente esta preparada.

9. Defensa contra la Ing. Soc. 11/30

Formación y entrenamiento

- Partes de un programa de entrenamiento de concienciación
  - Politicas de seguridad
    - El entrenamiento se basa en unas políticas de seguridad de la empresa.
    - Es imposible predecir todas las situaciones con las que un empleado se puede enfrentar. Es necesario que durante el entrenamiento las personan desarrollen un propio sentido de concienciación (basado en el entrenamiento) para estar preparadas para las dinámicas situaciones a que se pueden enfrentar en futuro.
  - ¿Que se tiene que proteger?
    - Una de las primeras cosas que un empleado tiene que reconocer es *que* es lo que tiene que proteger. En otras palabras, tiene que entender el valor de la información.

9. Defensa contra la Ing. Soc. 12/30

Formación y entrenamiento

- Partes de un programa de entrenamiento de concienciación
  - ¿Quién es el atacante y de que manera ataca?
    - Es importante saber quien es el atacante, un Ingeniero Social, y como se presentara (amable, confiable etc.).
    - Se tiene que reconocer los métodos usados en los ataques de Ingeniería Social.
      Los empleados tienen que ser conscientes de que, como son humanos, tienen vulnerabilidades que un Ingeniero Social conoce e intenta a explotar.
      Esto se puede enseñar usando juegos de roles.

9. Defensa contra la Ing. Soc. 13/30

66 67 68 69 70 71 72 73 74 75 76

Formación y entrenamiento

- Partes de un programa de entrenamiento de concienciación
  - Verificaciones
    - Ingenieros Sociales intentan que otras personas crean que ellos tienen derechos para acceder a cierta información o dar a las personas instrucciones para comenzar unas acciones (por ejemplo bajar e instalar un programa).
    - Para evitar esto, los empleados tienen que preguntarse las siguientes 3 cosas, en cualquier situación:
      1. ¿Es la persona sospechosa en realidad quien dice que es?
      2. ¿Es la persona sospechosa un empleado o alguien quien tiene una relación con la empresa que le da el derecho para acceder a información?
      3. ¿Esta la persona sospechosa autorizada a acceder a la información o comenzar una acción?

9. Defensa contra la Ing. Soc. 14/30

66 67 68 69 70 71 72 73 74 75 76

Formación y entrenamiento

- Partes de un programa de entrenamiento de concienciación
  - Verificaciones
    - Todas clases de información, verbal, en documento, E-mail, fichero o disco tienen que pasar estos 3 puntos de verificación antes que se transmitan.
      Si hay dudas, siempre se debe contactar al supervisor de un departamento o el departamento de seguridad, donde los especialistas entrenados pueden encargarse del caso.
    - Muchas personas dudarán en preguntar a una persona con autoridad por verificación para el acceso de datos, pero siempre se tiene que recordar que un Ingeniero Social va a intentar explotar esto cuando se le da una posibilidad.
    - Y si las personas con autoridad han entendido el valor de información, no hay razón para sentirse ofendido cuando se les pide verificación para acceder a unos datos. Todo el contrario, esto solo significa que un programa de seguridad funciona en la vida real.

9. Defensa contra la Ing. Soc. 15/30

Formación y entrenamiento

- Partes de un programa de entrenamiento de concienciación
  - Continuando con la concienciación
    - La mayoría de la gente olvida algo que han aprendido si no se enfrentan con la materia por mucho tiempo. Como la protección contra Ingeniería Social es tan importante, esto no es aceptable.
    - Se requiere un buen diseño para un programa de entrenamiento de concienciación continuando. Por un lado la gente tiene que acordarse de los aspectos de seguridad enseñados durante el entrenamiento, por otro lado la gente no debe pensar en esto como algo desagradable, aburrido y no debe sentirse demasiado controlado.

9. Defensa contra la Ing. Soc. 16/30

Formación y entrenamiento

- Partes de un programa de entrenamiento de concienciación
  - Continuando con la concienciación
    - Medidas para suportar el programa:
      - Meter artículos sobre temáticas de seguridad en el Newsletter de la empresa como en la Intranet
      - Ofrecer información adicional sobre seguridad para empleados interesados y recordar esto sobre E-mail y anuncios en áreas de los empleados.
      - Usar screensavers con mensajes relacionados con seguridad
      - Poner stickers en los teléfonos de los empleados, en los que dice “¿Es la persona que te llama en verdad quien dice que es?”
      - Configurar los programas E-mail para que todo el trafico sobre E-mail esté cifrado y usar firmas digitales.
      - Incluir concienciación de seguridad como una parte estándar en los informes sobre la capacidad de trabajo de los empleados y la empresa en general.
      - Ofrecer pequeños regalos relacionados con seguridad, por ejemplo galletas de suerte que contienen un recuerdo de seguridad en lugar de un dicho

9. Defensa contra la Ing. Soc. 17/30

77
78
79
80
81
82
83
84
85
86
87

Formación y entrenamiento

- Partes de un programa de entrenamiento de concienciación
  - Programa de premios
    - Muchas personas trabajan más duro si se puede ganar un premio. Un diseñador de un programa de entrenamiento de seguridad puede usar este principio para mejorar la seguridad en una empresa.
    - Se puede hacer público si un empleado ha tenido éxito en defender la empresa contra un ataque o si ha hecho una buen sugerencia para mejorar la seguridad de la misma.
    - Por supuesto los empleados también tienen que saber sobre las consecuencias si fallan con las políticas de seguridad. Aunque fallar es algo que puede pasar a cualquier persona, continuos fallos de una persona son un peligro para la seguridad de una empresa y no se pueden aceptar.

9. Defensa contra la Ing. Soc. 18/30

77
78
79
80
81
82
83
84
85
86
87

Formación y entrenamiento

- Partes de un programa de entrenamiento de concienciación
  - Trucos para el diseño de contraseñas seguras y recordables
    - Hay letras que se ven un poco como números, así que dentro de una contraseña se pueden sustituir.
      1 se ve como l
      0 se ve como O
      $ y 5 se ven como S
      8 se ve como B
      3 se ve como una E, pero del otro lado
    - Existen palabras que suenan como un número o un solo carácter (en Inglés), así que otra vez podemos sustituir.
      4 suena como “for”
      2 suena como “to” o “too”
      b suena como “be”
      u suena como “you”

9. Defensa contra la Ing. Soc. 19/30

Formación y entrenamiento

- Partes de un programa de entrenamiento de concienciación
  - Trucos para el diseño de contraseñas seguras y recordables
    - Usando estos trucos es fácil crear una contraseña como las siguientes:

      j0hn1ik3$app135 suena como “john likes apples”
      ub2$w33t4m3 suena como “you be too sweet for me

    - Por supuesto un ataque de manera brute force podría crackear estas contraseñas, pero tardara más tiempo y los ataques basados en el uso de diccionarios no tendrán éxito.

    - Sin embargo, la mejor contraseña no sirve para nada si no la tratamos como un secreto.
      Ni se debe contar a nadie ni escribir en un papelito. Esto es uno de los fallos más cometidos por los usarios. Esto debe estar prohibido porque el riesgo de que alguien encuentre el papel es inaceptable.

9. Defensa contra la Ing. Soc. 20/30

Formación y entrenamiento

- Partes de un programa de entrenamiento de concienciación
  - Trucos para el diseño de contraseñas seguras y recordables
    - Es bastante importante no usar una contraseña para más que una cuenta de usario.

    - Las contraseñas solo se deben reusar después de por lo menos 8 meses. Un Ingeniero Social puede descubrir que una victima está usando las mismas contraseñas en un ciclo periódico (por ejemplo porque el sistema operativo le obliga).

    - Donde se puede poner una contraseña, se debe poner.

    - Contraseña por defecto se tienen que cambiar en todos los equipos (en Internet existen listas de contraseñas por defecto, listados por fabricante).

9. Defensa contra la Ing. Soc. 21/30

77 78 79 80 81 82 **83** 84 85 86 87

Medidas organizatorias y de gestión

- La creación de políticas y programas de formación se pueden hacer dentro de una empresa o dejarse a una empresa especializada. Ambas posibilidades tienen ventajas y desventajas.
- Se tienen que nombrar personas responsables para la creación de policitas y programas de formación.
  Cuantas, depende de la magnitud de la empresa, pero por lo menos dos personas dentro del departamento de seguridad tendrán que tener suficiente conocimiento sobre Ingeniería Social para cargarse con estas tareas.
- Dependiendo de si una empresa ha elegido a cargar a otra con la responsabilidad de la creación de defensas contra Ingeniería Social pueden existir más personas, trabajando como consejeros para la primera empresa.

9. Defensa contra la Ing. Soc. 22/30

77 78 79 80 81 82 83 **84** 85 86 87

Medidas organizatorias y de gestión

- Las Políticas de seguridad son reglas estáticas en que todo la formación de seguridad se basa. Cada empleado atendiendo a un programa de formación de seguridad tiene que firmar que lo ha entendido y que no va a violar las políticas. Los empleados también tienen que saber las consecuencias de este caso.

- Recomendaciones para la creación de políticas de seguridad contra Ingeniería Social:
  - Adivinar los riesgos: Antes de la creación de políticas
    1. ¿Cuál es la información que se debe proteger (aunque ya sabemos que en general toda la información se debe tratar como delicada, porque *es* así) y con que prioridades?
    2. ¿Cuáles son los peligros específicos?
    3. ¿Cómo serán los daños en caso de que la compañía sufra a un ataque?

9. Defensa contra la Ing. Soc. 23/30

77 78 79 80 81 82 83 84 **85** 86 87

Medidas organizatorias y de gestión

- Recomendaciones para la creación de politicas de seguridad contra Ingeniería Social:
  - El cambio entre seguridad y disponibilidad
    - Aumentar el nivel de seguridad de un sistema puede ponerse en conflicto con el desarrollo de procesos de trabajo.
    - Reducir el nivel de seguridad puede mejorar el desarrollo de procesos de trabajo, pero con la desventaja de menos seguridad en ellos.
  - Soportar seguridad, ya desde arriba
    - Las políticas de seguridad tienen que estar apoyadas por la dirección de una empresa para que esto sea un ejemplo para los demás.
    - Empezando con el pico de una empresa, todos tienen que demostrar que han entendido porque la seguridad es tan importante para la empresa.
      Estos ejemplos animan a los demás a cumplir con las políticas.

9. Defensa contra la Ing. Soc. 24/30

77 78 79 80 81 82 83 84 85 **86** 87

Medidas organizatorias y de gestión

- Recomendaciones para la creación de politicas de seguridad contra Ingeniería Social:
  - Comprensibilidad
    - El autor de unas políticas de seguridad tiene que escribirlas de una manera que no contengan demasiada jerga para que también gente con menos conocimiento las entienda fácilmente.
      Cada documento tiene que declarar de una manera muy clara porque su contenido es tan importante y se tiene que obedecer.
    - Si no, unos empleados podrían considerar leerlo un tiempo perdido.
  - Políticas y procesos de seguridad
    - Las políticas y procesos de seguridad se deben poner en diferentes documentos porque las políticas no se cambian tan fácilmente como los procesos que están basados en ellas.

9. Defensa contra la Ing. Soc. 25/30

77 78 79 80 81 82 83 84 85 86 87

Medidas organizatorias y de gestión

- Recomendaciones para la creación de políticas de seguridad contra Ingeniería Social:
  - Reducir decisiones humanas
    - En algunos sitios tiene sentido minimizar las decisiones humanas para reducir el peligro de ataques de Ingeniería Social.
    - El autor de unas políticas de seguridad contra Ingeniería Social tiene que saber las posibilidades técnicas para conseguir esto.
  - Procesos de actualización
    - Es necesario darles una mirada retrospectiva a las políticas para saber si todavía son actuales o si se tienen que actualizar. Esto se debe hacer periódicamente, pero por lo menos cada 6 meses.

9. Defensa contra la Ing. Soc. 26/30

88 89 90 91 92 93 94 95 96 97 98

Medidas organizatorias y de gestión

- Recomendaciones para la creación de políticas de seguridad contra Ingeniería Social:
  - Pruebas
    - Las “Penetration tests” usando también métodos de Ingeniería Social se deben hacer periódicamente para encontrar vulnerabilidades y medidas contra una explotación.
    - Los Empleados con la responsabilidad de hacer decisiones que pueden afectan a toda la empresa deben ser informados antes de hacer una de estas pruebas de seguridad.

9. Defensa contra la Ing. Soc. 27/30

Medidas organizatorias y de gestión

- Recomendaciones para la creación de políticas de seguridad contra Ingeniería Social:
  - Clasificación de datos
    - Saber el valor de la información es importante, pero para protegerla es necesario clasificarla.
    - Sín clasificacion será la decisión de individuos, clasificar lo importante o sensitivos que son unos datos.
      Dependiendo de la sensitividad real puede resultar en un desastre si unos datos se clasifican mal por una persona. Por esto es mejor crear categorías generales y dejar muy claro de que categoría son unos datos.

9. Defensa contra la . Soc. 28/30

Medidas organizatorias y de gestión

- Recomendaciones para la creación de políticas de seguridad contra Ingeniería Social:
  - Carné de identifación
    - Cada persona dentro de una empresa esta obligado a llevar un carné de identifación de manera que se vea desde lejos. Este carné debe tener el nombre del empleado y una foto.
    - Se deben usar carnés con diferentes colores para diferentes grupos de gente dentro de una empresa (empleado, Temp, visitante etc.).
    - Personas que no llevan un carné se deben cuestionar inmediatamente, sin sentirse ofendido porque solo se aplican las políticas de seguridad.

9. Defensa contra la Ing. Soc. 29/30

Medidas organizatorias y de gestión

- Recomendaciones para la creación de políticas de seguridad contra Ingeniería Social:
  - Basura
    - A veces Ingenieros Sociales buscan en la basura información que se puede usar para el desarrollo de un ataque (esto se llama “dumpster diving”).
    - Para evitar esto, existen medios para destruir soportes de información de forma no recuperable.
      El papel se tiene que desgarrar, los discos tienen que guardarse en un sitio seguro para ser destruido después.

9. Defensa contra la Ing. Soc. 30/30

Medidas organizatorias y de gestión

- Recomendaciones para la creación de políticas de seguridad contra Ingeniería Social:
  - Derechos de acceso en un caso de cambio de posición o responsabilidad
    - Cada posición dentro de una empresa tiene sus responsabilidades y sus derechos. Si una persona cambia de posición, se tienen que comprobar que los derechos asociados con esta posición también cambian.
    - En general la política de “least privilege” o privilegios minimos, se debe usar.
    - Si un cambio de posición significa que a una persona le quitan unos derechos entonces esto se tiene que reflejar para evitar abusos.
    - En casos en que necesiten derechos adicionales, se pueden agregar a la base de una política correspondiente.
    - Si una posición dentro de una empresa se cierra porque un empleado se marcha de la empresa, muere etc., es importante cerrar o desactivar su cuenta inmediatamente para evitar el abuso de ella.

10. Conclusión 1/4

- Los ataques de Ingeniería Social son tan populares y tienen tanto éxito porque todavía hay mucha gente que no cree lo que un buen Ingeniero Social es capaz de hacer.

- La Ingeniería Social es una manera de atacar una compañía que se tiene que tomar en serio porque no se dirige contra equipos, sino las personas que las están operando.
  La manera de pensar de la gente es algo que un Ingeniero Social sabe usar para sacar información durante una conversación sencilla, preguntando por la información deseada escondida dentro del resto de las preguntas normales.

10. Conclusión 2/4

- Seguridad es una necesidad para proteger los recursos de la empresa. Puede ser mucho trabajo convencer a la gente de esto y de que no es algo desagradable que se tiene que evitar.

- Esto es un problema de seguridad en general, pero con Ingeniería Social es particularmente difícil porque hay poca gente que entiende que es contra lo que se tienen que defender cuando se enfrentan a un ataque de Ingeniería Social.
  Muchas veces se menosprecia el peligro y se pregunta como es posible que haya victimas de Ingenieros Sociales.

10. Conclusión 3/4

- Hablando y contando historias, ellos aparecen muy amables e inocentes, pero usando técnicas como name-dropping o usando autoridad o amenazas saben crear un escenario de presión para una victima en el que ella no sabe que hacer hasta que al fin dar al Ingeniero Social la información que el desea. Estos son más que historias, esto pasa cada día en diferentes lugares del mundo.

- Lo que falta para defenderse con éxito contra esta manera de ataques es educación. Los programas de formación bien diseñados y entrenamiento pueden cambiar el punto de vista de gente sobre la seguridad y, en particular, Ingeniería Social.

10. Conclusión 4/4

- Si queremos defendernos contra un atacante, tenemos que aprender sobre *todos* los aspectos y maneras con que nos pueden atacar.

  En particular cuando una manera se practica con tanto éxito y contra los eslabones más débiles de una cadena se seguridad:

  Nosotros.

Gracias por su atención.