Cyber MSME

Ciberseguridad para las micro, pequeñas y medianas empresas

Ingeniería Social – los usuarios son el vínculo más débil

Por CTS Customized Training Solutions & CASE

Erasmus+

Objetivos y metas

Al final de este modulo serás capaz de:

- definir la ingeniería social
- reconocer y distinguir las técnicas de ingeniería social más utilizadas
- entender los mecanismos manipuladores utilizados por el atacador
- establecer posibles fuentes de ataques
- analizar el riesgo de los ataques de ingeniería social en tu empresa.

Índice

Unidad 1: **¿Qué es la ingeniería social?**

Sección 1.1: Definición
- ¿Estás a salvo?
- El vínculo más débil

Sección 1.2: ¿Qué son los ataques de ingeniería social?
- ¿Qué tipos de datos pueden considerarse confidenciales?

Sección 1.3: Los principios de los ataques de ingeniería social
- ¿Qué pasa durante el ataque?

Sección 1.4: ¿Quién puede convertirse en victima?

Unidad 2: **Técnicas de ingeniería social**

Sección 2.1: Mensaje de un amigo
- ¿Por qué John lo hizo?
- ¿Cuándo puedes ser atacado con esta técnica?

Sección 2.2: Phishing
- ¿El escenario cómo debería parecer?

Sección 2.3: Vishing
- ¿El escenario cómo debería parecer?
- ¿Cuándo puedes ser atacado con esta técnica?

Sección 2.4: Hostigamiento
- ¿El escenario cómo debería parecer?

Sección 2.5: Resumen

Unidad 3: **Prevención de la ingeniería social**

Sección 3.1: Pros y contras

Erasmus+

Unidad 1: ¿Qué es la ingeniería social?

Sección 1.1: Definición

La ingeniería social en el contexto de TI es un término utilizado por varias actividades dolosas creadas por las interacciones humanas. Se basa en la manipulación psicológica. El punto es empujar al usuario para que cometa un error de seguridad. En otras palabras, el ataque de ingeniería social es posible solo si el usuario no es consciente de la intención prejudicial.

¿Estás a salvo?

Los ataques de ingeniería social pueden golpearte en cualquier momento, no importa lo grande o pequeña que sea el negocio que hayas construido.

El vinculo más débil

El vínculo más débil en todo el proceso es el usuario: tú, tus empleados, tus socios comerciales. Para minimizar el riesgo necesitas maximizar la sensibilización.

¿Cómo hacerlo?

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unidad 1: ¿Qué es la ingeniería social?

Sección 1.2: ¿Qué son los ataques de ingeniería social?

Entender los ataques de ingeniería social es el primer paso para aumentar tu sensibilización y la de tus empleados. Primero que todo, necesitas recordar que los cibercriminales y los estafadores organizan estos ataques. Sin embargo, no se trata siempre de dinero. Cualquier cantidad de información (como contraseñas) o **datos confidenciales** son bastante para fraudar.

¿Qué tipo de datos se consideran confidenciales?

- Datos personales que revelan las orígenes raciales o étnicas, opiniones políticas, creencia religiosa o filosófica
- Afiliación sindical
- Datos genéticos, datos biométricos procesados únicamente para identificar a un ser humano
- Datos relacionados con la salud
- Datos relacionados con la vida sexual o la orientación sexual de una persona*

*Fuente: Comisión europea> ¿Qué datos personales se consideran confidenciales?

Unidad 1: ¿Qué es la ingeniería social?

Sección 1.3: Principios de los ataques de ingeniería social

Normalmente, un ataque de ingeniería social tiene **3 pasos**...

Paso 1: el atacante se dirige a una victima

- Identificar a las victimas
- Investigación de base
- Elección de métodos de ataque

Paso 2: el atacante gana la confianza de la victima

- Involucrar a la victima en una historia
- Tomar las riendas de la interacción
- Ganar terreno

Paso 3: el atacante consigue el objetivo, robando los datos o rompiendo las prácticas de seguridad

- Efectuar los ataques
- Borrar las huellas
- Desaparecer

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unidad 1: ¿Qué es la ingeniería social?

Sección 1.3: Los principios de los ataques de ingeniería social

En el ataque de ingeniería social, el atacador utiliza la manipulación psicológica. Por esa razón es incluso más peligroso que un ataque cibernético a tu sistema. ¿Por qué? Porque necesitas estar seguro que tú y tus empleados podáis discernir entre la manipulación y los anuncios estándares. No es fácil, porque somos sólo humanos.

¿Qué pasa durante el ataque?

El atacamte juega con las debilidades de la victima. Entonces, pensamos en los ataques de ingeniería social como en un juego sucio, donde solo una persona conoce las reglas, además, ¡a veces también las crea!

Como cada juego, esto tiene también algunos mecanismos generales que podrían aumentar las probabilidades de ganar.

La mayoría de los ataques de ingeniería social se basan en 5 principios: **autoridad, prueba social, escasez, urgencia, familiaridad.**

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unidad 1: ¿Qué es la ingeniería social?

Sección 1.3: Los principios de los ataques de ingeniería social

autoridad :
El atacante se presenta como una figura autoritaria

escasez :
El atacante utiliza el mecanismo que la victima perderá si ellos no hacen nada

familiaridad :
El atacante convence a la victima para que ejecute operaciones específicas para ganar su confianza

prueba social:
El atacante usa la presión social para forzar a la victima para que realice una acción

urgencia :
El atacante usa la idea que la victima perderá si ellos no hacen nada lo antes posible

Erasmus+

Unidad 1: ¿Qué es la ingeniería social?

Sección 1.4: ¿Quién puede convertirse en victima?

Has conocido los 5 principios de los ataques de ingeniería social. Estos principios están conectados con los conductores psicológicos y la motivación de las personas. Estos, por supuesto, están creados en lo profundo de nuestro subconsciente.

Robert Cialdini, uno psicólogo, ponente y autor del libro intitulado "Influencia: ciencia y práctica" describió cómo las personas pueden ser influenciadas por los demás. De acuerdo con Cialdini, los factores clave son:

Reciprocidad

En general, las personas se sienten obligadas a recompensar después de recibir ayuda. Esta característica parece ser tan natural para todas las culturas en las cuales no nos sentimos incomodos cuando alguien nos pide que le devolvamos el favor.

Cialdini mencionó que los llamados profesionales de cumplimiento a menudo ofrecen un pequeño regalo a los potenciales clientes para jugar con este rasgo.

Los estudios demuestran que incluso un regalo no deseado influenciará al destinatario a la reciprocidad.

Unidad 1: ¿Qué es la ingeniería social?

Sección 1.4: ¿Quién puede convertirse en victima?

Compromiso y coherencia

A menudo las personas siguen sus hábitos y las primeras elecciones. Quieren parecer coherentes con su conducta. Aprecian también la coherencia de los demás.

Cialdini mencionó que está conectado también con el fuerte deseo que la gente tiene de cumplir compromisos, para proporcionar justificaciones adicionales y razones para suportarlos.

Prueba social

Ya hemos dicho que el mecanismo habla de los principios de los ataques de ingeniería social. La prueba social significa que las personas confían en personas similares a ellos al tomar decisiones. Es más obvio en situaciones ambiguas o inciertas.

Cialdini dijo que los llamados profesionales de cumplimiento proporcionan información falsa sobre los otros que están jugando con este rasgo. Por ejemplo, preparan entrevistas organizadas, datos falsos o casos de estudio.

Unidad 1: ¿Qué es la ingeniería social?

Sección 1.4: ¿Quién puede convertirse en victima?

Gusto

Bueno, no es un secreto — las personas necesitan que les guste. Como consecuencia de jugar con este rasgo, es más probable que las personas estén de acuerdo con las ofertas de las personas que les gustan.

Cialdini mencionó que agradar a las personas puede manifestarse en muchas maneras, por ejemplo, puede ser una atracción física o tendiendo a una persona similar.

Autoridad

Probablemente es el factor de influencia más peligrosos, dar al atacante el mayor poder. Generalmente, las personas siguen a los que parecen ser más fuertes, mejores, seguros de si mismos para ellos; que tienen algo que ellos no tienen. Los estudios enseñan que las personas suelen reaccionar de modo automático a las instrucciones de la autoridad e incluso a los símbolos de autoridad (como coches caros, uniformes, diplomas, títulos académicos, etc.). Que pasa incluso cuando el instinto sugiere que las instrucciones deberían ser rechazadas.

Erasmus+

Unidad 1: ¿Qué es la ingeniería social?

Sección 1.4: ¿Quién puede convertirse en victima?

Escasez

Nuevamente, hemos mencionado que el mecanismo habla de los principios de los ataques de ingeniería social. La escasez se basa en el deseo que la gente tiene de poseer las cosas menos disponibles. Menor disponibilidad puede ser exclusiva o limitada en el tiempo. Este rasgo ayuda, por ejemplo, a los anunciantes a promocionar bienes como “disponibilidad limitada", o “solo por poco tiempo".

Entonces, ¿quién puede convertirse en una victima de los ataques de ingeniería social?

En general — cualquiera. Sin embargo, los antecedentes psicológicos de una persona y la condición actual importan.

Recuerda siempre que la ingeniería social se basa en la manipulación.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unidad 2: Técnicas de ingeniería social

Sección 2.1: Mensaje de un amigo

Imagina que estás trabajando, escribiendo algunos informes en Excel en la nube de tu empresa, y al mismo tiempo, le echas un vistazo a tus redes sociales. Entonces, en un browser tienes abiertos los dos, Excel y Facebook.

Estás llenando estos gráficos aburridos y, de repente, tu mejor amigo (llamémoslo John) te escribe en Messenger. John te escribió que tus fotos desnudo están disponibles en la página web en adjunto — y te envió el enlace. Clicas en el enlace y...

Probablemente solo perdiste el acceso a tu cuenta de Facebook y/o también a tu página de negocio. A lo mejor has comprometido también algunos datos almacenados en tu ordenador.

¿Por qué John te hizo esto?

Bueno, seamos honestos. **No fue john...**

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unidad 2: Técnicas de ingeniería social

Sección 2.1: Mensaje de un amigo

Probablemente era un robot creado con datos robados. Tu amigo John fue una victima como tú. El atacante utilizó su identidad (en este caso, la cuenta de las redes sociales) para ganar tu confianza. Después de todo, conoces bien a John, habéis crecido juntos, y sois mejores amigos. ¿Cómo podía saberlo el atacante?

A lo mejor tenéis muchas fotos juntos, habláis mucho por Messenger o puede que fuera una coincidencia — pero funcionó. Ahora eres la siguiente victima en la larga cadena llamada phishing (fraude electrónico).

¿Cuándo puedes ser atacado mediante esta técnica?

Utilizando redes sociales, mensajería instantánea, chats, correos, SMS, etc.

Unidad 2: Técnicas de ingeniería social

Sección 2.2: Phishing

Hoy en día, la técnica más popular de ingeniería social es el phishing. El phishing es cualquier tipo de campaña de mensajes planeado para redirigir la victima a un formulario, página web o pedido específico. El atacante falsifica una fuente de confianza (por ejemplo, amigo, banco, agencia de seguro, fondos de inversión) y prepara un escenario razonable. El fuerte tema emocional suele ayudar a mitigar la incredulidad.

¿Cómo puede parecer el escenario?

Como pedir urgentemente tu ayuda

Tu “amigo" se quedó atascado en el extranjero, le robaron, le dieron una paliza y está en el hospital. Necesita dinero e indicarte como hacerle una trasferencia.

O

Tu “amigo" vio tus fotos desnudo en internet y te envió un enlace.

Erasmus+

Unidad 2: Técnicas de ingeniería social

Sección 2.2: Phishing

Como acciones con antecedentes aparentemente legítimos

Tu “banco" te envió un SMS con un enlace, donde te pedía la confirmación de balance.

O

Tu “proveedor de hosting" te envió un correo afirmando que su almacenamiento de datos fue hackeado, y necesitas contactar con ellos por el formulario adjunto.

Como pedir una donación de fondos para caridad, etc.

Alguna figura de autoridad te pidió ayuda para reparar los efectos de un terrible desastre natural, campaña política o caridad.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unidad 2: Técnicas de ingeniería social

Sección 2.3: Vishing

El vishing es una variante del phishing hecha utilizando la tecnología vocal, como llamada telefónica, llamada de Messenger/ Zoom, o mensaje vocal fraudulento. Los mecanismos de manipulación son los mismos que los vocales en el phishing, pero el atacante utiliza mensajes de voz o llamadas urgentes para convencer la victima a dar el paso.

¿Cómo puede parecer el escenario?

Enorme peligro

Después de la información del atacante sobre el enorme peligro, como el hackeo de una cuenta bancaria o de unos impuestos no pagados, la victima siente la presión de actuar rápidamente. Atrapado por el momento, la victima comparte sus datos confidenciales y las contraseñas durante la llamada.

Unidad 2: Técnicas de ingeniería social

Sección 2.3: Vishing

¿Cuándo puedes ser atacado por esta técnica?

Cuando tienes un perfil/página web público de tu empresa con tu número de teléfono (no solo los tuyos, sino también los de tus empleados), cuando compartes tu número de teléfono en las redes sociales, o cuando utilizas mensajes instantáneos y aplicaciones con opciones de llamada vocal, etc...

Sección 2.4: Hostigamiento

A veces en vez de peligro, hay una gran oportunidad. Tú eres el ganador, el afortunado, puedes invertir pequeñas cantidades de dinero y en poco tiempo ¡convertirlo en una fortuna! Es bueno recordar que los atacadores utilizan a menudo el hostigamiento con el pretexto de varios fondos europeos. Puedes ser atacado por formularios online, llamadas telefónicas, o incluso en personas.

Erasmus+

Unidad 2: Técnicas de ingeniería social

Sección 2.4: Hostigamiento

¿Cómo puede parecer el escenario?

Hay algo que quieres

El atacante elige algo que las personas desean, por ejemplo, descargar una nueva película. Mucha gente cae en la trampa por encontrar algo que quiere.

¡Gran oferta!

El atacador puede crear un anuncio informando sobre una muy buena oferta en sitios de ofertas clasificados, sitios de subastas, etc. Normalmente, el atacador abre una cuenta de vendedor con una buena calificación para minimizar tu subscripción.

Si la victima cae en la trampa puede ser infectada por un software dañino. Eso suele generar acciones contra la victima y sus contactos.

Unidad 2: Técnicas de ingeniería social

Sección 2.5: Resumen

Todos los escenarios mencionados son solo ejemplos de técnicas de ingeniería social. Recuerda que el atacante es listo, es una persona orientada a la tecnología que ha explorado técnicas manipuladoras.

Phishing, vishing, y hostigamiento tiene infinitos escenarios. Todos dependen del ingenio y de la creatividad del atacante.

Consulta las novedades regularmente para conocer las técnicas actuales de ingeniería social para mantenerte al día.

Erasmus+

Unidad 3: Prevención de ingeniería social

Sección 3.1: Pros y contras

Como puedes ver, las técnicas de ingeniería social son eficaces y poderosas, debido a la manipulación psicológica, falta de sensibilización y conocimiento propio. Todo el ataque puede ocurrir si la victima está propensa a elegir los mecanismos.

Entonces, ¿ qué puedes hacer para prevenir los ataques de ingeniería social?

Aumentar la sensibilización de las actividades peligrosas entre tú, tus empleados, los socios y los clientes. Recuerda que las técnicas de ingeniería social cambian a través del tiempo y del espacio, entonces es necesario actualizar tu conocimiento regularmente.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unidad 3: Prevención de ingeniería social

Sección 3.1: Pros y contras

Enseña a tus empleados, socios, y clientes lo valioso que son las contraseñas y los datos confidenciales. Recuerda que un post divertido en Facebook, donde te preguntan tu fecha de nacimiento, puede ser utilizado en tu contra. Piensa cuántas veces utilizaste tu fecha de nacimiento en una contraseña...

No guardes todos los datos y la información crucial en un mismo lugar. Si el atacante es capaz de robarlos con una captura de pantalla, debes trabajar en tu sistema de seguridad.

No cliques en ningún enlace e imagen que recibes antes de comprobar la fuente.
Incluso si la fuente parece similar, no confíes.
Echa otro vistazo al correo, IP, enlace, etc.

Unidad 3: Prevención de ingeniería social

Sección 3.1: Pros y contras

Prepara claras normas de seguridad para tu empresa. Planea el protocolo en caso de ataque y forma a tus empleados, socios y clientes sobre lo que hay que hacer.

No causes miedos innecesarios entre tus empleados, socios y clientes. El miedo ayuda al atacador a manipular la gente. La sensibilización y el conocimiento son lo contrario.

¿Estás listo para enfrentarte a las técnicas de ingeniería social?

Bibliografía y enlaces relevantes

European Commission > What personal data is considered sensitive

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

Webroot > What is Social Engineering? **Examples & Prevention Tips**

https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

Seon > **What is Social Engineering? Attacks, Techniques & Prevention**

https://seon.io/resources/protect-against-social-engineering-attacks/?utm_term=&utm_campaign=%5BS%5D%20Blog%20-%20dynamic%20%5BEMEA%5D&utm_source=google&utm_medium=cpc&hsa_acc=9367189488&hsa_cam=12655034312&hsa_grp=119030291966&hsa_ad=511148698722&hsa_src=g&hsa_tgt=dsa-41475539813&hsa_kw=&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAjwvuGJBhB1EiwACU1AibG5GowOFa1Q_FazH8_RDbrb3OEI7k7fQacOcLKrty9ZFQw-b7i_7hoCDWcQAvD_BwE

Imperva > **Social Engineering**

https://www.imperva.com/learn/application-security/social-engineering-attack/

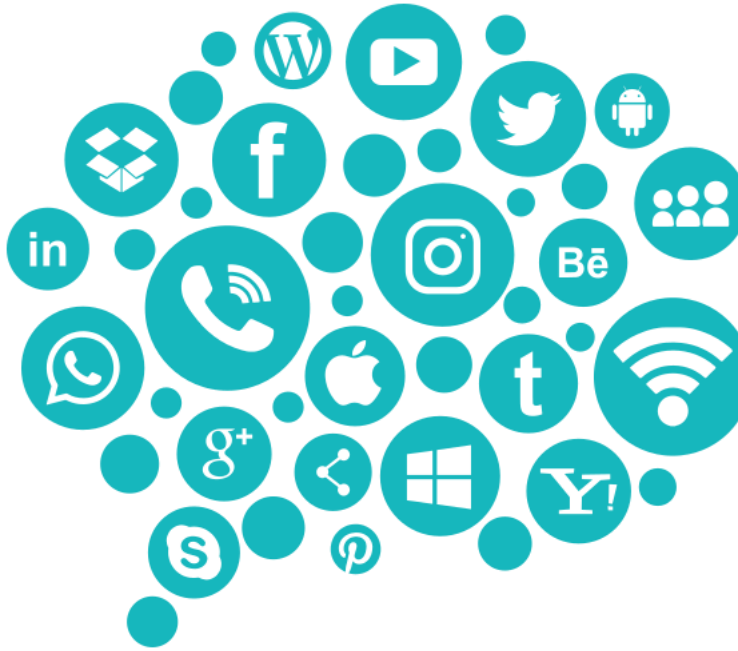
Verizon > Data Breach Investigations Report > **2021 DBIR Master's Guide**

https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

Terranova Security > **9 Examples of Social Engineering Attacks**

https://terranovasecurity.com/examples-of-social-engineering-attacks/

¡Gracias por tu atención!



The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.