Universidad de Buenos Aires
Facultad de Ciencias Económicas

La Ingeniería Social

AR Tema extractado del libro "**Análisis Funcional de Sistemas y Tecnologías de la Información**" de Aníbal M. Mazza Fraquelli - ISBN 978-987-26981-3-3

Presentación del Tema

La **ingeniería social (Social Engineering)** constituye una de las amenazas más sofisticadas y efectivas en el ámbito de la seguridad de los Sistemas de Información (SI – *Information Systems*). A diferencia de los ataques puramente técnicos, la ingeniería social explota el factor humano como vector principal de vulnerabilidad. En lugar de vulnerar directamente sistemas tecnológicos, el atacante manipula psicológicamente a las personas para que revelen información, otorguen accesos o realicen acciones que comprometen la seguridad organizacional.

En la era digital, la exposición de datos personales en redes sociales, bases públicas, filtraciones masivas y plataformas profesionales incrementa significativamente la superficie de ataque. La información que "los demás saben de nosotros" —hábitos, cargos laborales, relaciones personales, rutinas, preferencias, datos académicos— se convierte en insumo para ataques dirigidos y altamente personalizados.

Desde la perspectiva de la administración y la gobernanza tecnológica, comprender la ingeniería social no es un asunto exclusivo de ciberseguridad técnica, sino una cuestión estratégica vinculada a la cultura organizacional, la gestión del riesgo y la protección de activos informacionales.

Desarrollo

1. Concepto de Ingeniería Social

La ingeniería social puede definirse como el conjunto de técnicas de manipulación psicológica utilizadas para inducir a una persona a revelar información confidencial, ejecutar acciones indebidas o vulnerar controles de seguridad.

A diferencia del hacking técnico tradicional, la ingeniería social no requiere necesariamente conocimientos avanzados de programación o explotación de vulnerabilidades tecnológicas. Se basa en:

- Confianza.
- Autoridad.
- Urgencia.
- Empatía.
- Miedo.
- Curiosidad.

El atacante aprovecha sesgos cognitivos y dinámicas sociales para superar barreras de seguridad.

---

2. Principales Técnicas de Ingeniería Social

2.1 Phishing

El **phishing** consiste en el envío de mensajes fraudulentos que simulan provenir de entidades legítimas para obtener credenciales o información sensible.

Variante avanzada:

- **Spear Phishing**: ataque dirigido y personalizado.

Ejemplo organizacional:

Un empleado recibe un correo aparentemente enviado por el Director Financiero solicitando con urgencia una transferencia bancaria.

2.2 Vishing

Vishing (Voice Phishing / Phishing por voz) implica llamadas telefónicas fraudulentas.

Ejemplo:

Un supuesto técnico del área de TI solicita la contraseña para “resolver un problema urgente”.

2.3 Smishing

Smishing (SMS Phishing / Phishing por mensaje de texto) utiliza mensajes SMS con enlaces maliciosos.

2.4 Pretexting

Creación de una historia ficticia para obtener información.

Ejemplo:

El atacante se presenta como auditor externo y solicita acceso a documentación.

2.5 Baiting

Consiste en ofrecer algo atractivo (por ejemplo, un dispositivo USB encontrado) que al utilizarse instala malware.

---

3. La Información que los Demás Saben de Nosotros

En el entorno digital actual, gran parte de la información personal y profesional está disponible públicamente:

- Redes sociales.
- LinkedIn.
- Registros públicos.
- Filtraciones de bases de datos.
- Foros y publicaciones académicas.

Esta información permite construir perfiles detallados.

---

4. Perfilado del Objetivo

Los atacantes realizan lo que se denomina **OSINT (Open Source Intelligence / Inteligencia de Fuentes Abiertas)**, recopilando datos disponibles públicamente.

Ejemplos de información explotable:

- Cargo en la empresa.
- Proyectos en los que participa.
- Fechas de vacaciones.
- Eventos a los que asistió.
- Contactos frecuentes.

Con esta información, el atacante puede construir mensajes creíbles y personalizados.

---

5. Riesgo Organizacional

La ingeniería social afecta directamente los pilares del modelo **CIA (Confidentiality, Integrity, Availability / Confidencialidad, Integridad y Disponibilidad)**.

Puede derivar en:

- Robo de credenciales.
- Acceso no autorizado.
- Transferencias fraudulentas.
- Instalación de malware.
- Pérdida reputacional.

La debilidad humana puede anular controles tecnológicos robustos.

---

6. Factores Psicológicos Explotados

Los atacantes explotan:

- Autoridad (supuesto jefe).

- Escasez (oferta limitada).
- Urgencia (acción inmediata requerida).
- Familiaridad (uso de nombres reales).
- Miedo (amenaza de sanción).

Estos mecanismos activan respuestas impulsivas.

---

7. Ejemplo Integrado

Un atacante investiga en LinkedIn que un gerente financiero asistirá a una conferencia internacional.

Envía un correo al equipo contable simulando ser el gerente, desde una cuenta similar, solicitando con urgencia un pago.

La información pública permitió:

- Identificar ausencia del gerente.
- Usar tono y contexto creíble.

El ataque se apoya más en datos públicos que en vulnerabilidades técnicas.

---

8. Rol de la Cultura Organizacional

La ingeniería social no se combate únicamente con tecnología.

Se requiere:

- Capacitación periódica.
- Simulaciones de phishing.
- Protocolos claros de verificación.
- Cultura de reporte sin sanción.
- Doble validación en operaciones críticas.

---

9. Gestión de Identidad y Privacidad

La exposición excesiva de información aumenta riesgos.

Buenas prácticas:

- Limitar datos personales publicados.
- Configurar privacidad en redes.
- Evitar compartir información sensible en foros abiertos.
- Aplicar principio de mínima divulgación.

---

10. Dimensión Estratégica

Desde la administración:

- La ingeniería social es un riesgo transversal.
- Impacta finanzas, reputación y cumplimiento normativo.
- Requiere políticas formales y liderazgo visible.

El factor humano debe considerarse parte del sistema de control interno.

---

11. Integración con Gobernanza de TI

La gestión del riesgo de ingeniería social debe incluir:

- Controles preventivos (capacitación, MFA).
- Controles detectivos (monitoreo de actividad anómala).
- Controles correctivos (bloqueo inmediato y respuesta a incidentes).

La seguridad organizacional es socio-técnica, no exclusivamente tecnológica.

Conclusión

La ingeniería social representa una amenaza significativa para los sistemas de información, al explotar vulnerabilidades humanas en lugar de técnicas. En un entorno donde gran parte de nuestra información personal y profesional es accesible públicamente, la superficie de ataque se amplía considerablemente.

Desde la perspectiva administrativa, la mitigación de la ingeniería social requiere un enfoque integral que combine tecnología, políticas, capacitación y cultura organizacional. La información que otros conocen sobre nosotros puede ser utilizada para construir ataques altamente personalizados, por lo que la

gestión responsable de la identidad digital se convierte en una dimensión estratégica de la seguridad.

La protección de los sistemas de información no depende exclusivamente de firewalls y cifrado; depende también de la conciencia y comportamiento de las personas que interactúan con dichos sistemas.

Preguntas de autoevaluación

1. ¿Qué diferencia a la ingeniería social de un ataque puramente técnico?
2. ¿Qué es OSINT y cómo se relaciona con la ingeniería social?
3. ¿Qué factores psicológicos explotan los atacantes?
4. ¿Por qué la información publicada en redes sociales incrementa el riesgo organizacional?
5. ¿Qué medidas organizacionales pueden reducir la efectividad de la ingeniería social?

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.