

Claro. Revisé tu PPT completo: tiene **27 diapositivas** y el eje es *Ingeniería Social y Ciberseguridad en el Mundo Actual*, pasando por estadísticas, manipulación psicológica, phishing, contraseñas, herramientas OSINT, zero-days, panorama peruano, hacktivismo y una conclusión práctica.

Para que **no parezca una lectura de diapositivas**, te recomiendo exponerlas como una historia: **“el atacante no siempre necesita hackear una computadora; muchas veces necesita hackear a una persona”**.

GUION PARA TU SEMINARIO

DIAPPOSITIVA 1 — Presentación

En pantalla:

Ingeniería Social y Ciberseguridad en el Mundo Actual.

Lo que dices

“Buenas tardes a todos. Mi nombre es Héctor Reynaga, soy Ingeniero de Sistemas y especialista en Ciberseguridad.

Hoy no quiero darles una clase tradicional donde simplemente les voy a explicar qué es phishing, malware o contraseñas.

Quiero hacer algo diferente.

Quiero demostrarles que muchas veces el punto más débil de una organización no es el firewall, no es el antivirus y tampoco es el servidor.

Somos nosotros.

Y precisamente de eso vamos a hablar hoy: de cómo un atacante puede utilizar nuestra confianza, nuestra curiosidad, nuestro miedo o incluso nuestra ambición para conseguir acceso a información que aparentemente está protegida.”

Para sorprenderlos

Míralos y pregunta:

“¿Cuántos de ustedes creen que podrían reconocer un correo de phishing?”

Que levanten la mano.

Luego:

“Perfecto. Al final de esta charla voy a volver a hacerles la misma pregunta.”

DIAPPOSITIVA 2 — 600 millones de ciberataques al día

Tu PPT presenta la cifra de **600 millones de ciberataques diarios a nivel mundial.**

Lo que dices

“Quiero comenzar con un número que puede parecer exagerado: 600 millones de ciberataques al día.

Pero quiero que piensen en lo que significa realmente.

No estamos hablando de que existen 600 millones de hackers sentados frente a una computadora.

Muchos ataques son automatizados.

Existen bots que permanentemente están buscando servidores vulnerables, cuentas expuestas, servicios mal configurados y sistemas que puedan ser explotados.

Entonces, cuando ustedes conectan un dispositivo a Internet, en cierta forma están entrando a un entorno donde constantemente existen máquinas buscando oportunidades.”

Frase potente

“Internet no es un lugar donde nadie te está mirando. Es un lugar donde constantemente existen sistemas buscando qué pueden encontrar.”

DIAPPOSITIVA 3 — El factor humano

Aquí conecta la estadística anterior con el acceso y las credenciales. Tu presentación referencia material relacionado con que el acceso continúa siendo un punto crítico de falla.

Explicación

“Ahora viene lo interesante.

Podemos tener firewalls, antivirus, sistemas de detección, MFA, cifrado...

Pero existe un problema.

Todos esos sistemas están diseñados para proteger personas y organizaciones, y las personas podemos ser manipuladas.

Imaginen que un atacante no necesita vulnerar el firewall.

Simplemente consigue que alguien le entregue voluntariamente la contraseña.

¿Hackeó el sistema?

Técnicamente quizá no.

Hackeó a la persona.”

DIAPPOSITIVA 4 — Transición

Esta diapositiva prácticamente funciona como transición visual.

Lo que dices

“Y aquí aparece uno de los conceptos más importantes de toda la charla:

Ingeniería Social.

No necesariamente consiste en atacar una computadora.

Consiste en atacar las decisiones de una persona.”

Haz una pausa.

“Y para hacerlo, el atacante necesita entender algo que todos nosotros tenemos:

comportamiento humano.”

DIAPPOSITIVA 5 — Perú +360 %

Tu PPT señala un aumento del **360 % de estafas en Perú.**

Lo que dices

“Y esto no es solamente un problema que ocurre en Estados Unidos o Europa.

También tenemos que hablar de nuestro propio entorno.

En la presentación tenemos esta referencia sobre el incremento de estafas en Perú.

Y esto nos debería preocupar porque cada vez utilizamos más servicios digitales:

banca móvil, WhatsApp, redes sociales, compras por Internet, plataformas educativas, billeteras digitales...

Cada servicio adicional significa también una nueva oportunidad para un atacante.”

Pregunta al público

“¿Cuántos de ustedes tienen banca móvil?”

Probablemente casi todos levantarán la mano.

Luego:

“Ahora piensen: ¿cuántos tienen configurado algún mecanismo adicional de seguridad?”

DIAPPOSITIVA 6 — Introducción a Ingeniería Social

Aquí haz una transición.

Di:

“Entonces, ¿qué hace realmente un atacante de ingeniería social?”

No empieza necesariamente preguntándose:

‘¿Qué vulnerabilidad tiene este servidor?’

Muchas veces empieza preguntándose:

‘¿Qué puedo conseguir que esta persona haga?’”

Y aquí introduces los principios psicológicos.

DIAPPOSITIVA 7 — Principios psicológicos

Tu PPT presenta seis principios: **reciprocidad, compromiso y coherencia, aprobación social, autoridad, simpatía y escasez**, basados en la referencia indicada en la presentación.

Esta es una de las diapositivas donde puedes lucirte bastante.

1. Reciprocidad

“Si alguien hace algo por nosotros, sentimos cierta obligación de devolver el favor.”

Ejemplo

“Alguien te escribe:

‘Hola, te conseguí este material para tu examen.’

Y después:

‘Oye, ¿me puedes pasar tu usuario para verificar algo?’”

Frase

“Primero te doy algo. Después te cobro el favor.”

2. Compromiso y coherencia

“Cuando una persona toma una decisión, normalmente intenta mantener coherencia con ella.”

Ejemplo:

“Primero te hacen aceptar algo pequeño:

‘¿Me confirmas tu nombre?’

Después:

‘¿Tu correo?’

Después:

‘¿El código que te llegó?’”

Y dices:

“El atacante no consiguió todo de golpe. **Fue construyendo el compromiso paso a paso.**”

3. Aprobación social

“Si vemos que muchas personas están haciendo algo, tendemos a asumir que debe ser correcto.”

Ejemplo:

“Un mensaje dice:

‘Más de 10.000 estudiantes ya ingresaron al programa.’

¿Qué genera?

Confianza.”

4. Autoridad

Aquí puedes hacer una demostración:

“Imaginen que reciben:

‘Buenos días, soy el director académico. Necesito que me envíes inmediatamente tu información.’”

Pregunta:

“¿Cambiaría algo si el mensaje viniera del director?”

La mayoría dirá sí.

Entonces:

“Eso es autoridad. El atacante utiliza la jerarquía para reducir nuestra capacidad de cuestionar.”

5. Simpatía

“Es más fácil confiar en alguien que nos cae bien.”

Ejemplo:

“Una persona comienza una conversación amigable, encuentra intereses comunes y genera confianza.

Y cuando finalmente solicita información, la petición parece mucho menos sospechosa.”

6. Escasez

“Cuando creemos que algo está por acabarse, sentimos presión para actuar.”

Ejemplos:

“Tu cuenta será suspendida en 10 minutos.”

“Última oportunidad.”

“Solo quedan 2 cupos.”

Frase potente

“La urgencia es enemiga de la verificación.”

DIAPPOSITIVA 8 — Ejemplo / demostración

Aquí puedes interactuar.

Diles:

“Les voy a plantear una situación.

Reciben un mensaje:

‘Hola. Detectamos un inicio de sesión sospechoso en su cuenta. Para evitar el bloqueo, confirme su identidad en los próximos 10 minutos.’”

Pregunta:

“¿Qué harían?”

Después:

“Ahora díganme: ¿qué técnicas psicológicas acabamos de utilizar?”

Y deja que respondan:

- autoridad
- miedo/urgencia
- escasez de tiempo
- compromiso

Esto hará que la clase sea participativa.

DIAPOSITIVA 9 — Investigación / evidencia

La presentación referencia el **37th IEEE Security and Privacy Symposium (2016)**.

Di:

“Todo esto no significa que simplemente estamos hablando de teorías.

La ingeniería social y el comportamiento humano han sido estudiados dentro del ámbito de la seguridad informática.

Y esto es importante porque la ciberseguridad moderna ya no puede analizar solamente máquinas.

Tiene que analizar también:

personas + procesos + tecnología.”

DIAPOSITIVA 10 — Conclusión

Tu PPT introduce aquí una conclusión antes de entrar en las demostraciones prácticas.

Di:

“Hasta aquí quiero que se queden con una idea:

El atacante no necesita que seas ingenuo.

Necesita encontrar el momento adecuado.

Puede aprovechar cansancio, estrés, miedo, confianza, curiosidad o presión.”

DIPOSITIVA 11 — Correo falso

Aquí puedes hacer una de las mejores demostraciones.

Di:

“Ahora vamos a llevar esto a algo que todos ustedes utilizan: el correo electrónico.”

Explica que un correo puede aparentar venir de:

- banco
- instituto
- universidad
- empresa
- jefe
- compañero
- plataforma

Pregunta

“¿Qué revisarían primero?”

Luego explícales:

1. Remitente real

No solamente el nombre mostrado.

2. URL

Pasar el mouse antes de hacer clic.

3. Urgencia

“Actúe inmediatamente.”

4. Solicitud de credenciales

Una señal de alerta.

5. Ortografía y contexto

Pero advierte:

“Ojo: que un correo tenga buena ortografía no significa que sea legítimo.”

DIAPPOSITIVA 12 — Fugas de datos

Tu diapositiva introduce el tema de las grandes fugas de datos.

Di:

“Ahora supongamos que ustedes tienen una contraseña bastante buena.

¿Eso significa que están completamente protegidos?

No.”

Explica:

“Porque existe otro problema: las filtraciones de datos.

Puedes tener una contraseña excelente, pero si una empresa donde utilizaste esa contraseña sufre una brecha, tus datos podrían terminar expuestos.”

Frase

“No solamente debemos proteger nuestras cuentas; debemos asumir que los servicios que utilizamos también pueden ser comprometidos.”

DIAPPOSITIVA 13 — Herramientas

Aquí aparecen:

- Have I Been Pwned
- evaluación de contraseñas
- VirusTotal.

Explica Have I Been Pwned

“Existen servicios que permiten comprobar si una dirección de correo apareció en filtraciones conocidas.”

Aclara:

“No significa que el sitio vaya a recuperar tu contraseña. La idea es comprobar exposición en bases de datos conocidas.”

VirusTotal

“VirusTotal permite analizar archivos, URLs y otros indicadores frente a múltiples motores de seguridad.”

Momento WOW

Diles:

“Y aquí quiero que hagan algo: piensen en su correo principal.

¿Cuántas veces creen que pudo aparecer en alguna filtración?”

Eso genera interés.

DIAPPOSITIVA 14 — Fuerza bruta

Tu PPT introduce el **tiempo necesario para ataques de fuerza bruta**.

Explicación sencilla

“Un ataque de fuerza bruta consiste, simplificando, en probar muchas combinaciones hasta encontrar una que funcione.

Por eso la longitud y complejidad de una contraseña importan.”

Pero agrega algo importante:

“Sin embargo, en el mundo real el atacante no necesariamente empieza probando todas las combinaciones.

Muchas veces prueba primero las contraseñas más comunes.”

DIAPPOSITIVA 15 — Errores comunes

Tu PPT menciona sustituciones simples, uso de información personal, contraseñas de al menos 8 caracteres y reutilización.

Explica:

Error 1: cambiar letras por símbolos

“Password123”

“P@ssword123”

No es necesariamente una transformación tan buena como parece.

Error 2: información personal

“Nombre de mascota + año.”

“Nombre + cumpleaños.”

“Equipo favorito + número.”

Error 3: reutilizar

“Este es probablemente uno de los peores hábitos:

utilizar la misma contraseña para correo, Instagram, Facebook, banco, Netflix, universidad, etc.”

Frase potente

“Si una contraseña se filtra, todas las cuentas que compartan esa contraseña están en riesgo.”

DIPOSITIVA 16 — Nivel 1

Tu PPT coloca ejemplos como:

- Contraseña123
- Qwerty2026
- Cámara123

Di:

“Estas contraseñas tienen un problema fundamental:

son fáciles de adivinar porque utilizan patrones conocidos.”

Pregunta:

“¿Qué creen que probaría primero un atacante?”

La respuesta:

nombres comunes, palabras comunes, números, años y combinaciones predecibles.

DIPOSITIVA 17 — Nivel 2

Ejemplos:

C4m4r42026!

Segur1dad

Di:

“Aquí tenemos un error muy común.

Pensamos:

‘Le puse números, mayúsculas y un signo de exclamación. Entonces es segura.’

Pero si la estructura sigue siendo predecible, no necesariamente hemos conseguido una contraseña realmente robusta.”

DIAPPOSITIVA 18 — Nivel 3

Tu ejemplo:

C0m3rci0Segur0Exterior2026!

Di:

“Aquí ya tenemos una contraseña mucho más larga.

Pero quiero hacerles una pregunta:

¿Es realmente buena solamente porque es larga?”

Luego:

“No necesariamente.

Si contiene información relacionada con una persona, organización, lugar, año o contexto conocido, puede ser más predecible de lo que creemos.”

Regla que quiero que recuerden

“No piensen solamente en complejidad. Piensen en longitud, unicidad y aleatoriedad.”

DIAPPOSITIVA 19 — Evaluar contraseña

Tu PPT incluye una herramienta de Security.org para evaluar la fuerza de contraseñas.

Hazlo interactivo

“Vamos a hacer una prueba.

No quiero que me digan su contraseña real.

Inventen una.”

Luego coloca una contraseña ficticia y analiza qué ocurre.

⚠ Muy importante:

“Nunca introduzcan una contraseña real que utilicen actualmente en una herramienta pública.”

Esto te hará quedar profesional.

DIAPPOSITIVA 20 — Generador de contraseñas

Tu PPT muestra un generador de contraseñas de Security.org.

Di:

“Una de las mejores estrategias no es intentar crear una contraseña súper complicada que nosotros mismos recordemos.

Es utilizar un gestor de contraseñas y generar contraseñas aleatorias y únicas.”

Puedes explicar:

“Una contraseña puede ser completamente diferente para cada servicio.”

DIAPPOSITIVA 21 — OSINT

Aquí tienes dos herramientas:

- FaceCheck
- Globe.airplanes.live

Aquí sorpréndelos

Di:

“Ahora vamos a entrar en un concepto que seguramente muchos de ustedes han escuchado:

OSINT — Open Source Intelligence.

Inteligencia obtenida a partir de información disponible públicamente.”

Ejemplo

“Un atacante puede investigar una persona sin entrar a su computadora.

Puede observar qué publica.

Dónde trabaja.

Qué estudia.

Qué personas conoce.

Qué lugares frecuenta.

Qué fotografías publica.”

Y entonces:

“Con suficiente información, el atacante puede construir un perfil de la víctima.”

Frase fuerte

“La información que publicas por separado puede parecer inútil. Cuando alguien la conecta, puede convertirse en inteligencia.”

DIAPPOSITIVA 22 — Zero Days

Esta es una diapositiva muy buena para subir el nivel técnico.

Tu PPT presenta mercados donde se adquieren vulnerabilidades desconocidas, incluyendo ejemplos de exploits zero-click para Android/iOS y navegadores.

Explícalo así:

“Ahora vamos a pasar de la ingeniería social a una parte mucho más técnica.

¿Qué ocurre cuando encontramos una vulnerabilidad que el fabricante todavía no conoce o para la cual todavía no existe un parche?

Hablamos de un **zero-day**.”

Zero-click

“Y existe algo todavía más impresionante:

un ataque zero-click.

En determinados escenarios, la víctima puede no tener que hacer clic en nada.

El atacante puede aprovechar una vulnerabilidad para comprometer un dispositivo mediante la interacción con determinados servicios o contenidos.”

Frase WOW

“El ataque perfecto para un atacante es aquel en el que la víctima ni siquiera sabe que participó.”

DIAPPOSITIVA 23 — Mercado de vulnerabilidades

Tu presentación menciona Zerodium, Crowdfense y Exodus Intelligence como empresas vinculadas a la adquisición/comercialización de vulnerabilidades y exploits.

Di:

“Y aquí aparece algo que muchas personas desconocen:

las vulnerabilidades tienen valor económico.

Una vulnerabilidad crítica puede valer muchísimo dinero dependiendo de qué sistema afecta, qué tan difícil es explotarla y qué capacidades proporciona.”

Importante

No presentes las cifras como precios universales.

Di:

“Los valores que aparecen en la diapositiva corresponden a referencias de mercados específicos y pueden cambiar.”

Eso te da rigor.

DIPOSITIVA 24 — Perú

Tu presentación dedica una sección al panorama de ataques cibernéticos en Perú y al avance desde phishing hasta técnicas apoyadas por IA.

Di:

“Ahora volvamos a nuestro país.

Muchas veces pensamos que los grandes ataques ocurren solamente en otros países.

Pero Perú también forma parte de este ecosistema.

Tenemos ataques contra empresas, instituciones, ciudadanos y servicios digitales.”

Y aquí introduce IA

“Y ahora tenemos un elemento adicional:

la inteligencia artificial.

La IA puede ayudar a producir mensajes mucho más convincentes, personalizar campañas y reducir errores que antes permitían identificar un fraude.”

DIAPOSITIVA 25 — Monitoreo en línea

Tu PPT muestra:

- Kaspersky Cybermap
- Check Point ThreatMap
- Radware Live Threat Map

Di:

“Ahora quiero mostrarles algo visual.

Existen mapas que representan actividad relacionada con amenazas y ataques observados globalmente.

Lo importante no es interpretar cada punto como un ataque individual confirmado.

Lo importante es entender la escala.”

Frase

“Mientras nosotros estamos aquí hablando, Internet sigue siendo atacado.”

DIAPOSITIVA 26 — Hacktivistas

Tu PPT presenta ejemplos de grupos hacktivistas, incluyendo NoName, Killnet, Anonymous y otros grupos asociados a distintas motivaciones.

Explícalo

“Finalmente tenemos el hacktivismo.

La palabra combina hacking y activismo.

Son actores o grupos que utilizan técnicas digitales para intentar generar impacto político, social o ideológico.”

Aclara algo importante:

“No todos los grupos tienen las mismas capacidades, objetivos o estructura. El panorama es muy diverso.”

DIAPOSITIVA 27 — Tu mejor defensa

Esta es tu oportunidad de cerrar fuerte.

Tu PPT resume cuatro ideas: la ingeniería social ataca la confianza, verificar antes de confiar, contraseñas únicas + 2FA y reportar lo sospechoso.

Mira a los alumnos y di:

“Quiero terminar con algo muy sencillo.

Después de todo lo que hemos visto, probablemente alguien podría pensar:

‘Necesito un antivirus mejor.’

‘Necesito un firewall.’

‘Necesito una computadora más segura.’

Sí.

Pero existe algo todavía más importante.”

Pausa.

“Necesitas aprender a desconfiar inteligentemente.”

Luego:

“No significa desconfiar de todo el mundo.

Significa verificar antes de actuar.”

 CIERRE QUE TE RECOMIENDO

Aquí puedes dejar de mirar las diapositivas.

Camina un poco y diles:

“Quiero que recuerden cuatro cosas de esta charla.

Primero: la ingeniería social no intenta solamente romper sistemas; intenta manipular personas.

Segundo: cuando alguien te presiona para actuar rápidamente, detente.

Tercero: una contraseña diferente y el segundo factor pueden marcar una enorme diferencia.

Cuarto: si ves algo sospechoso, repórtalo.

Porque quizás tú seas la persona que evitó que una organización completa fuera comprometida.”

Y finalmente:

****“La ciberseguridad no es responsabilidad solamente del área de TI.**

Cada persona que utiliza un dispositivo conectado a Internet forma parte de la defensa.”**

Pausa.

Y remata:

****“El atacante solamente necesita que una persona se equivoque una vez.**

Nosotros necesitamos conseguir que esa persona piense antes de hacer clic.”**

TRES MOMENTOS PARA HACERLOS DECIR "WOW"

1. Al inicio

Pregunta:

“¿Quién aquí cree que sabe reconocer un phishing?”

Que levanten la mano.

Al final:

“Ahora que conocen autoridad, urgencia, escasez, reciprocidad y aprobación social... ¿siguen estando tan seguros?”

2. En contraseñas

Diles:

“Nunca me digan su contraseña. Quiero que inventen una.”

Y muestra ejemplos.

Después:

“El problema no es solamente que una contraseña sea corta. El problema es que nosotros somos muy predecibles.”

3. En ingeniería social

Haz esta demostración:

“Imaginen que les llega un WhatsApp:

‘Hola, soy el director del instituto. Estoy en una reunión. Necesito que me envíes urgentemente el código que acaba de llegar a tu celular.’

¿Quién lo enviaría?”

Después:

“Acabamos de utilizar **autoridad + urgencia + contexto + presión.**”

Eso les quedará grabado.



TU REGLA DE ORO COMO EXPOSITOR

No leas:

“Reciprocidad significa...”

Habla como especialista:

“¿Alguna vez alguien les ha hecho un favor y después ustedes sintieron que tenían que devolverlo? Perfecto. Ese comportamiento aparentemente normal es precisamente el que puede explotar un atacante.”

Eso te hará parecer mucho más profesor/especialista que simplemente leer definiciones.

Y sobre todo, **no intentes demostrar que sabes más que ellos.** Haz que ellos descubran que estaban expuestos sin darse cuenta.

Tu PPT ya tiene una estructura bastante buena para eso.