

## Lab - Explore Técnicas de ingeniería social

### Objetivos

Parte 1: Explorar Técnicas de ingeniería social

Parte 2: Crear un póster de Concientización sobre ciberseguridad

## LAS PREGUNTAS ESTÁN MÁS ABAJO

**NOTA: RESPONDER CADA PREGUNTA CON CAPTURAS DE PANTALLA COMPLETAS DONDE SE VEAN LAS SIGLAS DE SU NOMBRE AL LADO DEL RELOJ. EN LUGAR DE COLOCAR UN TEXTO DEBE DE SELECCIONAR EL TEXTO INVESTIGADO EN UNA PÁGINA WEB Y HACERLE CAPTURA DE PANTALLA COMPLETA, PARA LUEGO COLOCARLA AQUÍ. SI SON VARIAS PREGUNTAS, DEBE COLOCAR VARIAS CAPTURAS DE PANTALLAS COMPLETAS. NO COLOCAR INFORMACIÓN ENCONTRADA EN NETACAD, COLOCAR INFORMACIÓN INVESTIGADA EN OTRAS PÁGINAS WEB.**

### Introducción

La ciberseguridad es fundamental porque implica proteger el acceso no autorizado a datos confidenciales, información de identificación personal (PII), información de salud protegida (PHI), información personal, propiedad intelectual (IP) y sistemas confidenciales. La ingeniería social es la manipulación a las personas para que realicen acciones o divulguen información confidencial. En esta práctica de laboratorio, explorará técnicas de ingeniería social, a veces denominadas hacking humano, que es una categoría amplia para los diferentes tipos de ataques.

### Recursos necesarios

Computadora personal o dispositivo móvil con acceso a internet

### Aspectos básicos/Situación

Investigaciones recientes revelan que los tipos más comunes de ataques ciberneticos son cada vez más sofisticados y que los objetivos de ataque están creciendo. El propósito de un ataque es robar información, deshabilitar sistemas o servicios críticos, interrumpir sistemas, actividades y operaciones. Algunos ataques están diseñados para destruir información o sistemas de información, controlar maliciosamente un entorno informático o su infraestructura, o destruir la integridad de datos y / o sistemas de información. Una de las maneras más eficaces en que un atacante puede obtener acceso a la red de una organización es mediante un simple engaño. En el mundo de la ciberseguridad, esto se denomina ingeniería social.

### Ataques de ingeniería social

Los ataques de ingeniería social son muy eficaces porque las personas quieren confiar en otras personas y los ataques de ingeniería social no son el tipo de ataque contra el que se protege el usuario promedio; los usuarios están preocupados por botnets, robo de identidad o ransomware. Estas son grandes amenazas externas, por lo que no piensan en cuestionar lo que parece ser un mensaje de aspecto legítimo.

### Hostigamiento

La carnada depende de la curiosidad o la codicia de la víctima. Lo que distingue a los cebos de otros tipos de ingeniería social es la promesa de un artículo o bien que los hackers utilizan para atraer a las víctimas. Baiters puede ofrecer a los usuarios descargas gratuitas de música o películas si los usuarios entregan sus credenciales de inicio de sesión a un sitio determinado. Los ataques de cebo no se limitan a los esquemas en línea. Los atacantes pueden aprovechar la curiosidad humana con medios físicos como unidades USB.

### Espiar por encima del hombro

La navegación de hombro es, literalmente, mirar por encima del hombro de alguien para obtener información. La navegación de hombro es una forma eficaz de obtener información en lugares con mucha gente, ya que es relativamente fácil pararse junto a alguien y observar cómo completan un formulario o ingresan un número PIN en un cajero automático. La navegación de hombro también puede realizarse a larga distancia con la ayuda de teléfonos celulares modernos, binoculares u otros dispositivos para mejorar la visión. Para evitar que se hunden los hombros, los expertos recomiendan proteger la documentación o el teclado mediante el cuerpo o la mano. Incluso hay protectores de pantalla que dificultan mucho la navegación por el hombro.

### Pretexto

Pretexto es utilizar el engaño para crear un escenario para convencer a las víctimas de divulgar información que no deben divulgar. Los pretextos a menudo se usan contra organizaciones que conservan datos de clientes, como datos financieros, números de tarjetas de crédito, números de cuentas de servicios públicos y otra información confidencial. A menudo, los pretextos solicitan información a las personas de una organización mediante la suplantación de un supervisor, un empleado del servicio de asistencia o un cliente, generalmente por teléfono, correo electrónico o mensaje de texto.

### Suplantación de identidad, suplantación de identidad y ataques de caza de ballenas

En los ataques de suplantación de identidad, los atacantes intentan obtener información personal o datos, como nombre de usuario, contraseña y datos de tarjetas de crédito, disfrazándose de entidades confiables. La suplantación de identidad se realiza principalmente a través de correos electrónicos y llamadas telefónicas. El Spear Phishing es una versión más específica de la suplantación de identidad (phishing) en la que un atacante elige individuos o empresas específicos y luego personaliza el ataque de suplantación de identidad (phishing) a sus víctimas para que sea menos visible. La caza de ballenas es cuando el objetivo específico es un empleado de alto perfil, como un CEO o CFO.

### Scareware y ransomware

Los ataques de ransomware implican la inyección de malware que cifra los datos críticos de una víctima. The cyber criminals request a ransom to be paid to decrypt the data. Sin embargo, incluso si se paga un rescate, no hay garantía de que los cibercriminales descifren la información. El ransomware es uno de los tipos de ataque cibernetico de más rápido crecimiento y ha afectado a miles de organizaciones financieras, agencias gubernamentales, centros de salud, incluso escuelas y nuestros sistemas educativos.

El scareware aprovecha el temor de un usuario para convencerlo de que instale un software antivirus falso.

### Infiltración (tailgating)

El seguimiento ilegal engaña a la víctima para que ayude al atacante a obtener acceso no autorizado a las instalaciones físicas de la organización. El atacante busca entrar en un área restringida donde el acceso está controlado por dispositivos electrónicos basados en software o guardias humanos. El seguimiento ilegal también puede implicar que el atacante siga de cerca a un empleado para atravesar una puerta cerrada antes de que la puerta se cierre detrás del empleado.

#### Hurgar en la basura

En el mundo de la ingeniería social, el buceo con contenedores de basura es una técnica utilizada para recuperar información desechada que se arroja a la basura para llevar a cabo un ataque contra una persona u organización. Bucear en el contenedor no se limita a buscar en la basura tesoros obvios, como códigos de acceso o contraseñas escritas en notas adhesivas, sino que también puede incluir información electrónica que se deja en los equipos de escritorio o se almacena en unidades USB.

### Parte 1. Explore las técnicas de ingeniería social

#### Paso 1: Explore la carnada, la navegación de hombro y la predisposición.

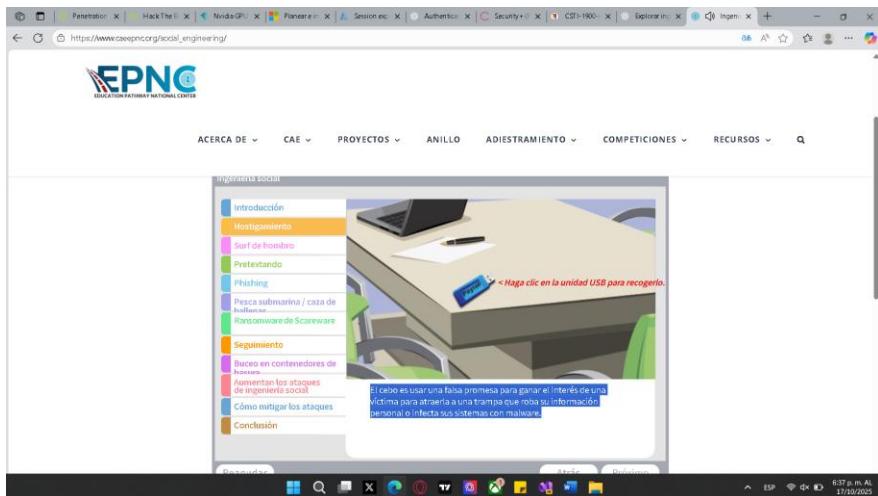
El Centro de soporte nacional para la seguridad de los sistemas y el aseguramiento de la información (CSSIA) organiza una actividad interactiva de ingeniería social. El enlace actual al sitio es [https://www.cssia.org/social\\_engineering/](https://www.cssia.org/social_engineering/). Sin embargo, si el enlace cambia, intente buscar "CSSIA Social Engineering Interactive".

Haga clic en Siguiente en la actividad interactiva y luego utilice el contenido para responder las siguientes preguntas.

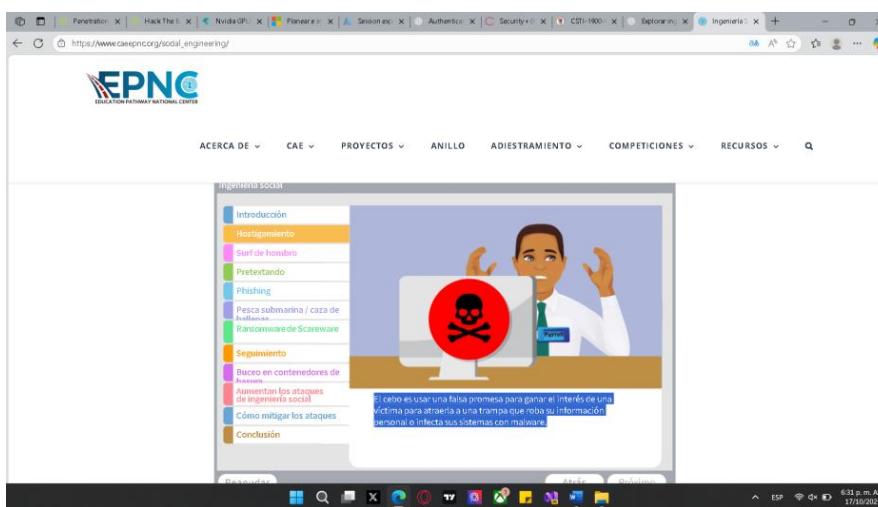
**NOTA: RESPONDER CADA PREGUNTA NO CON TEXTO SINO CON CAPTURAS DE PANTALLA COMPLETAS DONDE SE VEAN LAS SIGLAS DE SU NOMBRE AL LADO DEL RELOJ. EN LUGAR DE COLOCAR UN TEXTO DEBE DE SELECCIONAR EL TEXTO INVESTIGADO EN UNA PÁGINA WEB Y HACERLE CAPTURA DE PANTALLA COMPLETA, PARA LUEGO COLOCARLA AQUÍ. SI SON VARIAS PREGUNTAS, DEBE COLOCAR VARIAS CAPTURAS DE PANTALLAS COMPLETAS. NO COLOCAR INFORMACIÓN ENCONTRADA EN NETACAD, COLOCAR INFORMACIÓN INVESTIGADA EN PÁGINAS WEB.**

¿Qué es la carnada?

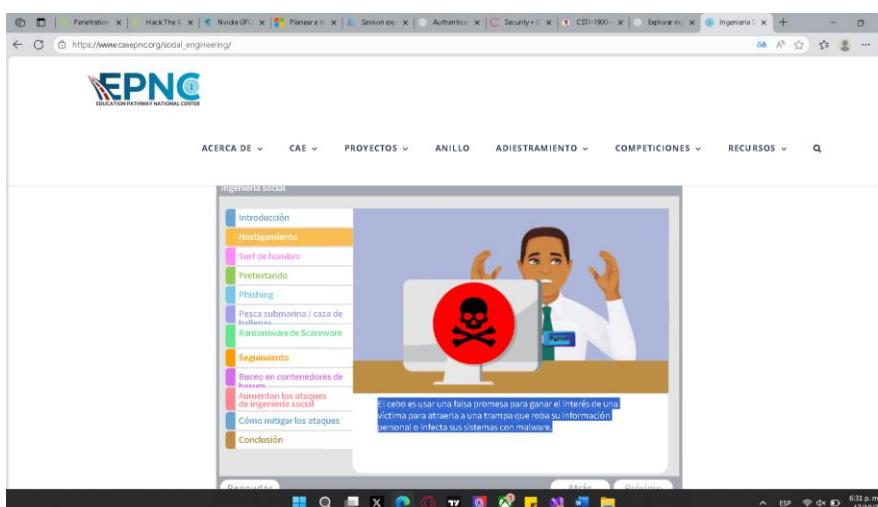
## Lab - Explore Técnicas de ingeniería social



¿Hizo clic en la unidad USB?



¿Qué sucedió con el sistema de la víctima?



A la víctima se le infectó su computadora con un malware

## Lab - Explore Técnicas de ingeniería social

¿Qué es espiar por encima del hombro?

The screenshot shows a computer monitor displaying the EPNC (Education Pathway National Center) website. The main content area is titled 'Ingeniería Social' and features a sub-section titled 'Surf de hombro'. A sidebar on the left lists various social engineering techniques with colored icons. The central image shows a woman holding a smartphone while a man sits at a desk with a computer monitor, illustrating the concept of shoulder surfing. A red call-to-action bubble says 'Haga clic en el teléfono para ver la' (Click on the phone to see the). Below the image is a descriptive text box: 'El shoulder surfing consiste en mirar por encima del hombro de alguien mientras usa una computadora y capturar visualmente inicio de sesión o contraseñas u otra información confidencial.'

¿Qué dispositivo se utilizó para espiar por encima del hombro?

This screenshot is a closer look at the same section from the previous image. It highlights the 'Surf de hombro' section and zooms in on the illustration of the woman's phone screen. The phone screen displays a login interface with fields for 'Login: Bob' and 'Password: 420Hate2537'. The surrounding environment remains the same, showing the EPNC website's navigation bar and sidebar.

Se utilizo un celular

¿Qué información se obtuvo?

El inicio de sección y contraseña

This screenshot shows the final result of the shoulder surfing attack. The phone screen now displays a successful login message: 'Login: Bob' and 'Password: 420Hate2537'. The background image and sidebar remain consistent with the previous screenshots, illustrating the completion of the attack.

## Lab - Explore Técnicas de ingeniería social

### ¿Qué es Pretextar (pretexting)?

The screenshot shows a section titled 'Ingeniería social' with a sub-section 'Pretextando'. The main content area contains a cartoon illustration of a devilish character on the left and a woman on the right. A speech bubble from the devil says 'Haga clic en el teléfono para contestar' (Click on the phone to answer). Below the illustration, there is explanatory text: 'El pretexting es cuando un atacante establece confianza con su víctima haciéndose pasar por personas que tienen derecho a saber autoridad y hace preguntas que parecen ser necesarias para confirmar la identidad de la víctima, pero a través de las cuales recopilan datos personales importantes.'

### ¿Qué tipo de información solicitó el ciberdelincuente?

The screenshot shows a similar layout to the previous one, with the 'Ingeniería social' and 'Pretextando' sections. The main content area features a cartoon of a devil and a woman. The devil's speech bubble says 'My name is Jane Smith Director of Research ID# 123-456'. The woman's speech bubble says 'Hello. This is IT. We noticed some unusual activity on your account. Please verify your name, title, office and employee badge number.' Below the illustration, there is explanatory text: 'El pretexting es cuando un atacante establece confianza con su víctima haciéndose pasar por personas que tienen derecho a saber autoridad y hace preguntas que parecen ser necesarias para confirmar la identidad de la víctima, pero a través de las cuales recopilan datos personales importantes.'

Se hace pasar por el departamento de TI para pedir el usuario del director

¿Caería como víctima?

The screenshot shows the same pretexting diagram and explanatory text as the previous ones, emphasizing the tactic of impersonating IT staff to gain access to sensitive information.

No caería porque preguntaría y confirmaría

### Paso 2: Explore el Phishing, el Spear Phishing y la caza de ballenas

La suplantación de identidad (Phishing) está diseñada para que las víctimas hagan clic en enlaces a sitios web maliciosos, abran archivos adjuntos que contengan malware o revelen información confidencial. Utilice la actividad interactiva para explorar diferentes técnicas de suplantación de identidad.

En este ejemplo de suplantación de identidad,

¿cuál es la táctica que utiliza el atacante para engañar a la víctima para que visite el sitio web de la trampa?

The screenshot shows a web-based training module for social engineering. At the top, there's a navigation bar with links like 'ACERCA DE', 'CAE', 'PROYECTOS', 'ANILLO', 'ADIESTRAMIENTO', 'COMPETICIONES', 'RECURSOS', and a search icon. Below the navigation is a sidebar with a vertical list of topics: Introducción, Hostigamiento, Surf de hombre, Pretendiendo, Phishing, Pesc submarina / caza de ballenas, Ransomware de Scareware, Seguimiento, Buceo en contenidores de basura, Aumentan los ataques de ingeniería social, Cómo mitigar los ataques, and Conclusión. The main content area features a cartoon illustration of a woman at a computer. A blue box labeled 'Trusted Bank' contains an email message to a client about a recent withdrawal. Below the message is a red button with the text 'Haga clic en el enlace de arriba para continuar.' (Click the link above to continue.) At the bottom of the main content area, there are 'Rearricular', 'Atrás', and 'Próximo' buttons. The status bar at the bottom right shows system information: 3:52 p.m. AL, 19/10/2025.

Utiliza un correo asíéndose pasar por un banco

¿Para qué se utiliza el sitio web de trap?

This screenshot shows another part of the social engineering simulation. The layout is similar to the previous one, with a sidebar of topics and a main content area featuring a cartoon illustration. In the main content area, there are two separate login forms for 'Trusted Bank' displayed side-by-side. Both forms have fields for 'Username' and 'Password'. A text box between the forms states: 'El phishing está diseñado para que las víctimas hagan clic en enlaces a sitios web maliciosos, abran archivos adjuntos que contengan malware o revelen información confidencial.' At the bottom of the main content area are 'Rearricular', 'Atrás', and 'Próximo' buttons. The status bar at the bottom right shows system information: 3:51 p.m. AL, 19/10/2025.

Para robar la información de inicio de sección

¿Cuál es la diferencia entre Phishing y Spear Phishing o caza de ballenas?

The screenshot shows a slide from a presentation titled "Spear Phishing / caza de ballenas". The slide includes a sidebar with navigation links like "introducción", "Hostigamiento", "Surf de hombre", "Pretendiendo", "Phishing", "Pescar ballena / caza de ballenas", "Ransomware de Scareware", "Seguimiento", "Buceo en contenidores de malware", "Aumentan los ataques de ingeniería social", "Cómo mitigar los ataques", and "Conclusión". The main content area features a cartoon character of a man in a suit and a screenshot of an email from "Richard.Brown@cauchyinsurance.com" with the subject "Pago más rápido". The email body says: "Espero que tu día vaya bien. Necesito enviar un pago más rápido de lo normal. Puedes hacerlo al fin de este mes el día de mañana." Below the email is a note: "Por favor, envíeme un correo electrónico con los detalles respondidos que necesitaré para enviar el pago." A green button at the bottom says "Haga clic en el botón Responder para continuar." Navigation buttons "Rearumar", "Atrás", and "Próximo" are at the bottom.

### Paso 3: Explore Scareware y Ransomware

Scareware es cuando las víctimas son engañadas al pensar que su sistema está infectado con malware y reciben falsas alarmas que les instan a instalar software que no es necesario o es en sí mismo malware. El ransomware es un tipo de malware que amenaza con publicar los datos de la víctima o encripta los datos de la víctima impidiendo el acceso o la capacidad de usar los datos. Las víctimas no pueden acceder a su sistema o a sus archivos personales hasta que realicen un pago de rescate para recuperar el acceso.

¿Qué datos afirma tener el atacante en este ejemplo? ¿Caería usted en este engaño?

The screenshot shows a slide from a presentation titled "Ransomware de Scareware". The sidebar is identical to the previous slide. The main content area features a cartoon character of a man in a suit and a screenshot of an email with the subject "\*\*SU COMPUTADORA HA SIDO BLOQUEADA\*\*". The email body says: "Su computadora nos ha alertado de que ha sido infectada con un virus y spyware. Se está robando la siguiente información: > Inicio de sesión de Facebook- Detalles de la tarjeta de crédito- Inicio de sesión de la cuenta de correo electrónico. Límanos dentro de los próximos 5 minutos para evitar que su computadora se desactive. Llame al: 44-8000-003- < Haga clic en el botón Llamar para continuar." Below the email is a note: "Scareware y ransomware. El scareware se clama de las víctimas son engañadas para que crean que su sistema está infectado con malware y reciben falsas alarmas que les piden que instalen software que no es necesario o que es en sí mismo malware. El ransomware es cuando se impide a las víctimas acceder a su sistema o archivos personales hasta que realicen un pago de rescate para recuperar el acceso." Navigation buttons "Rearumar", "Atrás", and "Próximo" are at the bottom.

El ejemplo de un malware en su computadora

## Lab - Explore Técnicas de ingeniería social

¿Qué solicita el atacante que haga la víctima para recuperar los datos?

The screenshot shows a web-based training module from EPNC. On the left, there's a sidebar with various attack types: Introducción, Hostigamiento, Surf de hombre, Pretendiendo, Phishing, Pesc submarina / caza de polluelos, Ransomware de Scareware, Seguimiento, Buceo en contenedores de basura, Aumentar los ataques de ingeniería social, Cómo mitigar los ataques, and Conclusión. The main content area displays a message in Spanish:

\*\*SU COMPUTADORA HA SIDO BLOQUEADA\*\* Su computadora nos ha alertado de que ha sido infectada con un virus y soyware. Se está robando la información de su sistema.

Haga clic en el botón Llamar para contactarnos.

Llame al: 44-8000-8033

Scareware y ransomware: El scareware es cuando las víctimas son engañadas para que piensen que su sistema está infectado con malware y reciben falsos alarmes que les indican software que no es necesario que es en sí mismo malware. El ransomware es cuando se impide a los víctimas acceder a su Sistema o dispositivo personal hasta que realizan un pago de rescate para recuperar el acceso.

**Haga clic en el botón Llamar para contactarnos.**

At the bottom, there are 'Reanudar', 'Atrás', and 'Próximo' buttons.

Solicita a la víctima que llame a para recuperar su información

¿Qué es la infiltración (tailgating)?

This screenshot shows another slide from the EPNC training module. The sidebar and navigation are identical to the previous one. The main content area features an illustration of a hand holding a card labeled 'Haga clic en tarjeta de acceso para entrar'. Below it, the text reads:

Tailgating es cuando un atacante que carece de la autorización, accede a una víctima con credenciales autorizadas a través de una puerta u otro punto de acceso seguro al edificio a un área autorizada.

At the bottom, there are 'Reanudar', 'Atrás', and 'Próximo' buttons.

¿De tres maneras de prevenir ataques de ingeniería social?

This screenshot shows the final slide of the module. The sidebar and navigation are consistent. The main content area contains three numbered tips:

1. Píense antes de actuar: Nunca comparta información en línea con personas que no conoce o que no son seguros. No haga clic en correos electrónicos o en otros enlaces adjuntos de correos electrónicos de remitentes desconocidos.
2. Esté atento a si el correo es específico con los enlaces a formularios web que solicitan información personal, incluso si el correo electrónico parece provenir de una fuente legítima. Nunca haga clic ni ingrese información confidencial en una ventana emergente.
3. Mantenga sus cuentas y dispositivos seguros: use software antivirus y filtros de spam, y actualice y parchee sus dispositivos con regularidad.

At the bottom, there are 'Reanudar', 'Atrás', and 'Próximo' buttons.

## Parte 2. Crear un póster de Concientización sobre ciberseguridad

Utilice PowerPoint para crear un póster que haga que otros conozcan las diferentes técnicas de ingeniería social utilizadas para obtener acceso no autorizado a una organización o a los datos de la organización.

Elija entre: hostigamiento, navegación de hombro, pretexto, suplantación de identidad (phishing), Scareware, ransomware, infiltración o buceo en el contenedor.

El póster debe mostrar las técnicas utilizadas y cómo los usuarios pueden evitar uno de estos ataques de ingeniería social. También incluya instrucciones sobre dónde debe colocarse el póster dentro de la organización.

