Actividad 05. Ataques de ingeniería social

1. Describe con tus propias palabras qué es la ingeniería social, los tipos y técnicas existentes

La **ingeniería social** es como un juego de manipulación pero en el mundo digital. Los ciberdelincuentes usan técnicas psicológicas para engañar a las personas y hacer así que revelen información confidencial o realizar acciones que no se deberían.

¿CÓMO FUNCIONA?

Los atacantes estudian el comportamiento y aprovechan las debilidades humanas (confianza, curiosidad, urgencia). Se podrían pasar por alguien que conocemos para pedir ayuda o enviar un correo electrónico falso que parece muy importante.

TIPOS Y TÉCNICAS:

- ***PHISHING:*** La técnica más común. Envía correos electrónicos falsos que parecen provenir de empresas o personas de confianza para que se haga clic en enlaces maliciosos o entregues tus contraseñas.
- ***VISHING:*** Similar al Phishing, pero se realiza a través de llamadas telefónicas. Los atacantes se hacen pasar por bancos, empresas de servicios públicos o técnicos de soporte para obtener información personal.

- ***SMISHING:*** El Phishing a través de mensajes de texto. Los atacantes envían SMS falsos que te llevan a sitios web fraudulentos.
- ***PRETEXTING:*** Los atacantes crean una historia convincente para obtener información.
- ***BAITING:*** Los atacantes ofrecen algo atractivo (dispositivo USB infectado, descarga gratuita, etc.) para que la víctima lo tome y así infectar el equipo.
- ***QUID PRO QUO:*** Ofrecer algo a cambio de información.

¿CÓMO PROTEGERSE?

1. ***DESCONFÍA DE LOS MENSAJES NO SOLICITADOS:*** No hacer clic en enlaces ni abrir archivos adjuntos de remitentes desconocidos.
2. ***VERIFICA LA IDENTIDAD DEL REMITENTE:*** Asegurarse de que el correo electrónico o mensaje de texto provenga de una fuente confiable.
3. ***NO COMPARTIR INFORMACIÓN PERSONAL POR TELÉFONO O CORREO ELECTRÓNICO:*** Evitar revelar datos sensibles a menos que se esté seguro de con quién se está hablando.
4. ***UTILIZAR CONTRASEÑAS FUERTES Y ÚNICAS:*** Cambiar las contraseñas regularmente y utilizar combinaciones de letras, números y caracteres especiales.
5. ***MANTENER EL SOFTWARE ACTUALIZADO:*** Las actualizaciones de seguridad corrigen vulnerabilidades que los atacantes pueden explotar.

2. Busca ejemplos de ingeniería social

EJEMPLOS:

1. ***El Falso Técnico de Soporte***: Recibes una llamada de alguien que se hace pasar por un técnico de tu proveedor de Internet, informándote de que hay un problema de seguridad en tu red y solicitando acceso remoto al ordenador.
2. ***Baiting en Redes Sociales***: Un ciberdelincuente crea un perfil falso en una red social y se hace amigo de sus víctimas para luego enviarles un mensaje privado con un enlace a un archivo infectado, haciéndoles creer que es una foto o un vídeo interesante.

3. ***El Estafador que Pide Dinero***: Un desconocido se acerca a ti en la calle y te pide dinero prestado, inventando una historia conmovedora para ganarse tu confianza.

3. Explica, con tus propias palabras, que medidas has de realizar en una organización para evitar los ataques de ingeniería social

MEDIDAS PARA PREVENIR ATAQUES DE INGENIERÍA SOCIAL EN UNA ORGANIZACIÓN:

1. ***CONCIENTIZACIÓN Y CAPACITACIÓN:***
   a. ***Programas de Entrenamiento Regulares***: Impartir talleres y cursos para que los empleados identifiquen los diferentes tipos de ataques de ingeniería social (phishing, pretexting, baiting, etc.).
   b. ***Simulaciones de Ataques***: Realizar simulaciones realistas para evaluar la capacidad de respuesta de los empleados ante situaciones de riesgo y reforzar su aprendizaje.
2. ***POLÍTICAS DE SEGURIDAD:***
   a. ***Política de Contraseñas Válidas***: Establecer requisitos estrictos para la creación y gestión de contraseñas, promoviendo el uso de contraseñas únicas y complejas.
   b. ***Política de Uso Aceptable de Dispositivos***: Definir las reglas para el uso de dispositivos personales en el entorno laboral y establecer medidas de seguridad para los equipos.
   c. ***Política de Correo Electrónico***: Implementar filtros antispam y educar a los empleados sobre cómo identificar correos electrónicos sospechosos.
3. ***TECNOLOGÍA DE SEGURIDAD:***
   a. ***Soluciones de Seguridad de Correo Electrónico***: Utilizar herramientas que filtren el correo no deseado y detecten enlaces y archivos maliciosos.
   b. ***Sistemas de Detección de Intrusiones***: Implementar sistemas que monitorean la red en busca de actividades sospechosas.
   c. ***Autenticación de Dos Factores***: Exigir una segunda forma de verificación para acceder a sistemas y aplicaciones sensibles.

4. ***GESTIÓN DE INCIDENTES:***
    a. ***Plan de Respuesta a Incidentes***: Desarrollar un plan detallado para responder de manera rápida y efectiva ante un ataque de ingeniería social.
    b. ***Equipo de Respuesta a Incidentes***: Designar un equipo responsable de investigar y contener los incidentes de seguridad.
5. ***CULTURA DE SEGURIDAD:***
    a. ***Fomentar una Cultura de Seguridad***: Crear un ambiente de trabajo donde la seguridad cibernética sea una prioridad para todos los empleados.
    b. **Comunicación Abierta**: Establecer canales de comunicación para que los empleados puedan reportar cualquier actividad sospechosa sin temor a represalias.