INGENIERÍA SOCIAL Y PHISHING

¿Qué es un Ataque de Ingeniería Social?

En un ataque de **ingeniería social**, un atacante utiliza la interacción humana (habilidades sociales) para obtener o comprometer información sobre una organización o sus sistemas informáticos. Un atacante puede **parecer modesto y respetable**, posiblemente **afirmando ser un nuevo empleado**, persona de reparación o investigador e **incluso ofreciendo credenciales** para respaldar esa identidad. Sin embargo, **al hacer preguntas**, él o ella **pueden reunir suficiente información para infiltrarse en la red de una organización**. Si un atacante no puede recopilar suficiente información de una fuente, puede contactar a otra fuente dentro de la misma organización y confiar en la información de la primera fuente para aumentar su credibilidad.

¿Qué es un Ataque de Phishing?

El **phishing** es una forma de ingeniería social. Los **ataques de phishing** usan **correo electrónico o sitios web maliciosos** para **solicitar información personal haciéndose pasar por una organización confiable**. Por ejemplo, un atacante puede enviar un correo electrónico aparentemente de una compañía de tarjetas de crédito o institución financiera acreditada que solicita información de cuenta, **a menudo sugiriendo que hay un problema**. Cuando los usuarios responden con la información solicitada, los atacantes pueden usarla para **obtener acceso a las cuentas**.

Los ataques de phishing también pueden parecer provenir de **otros tipos de organizaciones**, como organizaciones benéficas. Los atacantes a menudo **aprovechan los eventos actuales y ciertas épocas del año**, como:

- Desastres naturales (p. ej., huracán Katrina, tsunami de Indonesia)
- Epidemias y problemas de salud (p. ej., Virus H1N1)
- Preocupaciones económicas (por ejemplo, estafas de Entidades Comerciales locales)
- Elecciones políticas importantes
- Días festivos

¿Qué es un Ataque Vishing?

Vishing es el enfoque de ingeniería social que **aprovecha la comunicación de voz**. Esta técnica se puede combinar con otras formas de ingeniería social que **incitan a la víctima a llamar a un número determinado y divulgar información confidencial**. Los ataques de vishing avanzados pueden tener lugar por completo a través de las comunicaciones de voz mediante la explotación de soluciones de Voz sobre Protocolo de Internet (VoIP) y servicios de transmisión. VoIP **permite fácilmente falsificar la identidad de la persona que llama (ID)**, lo que puede aprovechar la confianza equivocada del público en la seguridad de los servicios telefónicos, especialmente los servicios de línea fija. La comunicación de línea fija no puede ser interceptada sin acceso físico a la línea; Sin embargo, este rasgo no es beneficioso cuando se comunica directamente con un actor malicioso.

¿Qué es un Ataque Smishing?

Smishing es una forma de ingeniería social que **explota los mensajes de texto o SMS**. Los mensajes de texto pueden contener **enlaces a elementos** tales como **páginas web**, **direcciones de correo electrónico** o **números de teléfono** que, **al hacer clic**, pueden **abrir automáticamente una ventana del navegador o un mensaje de correo electrónico o marcar un número**. Esta integración de la funcionalidad de correo electrónico, voz, mensajes de texto y navegador web aumenta la probabilidad de que los usuarios sean víctimas de actividades maliciosas diseñadas.

¿Cómo evitar ser una Víctima?

- **Sospeche** de **llamadas telefónicas no solicitadas**, **visitas o mensajes de correo electrónico** de personas que **preguntan sobre empleados** u otra **información interna**. Si un individuo desconocido afirma ser de una organización legítima, **intente verificar su identidad directamente con la empresa**.
- **No proporcione información personal** o **información sobre su organización**, incluida **su estructura o redes**, a menos que esté seguro de la autoridad de una persona para tener la información.

- **No revele información personal o financiera en el correo electrónico**, y **no responda** a **solicitudes de correo electrónico para esta información**. Esto incluye los siguientes enlaces enviados por correo electrónico.
- **No envíe información confidencial** por Internet **antes de verificar la seguridad de un sitio web**. (Consulte Protección de su privacidad para obtener más información).
- **Preste atención** a la **URL** (Dirección de Internet) de un sitio web. Los sitios web maliciosos pueden **parecer idénticos** a un sitio legítimo, pero la **URL puede usar una variación en la ortografía o en un dominio diferente**. (Por ejemplo: .com *vs* .net)
- **Si no está seguro** si una solicitud de correo electrónico es legítima, **intente verificarla comunicándose directamente con la empresa**.
- **No utilice** la información de contacto proporcionada en un sitio web conectado a la solicitud; en su lugar, **verifique las declaraciones anteriores para obtener información de contacto**. La **información sobre los ataques de phishing** conocidos también está disponible en línea de grupos como el Grupo de Trabajo Anti-Phishing.

Mantenga el software antivirus, cortafuegos y filtros de correo electrónico para reducir parte de este tráfico.

¿Qué hacer si cree que es una Víctima?

Si cree que podría haber **revelado información confidencial sobre su organización**, **repórtela** a las personas apropiadas dentro de la organización, incluidos los administradores de Red y personal de Seguridad. Pueden estar alertas ante cualquier actividad sospechosa o inusual.

Si cree que sus **cuentas financieras pueden verse comprometidas**, **comuníquese con su institución financiera de inmediato** y **cierre cualquier cuenta que pueda haber estado en peligro**. Esté atento a **cualquier cargo inexplicable a su cuenta**.

Cambie de inmediato cualquier contraseña que haya revelado. Si usó la misma contraseña para múltiples recursos, asegúrese de **cambiarla para cada cuenta** y no la use en el futuro. Esté atento a **otros signos de robo de identidad**.