Ingeniería Social

Ejemplos de investigación

* Hotel Marriott: un grupo de hackers utilizó tácticas de ingeniería social para robar 20 GB de datos personales y financieros de un hotel Marriott. Los piratas informáticos engañaron a un empleado del hotel Marriott para que le diera acceso a su ordenador.
* Departamento de Trabajo de los Estados Unidos (DoL): se trataba de un ataque de ingeniería social que robaba las credenciales de inicio de sesión de Office 365. El ataque utilizó un sofisticado phishing basado en dominios suplantados de forma inteligente que parecían el dominio legítimo del DoL. Los mensajes de correo electrónico parecían proceder de un empleado de alto nivel del DoL que les invitaba a presentar una oferta para un proyecto gubernamental. Al hacer clic en el botón de la oferta, el empleado accedía a un sitio de phishing utilizado para robar credenciales.
* Usuarios de Zoom: una campaña de phishing dirigida a empleados afectó al menos a 50.000 usuarios. Los ingenieros sociales utilizaron el miedo al despido para animar a los empleados a hacer clic en un enlace para reunirse con RRHH a través de Zoom. Al hacer clic en el enlace, el empleado accedía a un sitio de inicio de sesión de Zoom falso diseñado para robar contraseñas.
* FACC (fabricante austriaco de aviones): FACC perdió alrededor de 42 millones de euros cuando la empresa fue víctima de una sofisticada estafa de correo electrónico comercial (BEC). Se suplantó la cuenta de correo electrónico del director general de la empresa y se utilizó para enviar un correo electrónico "urgente" solicitando una transferencia de fondos. Este correo electrónico engañó a un empleado encargado de pagar la cuenta, que accedió a la solicitud, ingresando el dinero en la cuenta del estafador.
* Llamada de atención de Crowdstrike Incluso los proveedores de seguridad están sintiendo la fuerza de la ingeniería social. Crowdstrike se ha convertido en un peón involuntario en el juego de los ingenieros sociales. Los estafadores están utilizando la marca de confianza de Crowdstrike y otros proveedores de seguridad para enviar correos electrónicos de phishing a los empleados. El correo electrónico contiene detalles de una posible infección de malware y un número de teléfono al que llamar para eliminar el malware instalado. Si el empleado llama al número, se le engaña para que dé al atacante acceso a su ordenador.

Reconocimientos de los signos

Tómese el tiempo para considerar la situación en pleno, y examine el mensaje con cuidado, incluso si resulta preocupante.

* ¿Es un mensaje totalmente inesperado?
* ¿Proviene del lugar correcto?
* Asegúrese de que está interactuando con contactos confiables confirmando sus identidades. Cuando sea posible, contacte a su remitente directamente para asegurarse de que hayan enviado lo que se recibió.
* Además, compruebe si hay errores ortográficos, cosas extrañas en el logotipo, u otros detalles que puedan indicar que el mensaje sea falso. ¿Esta organización se suele comunicar de esta manera?
* De nuevo, en caso de duda, tome su teléfono y llame al número que usó para llamar (no al número indicado en el mensaje) para obtener más información.

Cualquier archivo adjunto en un mensaje puede ocultar un virus o alguna otra clase de malware, como un ransomware. Un enlace en un mensaje puede llevarle a una página web suplantada, en la cual le roban sus datos o infectan su dispositivo con malware.

Para proteger su dispositivo y sus datos contra ciberamenazas e intentos de intrusión, debe usar un antivirus y hacer respaldos frecuentemente.

Pero también debe usar una solución de correo electrónico seguro para garantizar que los mensajes en su bandeja de entrada no contengan malware u otros elementos malintencionados, para bloquearlos si se da el caso.

Investigación de formas para prevenir

¿Su empresa o escuela tiene procedimientos para ayudar a prevenir la ingeniería social?

Si, tanto para el centro educativo que estoy como para la empresa en donde hago mis prácticas.

Si es así, ¿cuáles son algunos de esos procedimientos?

Para el centro educativo, siempre se recomienda jamás compartir datos relacionados con la universidad a correos no oficiales de la universidad, por ejemplo, correos institucionales, matriculas pertenecientes a la universidad y cuentas bancarias.

Para la empresa se cataloga similar, jamás responder a correos que no sean oficiales de la misma empresa y si es el caso, investigar a los directivos si enviaron o compartieron los correos para recibir información de la empresa. De igual forma, no se comparten información de correos compartidos que se utilicen dentro de la empresa.

* **Utiliza software antimalware y firewalls**Una medida básica para otorgarle a tus redes y dispositivos una capa de protección inicial es el uso de software antimalware y firewalls. Este software es capaz de identificar malware que pudo ser descargado de manera inadvertida durante un ataque de ingeniería social y notificar de su existencia, facilitando su posterior eliminación.
* **Mantén tus sistemas actualizados**El uso de técnicas como el hacking ético y la creación de normativas en materia de ciberseguridad han permitido que las empresas que fabrican software y dispositivos IoT (Internet of Things) identifiquen las vulnerabilidades de sus productos y servicios, y creen actualizaciones que corrigen estas fallas. Por ello, es de suma importancia asegurarse de tener las versiones más actualizadas de programas y aplicaciones para disminuir el riesgo de que un ataque de ingeniería social tenga éxito.
* **Aplica filtros de correo electrónico**Otra medida básica que puede tomarse para frenar los ataques de ingeniería social es optimizar la configuración del correo electrónico empresarial, de manera que los filtros de spam sean más eficientes e impidan que los correos electrónicos de phishing lleguen a la bandeja de entrada. Estos filtros pueden ajustarse para mantener una lista de direcciones de correo electrónico seguras.
* **Desconfía de las solicitudes de datos**Cualquier tipo de comunicación en línea que solicite que ingrese datos confidenciales, probablemente es una estafa. Por ello, siempre es importante que compruebe el remitente antes de compartir información sensible, y que evite interactuar con sitios web sospechosos.
* **Crea políticas de seguridad claras**Toda empresa debería tener su propia política de seguridad, que incluya el uso de contraseñas seguras, doble factor de autenticación y un enfoque de seguridad confianza cero. Estas medidas, en conjunto, pueden limitar en gran medida el impacto de un ataque de ingeniería social.  
  Para crear estas políticas de manera que se adapten a las necesidades reales de tu empresa, lo mejor es asesorarse con expertos en materia de ciberseguridad. Por eso, en Delta Protect ofrecemos un servicio de CISO que pone a tu disposición un equipo multidisciplinario para orientar tus recursos y acciones en dirección a un entorno más seguro.
* **Capacita a los empleados**El consejo más importante de todos probablemente es la formación y concienciación de los empleados, para que logren identificar mensajes sospechosos y eviten caer en las estafas típicas de la ingeniería social. Es imprescindible que todos los empleados conozcan el tipo de datos que pueden compartir sin restricción, el tipo de datos que son confidenciales y los intermedios.

<https://www.metacompliance.com/es/blog/phishing-and-ransomware/5-examples-of-social-engineering-attacks>

Nadeem, M. S. (2024, March 4). ¿Cómo reconocer los ataques de ingeniería social? Mailfence Blog. <https://blog.mailfence.com/es/que-es-la-ingenieria-social/>

Protect, D. (2023, September 20). Ingeniería social: 6 consejos para proteger a tu empresa de su impacto. <https://es.linkedin.com/pulse/ingenier%C3%ADa-social-6-consejos-para-proteger-tu-empresa-de>