ZURICH

Spear Phishing una amenaza derivada del Phishing

¿EL SPEAR PHISHING, ES CONSIDERADO COMO UN NUEVO TIPO DE ESTAFA/FRAUDE INFORMÁTICO?

Sí, efectivamente. Se encuentra considerado como un nuevo tipo de phishing por sus características propias a la hora del modo de operación de esta estafa o fraude informático. Es decir, principalmente, son más sofisticados y en lo que respecta a la utilización de **Ingeniería social**, como técnica psicológica se encuentra personalizada hacia una persona o grupo en particular u organismo determinado.

DIFERENCIA ENTRE EL PHISHING Y SPEAR PHISHING

En el phishing, el ciberdelincuente envía masivamente correos electrónicos cuyo contenido llamativo y/o mensajes de alertas buscando afectar un buen número de víctimas. Sin embargo, el Spear Phishing, es un ataque personalizado y en dónde los correos electrónicos son dirigidos y mantienen una comunicación real con las potenciales víctimas.

FASE DE UN ATAQUE SPEAR PHISHING

El Ciberdelincuente actuará bajo las siguientes fases:

1. La elección del objetivo, puede ser una empresa u organización.
2. El análisis del objetivo, permitirá recopilar la información disponible y la cual podría ser utilizada para algún tipo de ilícito.
3. Se elaboran correos electrónicos falsos y personalizados a un grupo reducidos de víctimas.
4. Se envían correos los cuales podrían contener enlaces direccionados a sitios falsos y/o que contengan archivos adjuntos con malwares.

¿CUÁL ES EL OBJETIVO DE UN SPEAR PHISHING?

Generar **"Puertas traseras"** en el cual permite a los ciberdelincuentes controlando los equipos de manera remota.

Capturar credenciales de las víctimas que pueden ser utilizadas con fines delictivos.

Ejecutar código que podrían ejecutar en equipo infectado y/o descargar nuevos virus informáticos.

Comunicación y envío de información entre equipo y servidores tomando el control.

RECOMENDACIONES PARA EVITAR SER VÍCTIMA DE SPEAR PHISHING

1. Revisar detalladamente el remitente y dominio del correo electrónico, letra por letra.
2. Si te solicita transacciones no habituales o información confidencial, contactar directamente al remitente por otra vía que no sea el correo o el contacto que indica por correo para corroborar la información.
3. No descargues archivos adjuntos de direcciones desconocidas y nunca acceder a los links de remitentes que no estén en tu lista de contactos.
4. Nunca respondas a este tipo de mails.
5. Protección de Dispositivos, manteniendo actualizado el sistema operativo y el antivirus.

El Grupo Zurich y su compromiso actual con la seguridad de la información extiende a todos sus colaboradores y clientes la Cultura organizacional en materias de Ciberseguridad llegando hasta ti.

Recuerda: Que las técnicas utilizadas por los ciberdelincuentes para la Ingeniería social no vulneren tu seguridad ni la de tu familia. Evita ser víctima de fraudes y/o estafas, por eso mantente alerta y sigue nuestras recomendaciones.

#NO ME QUEDO OFF LINE