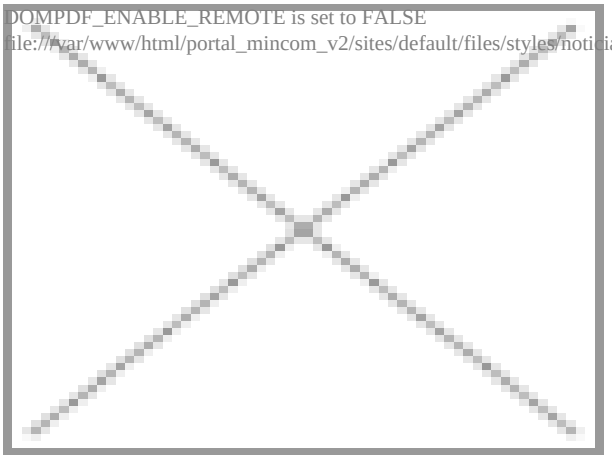

Source:
Tomado de Juventud Rebelde

De la combinación de las técnicas de ingeniería social para estafar a los usuarios y robarles datos sensibles, nacen nuevas modalidades de cibercrímenes.

Cada vez surgen más engaños relacionados con las tendencias de las redes sociales, ingeniería social con criptomonedas, y ya se empieza a hablar de la ingeniería social en el metaverso.

Prepending
La técnica del prepending consiste en agregar el nombre de la víctima al principio de un asunto en un correo electrónico con vistas a lograr una mayor sintonía con esta. Digamos que usted se llame Ramón, y recibe un correo que comienza con su nombre. Lo mismo puede suceder con un post o mensaje en redes sociales. Esta supuesta afinidad busca ganarse la confianza de la persona, y mediante la falsa cercanía, entablar una relación que finalice con la obtención de datos sensibles.

Usurpación de Identidad
El fenómeno de la usurpación de identidad no es exclusivo de internet. Sucede desde hace milenios también en el mundo físico. En el mundo digital el impostor se hará pasar por una persona en específico en aras de acceder a recursos y tener beneficios de sus contactos. Otra intención maliciosa es la de robar la identidad de otra persona para realizar malas acciones y de esta forma manchar su reputación.

La estafa del ultimátum
Es muy común que los usuarios reciban facturas falsas a través del correo electrónico. Si la víctima no se detiene a leer cada detalle, puede pagar el dinero con tal de «salir de ese problema», y terminar con pérdidas monetarias.

Este tipo de correos llega con advertencias, por lo general, de cortes de servicio. Se emplea también para robar credenciales. Por ejemplo, el usuario recibe una supuesta advertencia de su administrador de correo electrónico en su centro de trabajo de que va a expirar su cuenta, y debe reingresar sus datos para evitarlo. Como los clientes de correo muchas veces no muestran con claridad la dirección que envía, el incauto pasa sus señas y ahí viene la debacle. Los atacantes emplean el miedo y el principio de urgencia como un arma.

Credential Harvesting
La cosecha de credenciales, o credential harvesting, consiste en el uso de diferentes técnicas para recopilar contraseñas y posteriormente darles un uso. Una vez que los atacantes tienen contraseñas, tendrán los privilegios en los sistemas que emplean sus víctimas, lo que puede llevar a incrementar el impacto del ataque. Estar concienciado contra el phishing y la verificación en dos pasos (2FA, por sus siglas en inglés) reducirá las posibilidades de que un ataque de este tipo se realice con éxito.

Reconnaissance
Las redes sociales instan a compartir nuestras vidas de una forma pública. En eso hay muchos peligros, pero mencionaré solo dos. Primero, todos los datos que compartimos en redes se convierten en la mayoría de los casos en propiedad de esa red, que los empleará como mercancía.

En segundo lugar, y no menos importante: siempre puede haber alguien interesado en recopilar tus datos para luego atacar. Este método lo emplean mucho los extorsionistas, que poco a poco realizan un seguimiento de la vida pública digital de sus víctimas para atar cabos —quiénes son sus amigos y familiares, dónde vive, qué lugares frecuenta, entre otros—, y así proceder con una extorsión monetaria. Aunque parezca de película, este tipo de ataque es bien frecuente. ¡Cuidado con lo que haces público en internet!

Hoax
Si el término fake news está de moda, los engaños (hoax) no lo son menos. Intentan manipular a la víctima para que haga alguna acción en su equipo que lo deje desprotegido o incluso inservible. Estos ataques se basan una vez más en el miedo. Por ejemplo, el atacante buscará atemorizar a la víctima diciéndole que tiene un virus que le dejará inservible el equipo y que la solución pasa por hacer cambios en la configuración o borrar determinados archivos.

Muchos centros de llamadas falsos emplean este método. El usuario recibe una comunicación telefónica en la que le indican que la compañía X ha detectado un peligro en su ordenador. De ahí pasan a lograr que el atacado entregue el control remoto de su equipo y luego cobran por eso. Generalmente estos ataques se socializan, pues tienen llamadas a la acción para que el usuario comparta el mensaje.

Watering Hole Attack
Muchos depredadores del mundo animal se hacen con sus presas esperándolas próximas a un abrevadero. En inglés se puede decir abrevadero como water hole, y en internet el watering hole attack es un método que toma su nombre del comportamiento de los animales en la naturaleza.

De forma habitual el «ataque en el abrevadero» se ve más en organizaciones empresariales que emplean sistemas de gestión de contenidos (CMS, por sus siglas en inglés) de terceros. El cibercriminal infecta un CMS y después de recopilar información sabe que los empleados de la organización objetivo suelen visitarlo. Al ingresar en el CMS corrupto, el atacante obtiene datos que luego emplea en acciones de ransomware, por ejemplo. El ransomware siempre busca un pago monetario.

Typo Squatting
Aunque se parece al pharming, no es igual. El typo squatting es una técnica que consiste en utilizar un nombre de dominio muy similar al del dominio legítimo, con el fin de poder suplantarlo.

Estas sutiles variaciones suelen coincidir con errores tipográficos de los usuarios. Por ejemplo, en vez de ser juventudrebelde.cu el dominio con typo squatting podría ser juventudreblede.cu. ¿Notó el ligero cambio? De este modo, e imitando la apariencia del sitio web, un usuario podría pensar que está en el legítimo y compartir información sensible, como la que muchas veces piden los formularios.

Estas son algunas de las técnicas más empleadas para realizar ataques de ingeniería social, pero sería un error pensar que los atacantes solo emplearán las aquí mencionadas. Aunque es muy difícil lograr un entorno digital ciento por ciento seguro, conocer los métodos de agresiones y estar alertas es siempre la mejor

manera de prevenir un desenlace desafortunado.

https://bit.ly/3xXFS98 [1]

Links
[1] https://bit.ly/3xXFS98