

Noticias, comentarios y anuncios tecnológicos

En esta edición:

Ingeniería social

Técnicas de engaño
utilizados por delincuentes

Malware

Diferentes tipos de software
que afectan nuestros
equipos y datos

Phishing

Suplantación de la
identidad

Ransomware

El "arte" de la extorsión



<http://pcworld.com.mx/que-es-la-ingenieria-social-y-por-que-debes-conocerlo/>

Ingeniería social

La ingeniería social constituye una serie de prácticas dirigidas a engañar a las personas mediante métodos de convencimiento generalmente amistosos, con el fin de obtener información o datos privilegiados.

Una de las prácticas más habituales constituye la llamada telefónica, en la cual una persona simula ser funcionario de una institución pública o privada, planteando un tema de urgencia o de seguridad que requiere la entrega de información privilegiada. Esta información puede referirse a contraseñas de sistemas informáticos, datos personales o confidenciales, entre otros.

Asimismo, este tipo de engaño puede recibirse a través del correo electrónico, solicitando responder con información puntual, o solicitando ingresar a enlaces que se adjuntan en estos mensajes electrónicos.

En muchas ocasiones, la insistencia es una característica propia de este tipo de actividad. La mejor defensa que podemos interponer es "una sana desconfianza". Ante la menor duda, no dudemos en finalizar este tipo de comunicación de forma inmediata.



Phishing

El phishing o “arte de la pesca”, es otro concepto asociado a la ingeniería social.

Consiste en métodos digitales orientados a engañar a las personas para obtener información confidencial.

El método más común se lleva a cabo a través del correo electrónico, en donde el delincuente se hace pasar por otra persona (suplantación de identidad), solicitando el envío de información personal o reservada, o requiriendo el ingreso a un sitio web específico - que resulta ser un sitio web falso - para el cual hay que ingresar un nombre de usuario y contraseña determinados.

Actualmente, es una práctica dirigida particularmente a obtener ingreso a plataformas bancarias.

Desconfíe de correos electrónicos de desconocidos, de solicitudes sospechosas, y particularmente del ingreso a sitios web que le son remitidos de forma directa, sin que usted haya digitado y corroborado por cuenta propia el enlace web respectivo.

Malware

Es un concepto asociado a “software malicioso”, que básicamente puede robar, encriptar, modificar o destruir la información digital.

Pueden afectar el funcionamiento de un equipo de cómputo al corromper su sistema operativo y aplicaciones de software, interrumpiendo el funcionamiento de un computador.

También, pueden pasar totalmente desapercibidos; sin embargo, funcionando de forma activa para lo que fueron concebidos.

Existen muchos tipos y variedades de malware, cada uno de ellos con características y propósitos muy específicos. Algunos de ellos se conocen como: virus, gusanos, caballos de troya, spyware, keylogger, ransomware, entre otros.

Se aconseja como mínimo la utilización de un software del tipo EDR (Endpoint Detection and Response), que básicamente es un software de protección del computador del tipo “internet security”.



Ransomware

Constituye un tipo de malware que encripta la información de un disco duro, por lo tanto, evita su utilización. Para poder liberarla se solicita un pago a través de la internet, generalmente en criptomoneda, por lo cual su trazabilidad es totalmente anónima.