Ingeniería social y detección de intrusos en *hacking* ético.

Phishing.

Servicio Nacional de Aprendizaje SENA

Phishing.

Los *spammers* suelen enviar correos electrónicos en masa a cuentas de correo electrónico, por ejemplo, los que dicen ser de rifas, juegos y espectáculos en Colombia e informan que ha ganado millones de pesos, le piden que haga clic en un enlace del correo electrónico para proporcionar los datos de su tarjeta de crédito o que introduzca información como su nombre, dirección, edad y ciudad; usando este método, el ingeniero social puede reunir los números de la seguridad social y la información de la red.

Con los intentos de *phishing* a través del teléfono, a veces llamados phishing de voz o *"vishing"*, el phisher llama afirmando representar a su banco local, la policía o incluso la Agencia Tributaria; a continuación, le asustan apelando a su miedo con algún tipo de problema e insisten en que lo solucione inmediatamente facilitando su información de cuenta o pagando una multa; normalmente, le piden que pague con una transferencia bancaria o con tarjetas prepago, porque son imposibles de rastrear.

Phishing vía SMS, o *"smishing"*, es el gemelo malvado del *vishing*, que realiza el mismo tipo de estafa (algunas veces con un enlace malicioso incorporado en el cual hacer clic) por medio de un mensaje de texto SMS.

Una forma de *phishing smishing* es cuando alguien trata de engañarlo para que le dé su información privada a través de un mensaje de texto o SMS. El *smishing* se está convirtiendo en una amenaza emergente y creciente en el mundo de la seguridad en línea.

En pocas palabras, el *smishing* es cualquier tipo de *phishing* que involucra un mensaje de texto; a menudo, esta forma de *phishing* implica un mensaje de texto en un SMS o un número de teléfono. El *smishing* es particularmente aterrador, porque a veces la gente tiende a confiar más en un mensaje de texto que en un correo electrónico. La mayoría de la gente es consciente de los riesgos de seguridad que implica hacer clic en los enlaces de los correos electrónicos; esto es menos cierto cuando se trata de mensajes de texto.

Atacante

Teléfono del usuario (johnny recibe un SMS)

Tracy llamado al 01 8000 911911

Fraude XIM (Atención al cliente del banco)

El *smishing* utiliza elementos de ingeniería social para que usted comparta su información personal, esta táctica aprovecha su confianza para obtener su información. La información que un *smishing* busca puede ser cualquier cosa, desde una contraseña en línea hasta su número de seguro social o la información de su tarjeta de crédito. Una vez que el *smisher* tiene eso, a menudo puede empezar a solicitar un nuevo crédito a su nombre. Ahí es donde realmente va a empezar a tener problemas.

Otra opción que utiliza el *smisher* es decir que si no hace clic en un enlace e introduce su información personal, se le cobrará por día por el uso de un servicio. Si no se ha registrado en el servicio, ignore el mensaje; si ve algún cargo no autorizado en el extracto de su tarjeta de crédito o de débito, llévelo a sus bancos, ellos estarán de su lado.