Fraude y/o *phishing*

Aunque este riesgo pueda estar orientado más a adultos, se incluye como riesgo para los menores ya que dependiendo de la edad, puede tener cuenta de correo, perfiles en redes sociales, cuentas de juegos *on-line*, etc. y pueda ser víctima de este delito.

El *phishing* consiste en el engaño realizado por un ciberdelincuente para ejercer un perjuicio económico al menor y a cualquier persona a través de compras, juegos de azar, apuestas, etc., así como estafas mediante suplantación de identidad para obtener claves o datos personales. El ciberdelincuente suplanta la identidad corporativa de una empresa, pudiendo ser un banco, una empresa de juegos, una red social, en la que tenemos una cuenta creada o no, con la intención de conseguir nuestros datos personales de usuario, contraseña de acceso, cuentas del banco, etc. (SecureKids, 2016).

La forma de *phishing* más utilizada es la que se difunde a través del correo electrónico, aunque últimamente se están utilizando otros canales de comunicación como pueden ser las redes sociales, aplicaciones de mensajería instantánea e incluso mensajes de SMS.

Cualquiera que sea el medio utilizado para intentar la realización de *phishing*, el fin es obtener información confidencial y personal del menor o usuario: nombre, apellidos, direcciones de correo electrónico, numeración de tarjetas de crédito, códigos de acceso a entidades bancarias, etc. así como las credenciales de perfiles de redes sociales, cuentas de juegos on-line, etc. Para conseguir esta información por parte de la víctima utilizan la ingeniería social y de enlaces web que se dirigen a una página web falsa y fraudulenta que aparenta ser la corporativa real de la empresa, utilizando en algunos casos documentos adjuntos, logos de la empresa, etc. para conseguir la adquisición de los datos (OSI – Oficina de Seguridad del Internauta, 2016).

El objetivo de los mensajes fraudulentos, que utilizan los ciberdelincuentes para embaucar a la víctima, es para que el destinatario tome una decisión rápida ya que si no, las consecuencias

pueden ser dañinas o la pérdida de algún beneficio económico o regalo. Utilizan, en algunos casos y sobre todo para los menores, imágenes de juegos, regalos, etc. para llamar más aún la atención y caiga en la tentación de ofrecer sus datos sin saber que van a llegar a manos equivocadas.

Entre muchas técnicas para desarrollar el *phishing* están las siguientes: (OSI – Oficina de Seguridad del Internauta, 2016).

- Aducir problemas de carácter técnico de las empresas que están suplantando.
- Problemas de privacidad en la cuenta de usuario.
- Promoción de nuevos productos de la empresa.
- Premios, regalos o descuentos en productos determinados.
- Desactivación del servicio.

Los mensajes siempre llevarán un fichero adjunto o un enlace a una página web donde puedas introducir tus datos personales para acceder al servicio de la empresa que están suplantando. En muchas ocasiones, estos mensajes pueden contener errores de traducción con faltas de ortografía y errores en la gramática, ya que son traducidos de forma automatizada.

En estas situaciones, que se exponen los menores y adolescentes, pueden servir como vía de acceso más fácil para la consecución de los datos de los progenitores mediante infecciones en los equipos informáticos, tabletas o *smartphones* que se estén utilizando en ese momento.

Bibliografía

- SecureKids. (16 de 06 de 2016). *Secure Kids – Phising, peligro en Internet*. Obtenido de Secure Kids –

Phising, peligro en Internet: https://securekids.es/phishing-dentro-red/

- OSI – Oficina de Seguridad del Internauta. (15 de 03 de 2016). *El phising, la moda que nunca pasa*. Obtenido de El phising, la moda que nunca pasa: https://www.osi.es/es/actualidad/blog/2016/03/15/el-phishing-la-moda-que-nunca-pasa