¿QUÉ SE ENTIENDE POR PHISHING, EJEMPLOS Y CÓMO PREVENIR?

El phishing es un tipo de amenaza donde un maleante intenta obtener de un usuario sus datos personales, claves, cuentas bancarias, número de tarjeta de crédito; o sea todos los datos posibles para luego usarlo de forma fraudulenta.

¿CÓMO LO HACEN?

Los delincuentes suplantan la imagen de una empresa, o entidad pública y de esta manera engañan a la víctima haciéndole creer que los datos solicitados proceden del sitio oficial.

¿CÓMO IDENTIFICAR EL PHISHING?

El phishing se puede practicarlos de varias formas:

- Con un mensaje de texto (SMS) a su teléfono móvil. - la recepción de un mensaje corto donde se solicita sus datos personales. (Ejemplo: Ingrese a este link para confirmar su ID y asegurar su cuenta bancaria https://www.subanco.com)
- Con una llamada telefónica. - puede recibir una llamada telefónica en la que el emisor suplanta a una entidad pública o privada para que usted le facilite datos privados (Ejemplo: ¿Nos podría facilitar los últimos cuatro dígitos de su tarjeta de crédito?)
- Una web que simula una entidad. - es muy utilizada, en ella se simula suplantando visualmente la imagen de una entidad oficial, empresas etc., pareciendo ser las oficiales; el objetivo principal es que el usuario facilite sus datos privados. (Ejemplo: Ingrese a su cuenta a través de este enlace https://www.soytubanco.com)
- Correo electrónico. - el más usado y conocido por los internautas, el procedimiento es la recepción de un correo electrónico donde simulan a la entidad u organismo a la que quieren suplantar para obtener datos del usuario, los datos son solicitados supuestamente por motivos de seguridad, mantenimiento de la entidad, mejorar sus servicios, encuestas, confirmación de su identidad.

¿CÓMO PREVENIR PARA NO SER VÍCTIMA DEL PHISHING?

Tomar en cuenta estos sencillos tips:

- Nunca responda una solicitud de información personal a través de correo electrónico, mensaje de texto o llamada telefónica.
- Las empresas públicas o privadas nunca solicitan datos personales, porque ya los tienen.
- Siempre que acceda a su banca electrónica, correo electrónico, red social o cualquier otro portal, coloque la dirección URL en la barra de direcciones, nunca por links procedentes de cualquier otro sitio, mensaje de texto o correo electrónico.

Las entidades bancarias contienen certificados de seguridad y cifrados seguros, por lo que no se debe tener miedo de usar la banca por internet.

Telf: 2236-092 / Conmutador 3955-900
dnc.direccion@policiaecuador.gob.ec

Autor:
Ing. Edwin Cushicondor - DNTIC