CÓMO ROBAN TU IDENTIDAD EN 5 PASOS

Prevee y dale la vuelta a los correos falsos.

Cuando es detectado un correo apócrifo de alguna Entidad Financiera, la Condusef emite alertas para que no seas víctima de robo de identidad. Adicional a eso te da recomendaciones y te dice qué hacer en caso de caer en este tipo de delito.

Te preguntarás:
¿Cómo obtienen mis datos? ¿Cómo operan?

En todos los casos lo primero que busca el delincuente es crearte incertidumbre si tienes una cuenta en esta institución financiera. Con un discurso como el de "tenemos duda si su cuenta está siendo bien utilizada…" te crean la duda y te "invitan" a que por medio de una liga te dirijas al sitio de la institución para "validar tus datos".

Cabe mencionar que este es un ejemplo pero puede ser cualquier institución financiera, por lo que debes poner mucha atención a la comunicación electrónica que tienes con tu banco, si tienes dudas consulta en una sucursal o por teléfono.

PASO 1

Robarte el código de cliente, para ello el ciberdelincuente envía un correo falso de forma masiva con la finalidad de pescar a una persona que tenga una cuenta en ese banco (cabe mencionar que el correo puede estar a nombre de cualquier banco que ofrezca banca por internet), el correo te invita a verificar tus datos porque el banco supuestamente tiene la duda que no seas tú, al finalizar el mensaje, hay un *link* que debes visitar para comenzar a verificar tu identidad.

Si ingresas, notarás que la página es igualita a la de tu banco (inclusive los banners se mueven y si ingresas a ver productos los puedes consultar), como vas a verificar tu identidad, ingresas tu código de clliente como lo haces de manera habitual, en esta ocasión el ciberdelincuente ya te robó el primer dato para ingresar a tu banca por internet.

PASO 2

Te piden el NIP de acceso, los delincuentes se esfuerzan en generar confianza y para que les sigas entregando información te dejan prácticamente igual la página *web*.

PASO 3

Otro dato que te piden es el NIP dinámico, que genera tu token o dispositivo de seguridad. Sin sospechar les estás proporcionando una clave para realizar operaciones bancarias.

PASO 4

Con el pretexto de actualización de datos también piden tu nombre completo y teléfonos para localizarte. ¡Ten cuidado!, también con eso pueden llamarte derivando en una extorsión.

PASO 5

Los delincuentes cuidan los momentos: te afirman que es un proceso seguro, por lo que no debes dudar de darles tu correo electrónico y la contraseña del mismo. Simplemente no lo hagas, porque también podrán entrar a tu correo personal y obtener más información sobre ti, que pueden utilizar de manera inadecuada y afectarte.

Para darte confianza te "generan" un número de folio con el que podrás hacer referencia cuando por fin contactes a la institución. Cuando lo hagas será demasiado tarde.

Habrán consumado el robo, y comenzarán a saquear tu cuenta de banco, o usarán tus datos telefónicos o de correo de manera inapropiada.

Este es un ejemplo de cómo te pueden afectar, y se las pueden ingeniar para que parezca cualquier institucion financiera. El ejemplo no es exclusivo de ésta institución en particular y pretende darte a conocer imágenes reales de cómo opera la delincuencia, para que estés prevenido y no te dejes engañar.

Recuerda: **NO PROPORCIONES TUS DATOS**, especialmente si tienes duda. Sólo accede a tu institución por medio de la liga oficial, la cual muchas veces viene acompañada de un ícono de candado de seguridad. Ten comunicación con tu institución financiera, es mejor preguntar directamente que ser víctima de la delincuencia.