SPOOFING

¿QUÉ ES ESO?

Los defraudadores siempre buscan nuevas técnicas para obtener un beneficio propio a costa de dañar la economía de terceros. Una de las más actuales es el *spoofing* telefónico, pero, ¿sabes qué es o en qué consiste?

La palabra *spoofing* se puede traducir como "hacerse pasar por otro". En términos de seguridad informática se refiere al uso de técnicas o suplantación de identidad por parte de quien comete el delito.

Al igual que muchos otros fraudes, el *spoofing* es una maniobra usada para intentar obtener información personal valiosa y usarla en actividades ilegales; una de las formas que ha tenido mayor auge es a través del teléfono.

¿CÓMO ES EL *SPOOFING* TELEFÓNICO?

Con el objetivo de ocultar su identidad real, una persona falsifica deliberadamente la información que será transmitida al identificador de llamadas (*CALLER ID,* en inglés) de tu celular. De esta manera, al momento de recibir la llamada, tu pantalla reflejará una identificación manipulada y no la real.

La función del identificador de llamadas, mediante la exhibición del nombre y número, se usa para evitar aquellas que no son solicitadas o deseadas. Sin embargo, los ciberdelincuentes manipulan los datos para hacerse pasar como representantes de bancos, aseguradoras y de otras instituciones de servicios financieros.

Es posible que no identifiques inmediatamente algún intento de *spoofing* telefónico, por eso debes ser cuidadoso cuando te piden dar información personal o bancaria.

Para proteger tus finanzas toma en cuenta las siguientes recomendaciones:

1 Ante cualquier sospecha o llamada inesperada no proporciones información personal, como números de cuentas bancarias, claves de ingreso o cualquier otra que tenga que ver con tus datos.

2 Si recibes la llamada de algún representante de Banco, aseguradora o institución financiera que te pide verificar tus datos personales, interrumpe la llamada y comprueba su autenticidad marcando directamente a la institución.

3 Sé precavido aunque te presionen para entregar información inmediatamente.

4 Recuerda que las instituciones deben exhibir su número telefónico o el de la entidad que representan. Si es posible, deben agregar el nombre de la compañía cuyos productos o servicios están comercializando para que así no tengas ninguna duda de quien llama.

5 Acércate con tu Banco para solicitar los mecanismos de prevención y sistemas de alerta de movimientos, ya que esto te permite detectar de manera inmediata cargos o movimientos extraños en tu cuenta.

En 2017 La CONDUSEF registró 8.7 millones de reclamaciones con impacto monetario a la Banca; 20% más que en 2016.

OTROS TIPOS DE *SPOOFING*

Además del telefónico, existen otras modalidades:

• *Spoofing* de IP

Consiste básicamente en sustituir la dirección IP origen por otra. Este tipo de *spoofing* es usado en un tipo de ataque de inundación conocido también como ataque *smurf*.

•ARP *Spoofing*

Como su nombre lo dice, en este fraude se encargan de suplantar las tramas ARP de tu equipo de cómputo. De esta forma consiguen enviar los equipos atacados a un *host*, para ver, controlar y utilizar los datos de tu máquina.

• DNS *Spoofing*

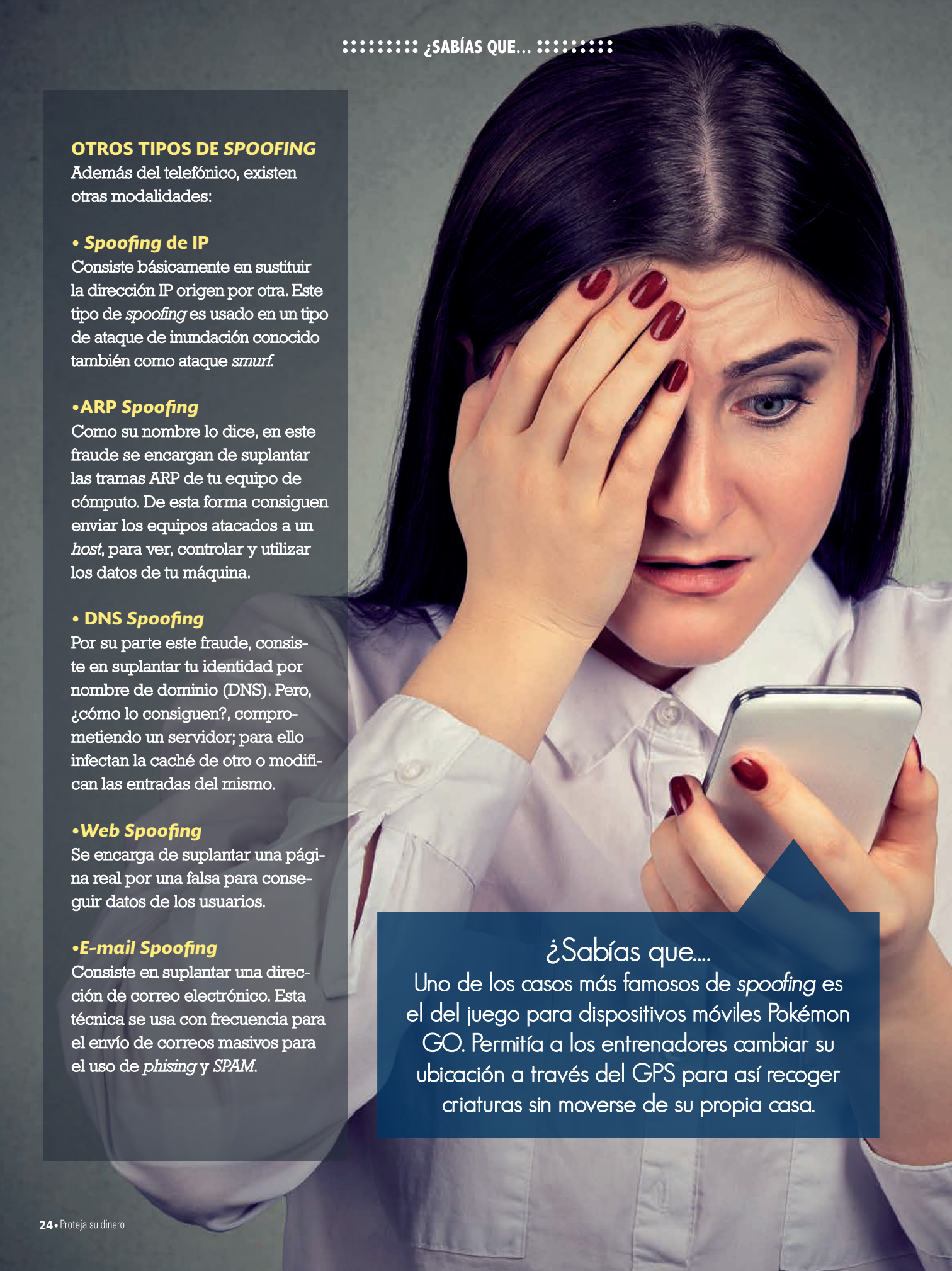
Por su parte este fraude, consiste en suplantar tu identidad por nombre de dominio (DNS). Pero, ¿cómo lo consiguen?, comprometiendo un servidor; para ello infectan la caché de otro o modifican las entradas del mismo.

•*Web Spoofing*

Se encarga de suplantar una página real por una falsa para conseguir datos de los usuarios.

•*E-mail Spoofing*

Consiste en suplantar una dirección de correo electrónico. Esta técnica se usa con frecuencia para el envío de correos masivos para el uso de *phising* y *SPAM*.



¿Sabías que....

Uno de los casos más famosos de *spoofing* es el del juego para dispositivos móviles Pokémon GO. Permitía a los entrenadores cambiar su ubicación a través del GPS para así recoger criaturas sin moverse de su propia casa.