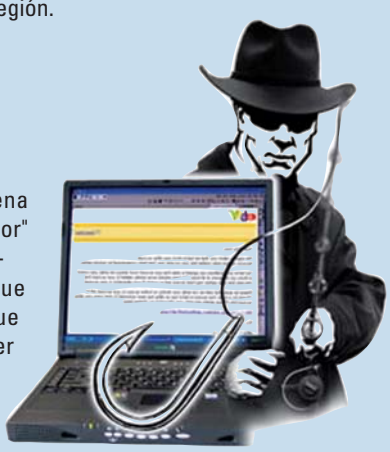
Este fraude tiene unas características muy similares al phising, pero en vez de enviar e-mails se realizan llamadas telefónicas por Internet solicitando los números de las tarjetas de crédito, claves secretas, etc.

¿CÓMO SE LLEVA A CABO ESTE FRAUDE?

El criminal configura un war dialing (técnica consistente en hacer llamadas a una serie de números de teléfono automáticamente con el fin de encontrar módems conectados y permitiendo la conexión con algún otro ordenador) para llamar a números telefónicos en una determinada región.



1er PASO:

- Cuando la llamada es contestada, suena una grabación y alerta al "consumidor" de que su tarjeta de crédito está siendo utilizada de forma fraudulenta y que éste debe llamar al número que sigue inmediatamente. El número puede ser un número gratuito falseado para la compañía financiera que se pretende representar.

2º PASO:

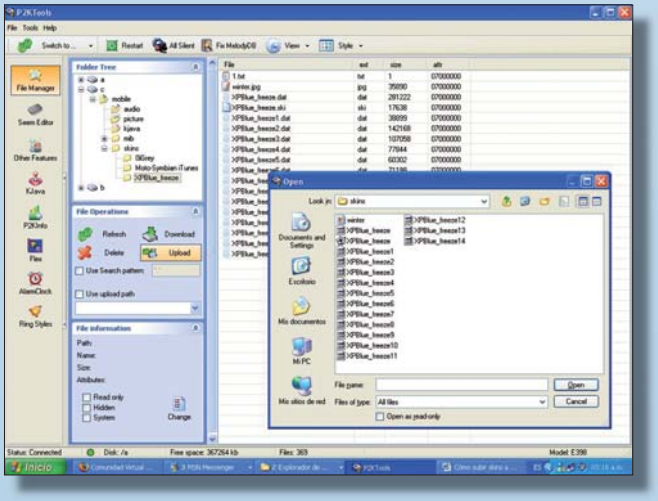
- Cuando la víctima llama a este número, es contestada por una voz computerizada que le indica al "cliente" que su cuenta necesita ser verificada y le requiere que ingrese los 16 dígitos de su tarjeta de crédito.

3er PASO:

- Cuando la persona provee la información de su tarjeta de crédito, el visher tiene toda la información necesaria para realizar cargos fraudulentos a la tarjeta de la víctima.

4a PASO:

- La llamada puede ser también utilizada para obtener detalles adicionales como el PIN de seguridad, la fecha de expiración, el número de cuenta u otra información importante.



Tome nota

Nunca revele sus datos bancarios telefónicamente. Su entidad nunca se los pedirá por esta vía.

Dude cuando conteste al teléfono y suene una grabación, puede ser un fraude.

ADICAE
Asociación de Usuarios de Bancos, Cajas y Seguros