Beware of the

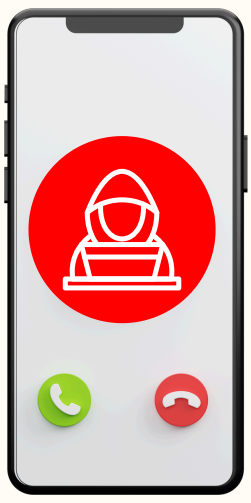
2-Step Cyber Attack

Vishing, or “voice phishing,” occurs when a cybercriminal tries to convince you to provide sensitive information over the phone.

How does it work?

Step 1

The scammer poses as a representative of a legitimate company, claims an urgent issue such as fraud or changes in services, and requests your account information to "help" you.



Step 2

Once they gain your trust, they ask for sensitive information such as account numbers, security codes, or for you to make a transfer to an account that appears to be "safe."

And that's it; with this information, they will have the ability to access your accounts and misuse them.

So before you provide your data, check these red flags...

- Scammers create urgency with issues like fraud or suspended services to rush decisions.
- Personal or financial information, such as passwords and credit card numbers, is requested under the guise of "verification."
- They seek to attract you with irresistible offers or surprise prizes that require the provision of personal data.

⚠️ ⚠️ ⚠️

If you detect any of these signs, end the call and check directly with the institution that supposedly contacted you.

Don't fall into the trap!

YOUR LOGO HERE

Grupo Smartekh | Security Culture Management