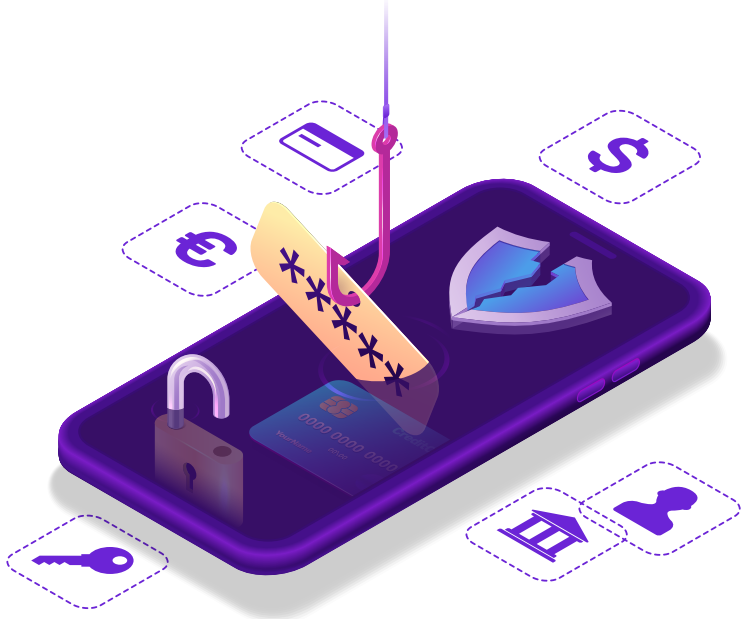
keepnet LABS

Understanding Vishing Attacks

What is Vishing?

Vishing, or voice phishing, is a form of social engineering where fraudsters use phone calls to trick individuals into revealing personal information.



How does Vishing work?

Step 01
The attacker impersonates a legitimate organization or authority.

Step 02
The victim receives a call, often with a sense of urgency.

Step 03
The attacker manipulates the victim into sharing sensitive information.

Common Vishing Scams

Bank Fraud
Attackers pretend to be bank officials to get credit card details.

Tech Support
Scammers claim to be tech support to gain access to your computer.

Tax Scams
Fraudsters pose as tax officials demanding immediate payment.

How to Identify Vishing Attacks

1. **Unrecognized Phone Numbers:** Be wary of calls from numbers you don't recognize.

2. **Urgent Requests:** Scammers often create a sense of urgency to pressure you into sharing information.

3. **Requests for Personal Information:** Legitimate organizations typically don't ask for sensitive information over the phone.

How to Protect Yourself

Never share personal information over the phone unless you initiated the call.

●

If in doubt, hang up and call back using a verified number.

●

Regularly update and maintain security software on your devices.

Reporting Vishing Attacks

Contact your bank or the relevant organization immediately if you suspect you've been a victim of vishing.

●

Report the incident to your local law enforcement agency.

Looking to safeguard your business from vishing threats?
Discover how Keepnet can fortify your defenses by clicking here!