The A-Z of Cybersecurity

Your guide to identifying scams and cyber threats

Fraud

frawd

NOUN

1. deceit, trickery
2. A person who is not what they pretend to be

In the digital world, cybercriminals use **deception and emotional manipulation tactics** to trick people into revealing confidential information or taking actions that can harm them, or their employers, financially.

Phishing

fi·shuhng

EXPLANATION

A social engineering tactic that relies on fraudulent emails to lure recipients into sending money or disclosing confidential information.

Spear phishing

speeuh fi·shuhng

EXPLANATION

A targeted, more personalized form of phishing, where scammers address you by name or claim to represent a company or a person you know.

Whaling

way·luhng

EXPLANATION

A targeted phishing attack that's aimed directly at **corporate executives or other high-ranking individuals**. In other words, the big fish ("whales") in an organization.

Vishing

vish·ing

EXPLANATION

A form of phishing that employs **phone calls or voicemail messages** rather than email.

Smishing

smish·ing

EXPLANATION

Yet another type of phishing that targets potential victims via **SMS (text) messaging**.

Quishing

quish·ing

EXPLANATION

A type of phishing where scammers convince people to **scan a fake QR code** that takes them to a malicious website.

Zishing

zish·ing

EXPLANATION

A phishing technique that takes place on **videoconferencing calls and uses deepfake technology** to fool victims.

Email Spoofing

ee·mayl **spoo**·fuhng

EXPLANATION

When scammers **hide their identity by disguising their email address or display name**, so emails appear to come from someone the recipient recognizes.

Scareware

skeuh·weuh

EXPLANATION

A scareware attack **frightens computer users into installing malicious software or opening virus-infected files**.

Romance or honeypot scam

EXPLANATION

When criminals create **realistic profiles on dating apps and social media platforms and feign romantic interest in potential victims** to ask for money.

What to do after being scammed?

Take Action

Contact your bank and any other businesses that manage your financial accounts to let them know what happened.

Change usernames and passwords, and enable multifactor authentication for digital interactions.

Help future victims by **reporting the crime.**