Photo by Pexels

Human Hacking: The Weakest Link in Cybersecurity

A Simple Guide to Spotting and Stopping People-Based Cyber Attacks

Created By: Fadhl Etty

Table of Contents

Photo by Pexels

1

What Is Social Engineering?

The Art of Human Hacking

- Social engineering is when someone manipulates you into giving up private info.
- It’s not just technology - it’s psychology.
- These attackers don’t hack computers - they hack people.
- **Simple Analogy:** Imagine someone sweet-talking their way into your house pretending to be the plumber.

Photo by Pexels

2

How They Trick You

It Starts with Trust

- Attackers build false trust to get you to let your guard down.
- They might pretend to be your boss, a friend, or tech support.
- They use urgency, fear, or flattery to pressure you.
- **Simple Analogy:** Like a con artist convincing you they’re a long-lost cousin who needs money.

3

Common Types of Attacks

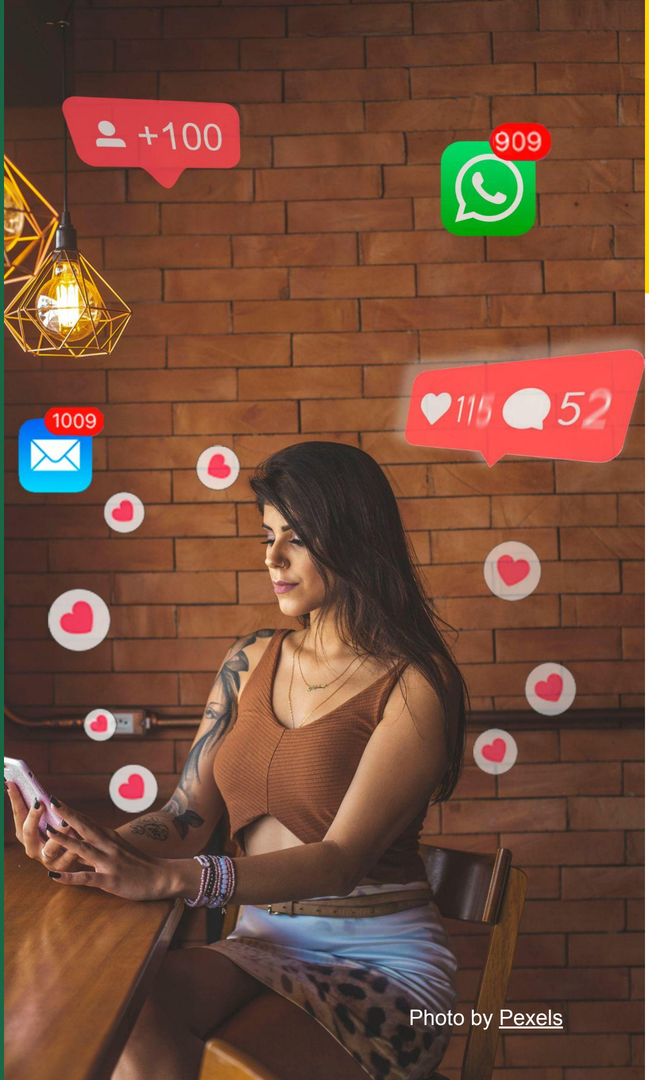
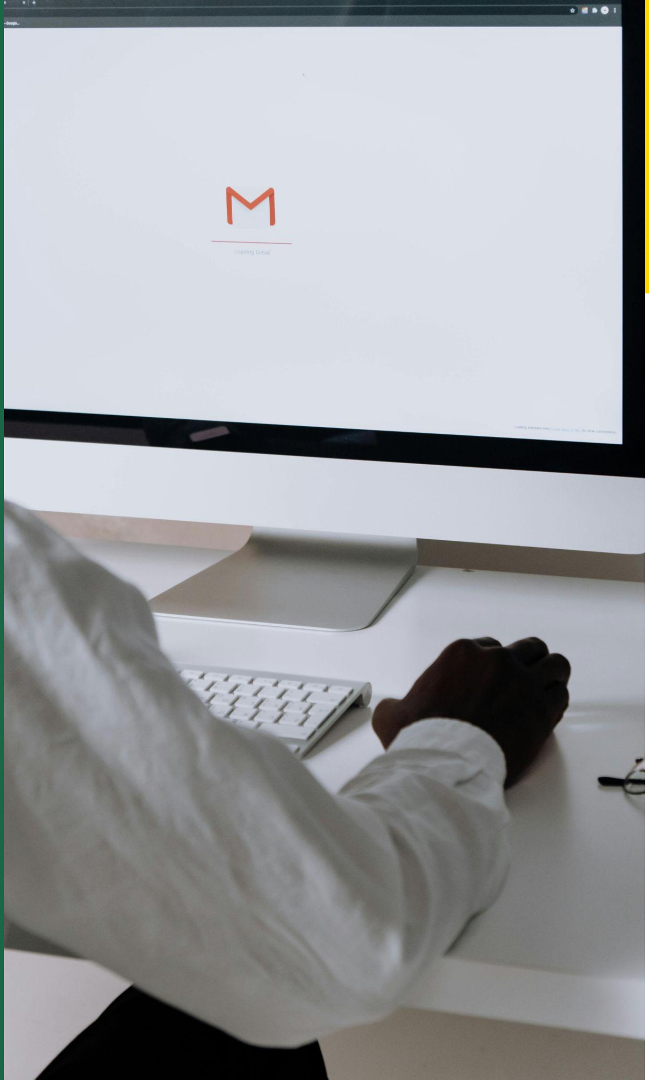


Photo by Pexels

They Come in Many Forms

- Phishing - Fake emails or messages asking for info.
- Vishing - Voice calls pretending to be banks or companies.
- Smishing - Text messages with dangerous links.
- Pretexting - Creating a fake story to get you to reveal secrets.
- Baiting - Leaving USB drives or links for people to “take the bait.”
- **Simple Analogy:** It’s like a magician using misdirection—while you focus on one hand, the other takes your wallet.



4

Spot The Fakes

Quick Checks Before You Click

- Avoid replying directly to the suspicious message.
- Always double-check the sender's email. Scammers tweak real email addresses to fool you. One extra letter can change everything.
- Don’t trust unexpected emails asking for money or information. Call or text the person directly to confirm.
- **Simple Analogy:** It’s like a fake delivery driver wearing a nearly perfect uniform - until you notice the logo is spelled wrong.

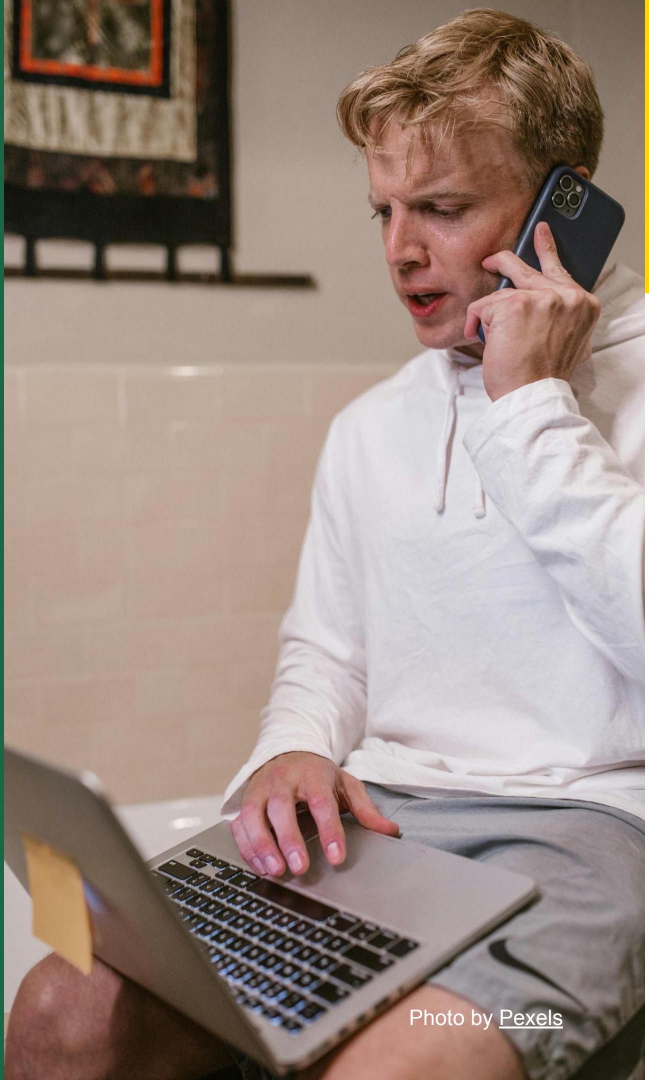


Photo by Pexels

5

What To Do If You Fall for It

Mistakes Happen - Respond Smart

- Don’t panic. Report it immediately to IT or security.
- Turn on two-factor authentication (2FA) and change passwords immediately if unauthorized access is suspected.
- If an account has been hacked, close it quickly after saving important data.
- If a scammer is pretending to be you, tell your clients or coworkers right away so they don’t fall for it.
- **Simple Analogy:** If you lose your wallet, you cancel the cards - same idea with digital security.

6

Staying Mentally Secure

Your Brain Is the Firewall

- Be skeptical - especially of unknown calls, messages, or links.
- Double-check anything that seems suspicious - even if it comes from someone you know.
- Use secure communication methods to verify requests.
- Educate yourself and others.