A HACKER'S SECURITY GUIDE // INFOGRAPHIC 01/08

PHISHING & SCAMS: ANATOMY OF DECEPTION

Attackers impersonate your bank, social networks, or service providers to steal your data and money. Learn to spot the scam before you click.

>> WARNING SIGNS

01 Artificial urgency

"Act now or your account will be locked." They want you to act without thinking.

02 Prizes and easy money

"You won a prize — enter your details to claim it." They exploit greed.

03 Almost-identical address

www.faceb00k.com instead of facebook.com: zeros that look like the letter "o".

04 Shortened links

bit.ly/Ub1XC1 hides the real destination. Your browser may end up on a different site.

05 Unexpected attachments

Files that install malware when opened and steal your data.

06 "Official" design

They use the company's real logos, copy, and look. Looking legit proves nothing.

>> VARIATIONS ON THE SAME SCAM

PHISHING — e-mail

SMISHING — SMS / WhatsApp

QUISHING — fake QR codes on parking meters, in restaurants, and in messages

>> PROTOCOL FOR ANY SUSPICIOUS MESSAGE

1. **Always doubt first**
   Be skeptical of every message you receive, from known senders or not. Think twice before you click.

2. **Don't click or open attachments from strangers**
   Ideally, just ignore them outright.

3. **Never hand over your data by message**
   Legitimate services don't ask for your username and password this way.

4. **Verify through the official channel**
   When in doubt, call the company by phone to confirm whether the message is real.

5. **Inspect the exact address**
   Before entering any data, confirm that the URL matches the real site's address exactly.

GOLDEN RULE

Always doubt, then verify before you trust.