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.

A HACKER'S SECURITY GUIDE // INFOGRAPHIC 02/08

THE PROTECTION LADDER: FROM PASSWORDS TO PASSKEYS

Every level you climb dramatically reduces the odds of having an account stolen.
Find out which step you're standing on today.

>> LEVEL UP

LEVEL 0 — DANGER ZONE

Weak or reused password

Built from personal info, easy to guess, or shared across services: if one is compromised, they all fall.

LEVEL 1

Strong password

Uppercase, lowercase, numbers, and special characters. Use a mnemonic rule: for example, the first letters of a phrase.

LEVEL 2

Unique per service + password manager

A different password for every system. With many accounts, a password manager remembers them for you.

LEVEL 3

Multi-factor authentication (MFA)

A second factor on top of your password: even if it's stolen, it's not enough to get in.

LEVEL 4 — THE GOAL

Passkeys

Passwordless access tied to your device: there's nothing to steal or guess through phishing.

>> RULES THAT APPLY AT EVERY LEVEL

→ Don't share your passwords

If an emergency forced you to share one, change it immediately afterward.

→ Hard security questions

If anyone can answer them using your public info, they're an open door.

→ Don't write them on paper or in files

No notebooks, no phone notes. If there's no other way, keep the paper somewhere very secure.

→ Change them fast after strange activity

If you spot odd activity on an account, change the password right away. And refresh them from time to time without waiting for the system to force you.

WATCH OUT

Make sure no one is watching while you type your password: prying eyes steal passwords too.

A HACKER'S SECURITY GUIDE // INFOGRAPHIC 03/08

YOUR PHONE IS YOUR LIFE: 10 ESSENTIAL PROTECTIONS

Photos, accounts, banking, messages: everything lives on your phone. These ten measures cover theft, loss, malicious apps, and scams.

01 Lock code + auto-lock

Make sure it can only be used with your code or password, and locks itself when you stop using it.

02 Data encryption

Enable encryption for internal storage and for external memory cards.

03 PIN on the SIM card

Without a PIN, your line can be used in another device to receive your verification codes.

04 Remote tracking and wipe

Software that can locate the device and, if needed, lock it and erase its data remotely.

05 Apps from official stores only

They passed vetting by the company and the community. Outside of them, malware territory.

06 Reviews, downloads, and permissions

Check ratings and download counts before installing. If the permissions are excessive, stop: ask someone with experience.

07 Updates current

An up-to-date operating system and apps close known vulnerabilities.

08 Safe charging

Don't charge just anywhere. On public USB ports use protection and charge-only mode, with no data syncing.

09 Discreet screen

A privacy filter against prying eyes and limited notifications while the device is locked.

10 Backups + cleanup

Back up regularly. Move sensitive content to your computer and delete it from the phone.

>> BONUS: TEXT MESSAGE SCAMS

Smishing

The same phishing tricks arrive by SMS and messaging apps: prizes, "problems with your account," package deliveries. Apply the same protocol: doubt, don't click, verify through the official channel.

IF IT'S LOST OR STOLEN

With items 1–4 enabled, your information stays protected even when the device is out of your hands.

A SECURE DIGITAL HOME: WI-FI, IOT, AND COMPUTERS

Threats also reach your home remotely, over the internet and wireless networks.
Four zones to protect.

ZONE 1 The Wi-Fi router

It's the front door to your digital home. Configure it securely by choosing the right options; if you don't know how, ask a technician. An unprotected network lets an intruder reach your devices and data.

ZONE 2 IoT devices

Cameras, smart speakers, plugs, and appliances can become an access channel into your network. Choose and install them carefully, change default passwords, and keep them updated.

ZONE 3 The computers

Preventive maintenance: avoid malware infections and faulty behavior. Active antivirus, an updated system, downloads only from trusted sources.

ZONE 4 Your information

Regular backups: decide which files to protect, where, and how often. The cloud alone is not enough.

>> THE BACKUP PLAN IN 3 QUESTIONS

Q1 What?
The information you can't afford to lose: documents, family photos, work files.

Q2 Where?
Always in more than one place, cloud or not. If the cloud fails or you lose access, the local copy saves you.

Q3 How often?
On a defined, regular schedule, based on how much your information changes. Not "whenever I remember."

THE TWO-PLACES RULE

Anything important lives in at least two places, always. **Everything else is optional; this is not.**

A HACKER'S SECURITY GUIDE // INFOGRAPHIC 05/08

IDENTITY THEFT AND PROTECTING YOUR MONEY

It's one of the fastest-growing crimes in the world: criminals steal your personal data to commit fraud in your name. Recovering is very hard; prevention is the winning move.

>> WHAT ATTACKERS ARE AFTER

- ID DOCUMENTS
- CREDIT AND DEBIT CARDS
- RECEIPTS AND UTILITY BILLS
- YOUR DIGITAL DATA

>> LINE OF DEFENSE: PREVENT → DETECT → REACT

1. **PREVENT — Be careful with your private information**
   Keep your data and personal documents out of other people's hands. Don't post identifying details, shred papers with sensitive information before throwing them out, and hand over your ID only when absolutely necessary.

2. **DETECT — Monitor accounts and cards**
   Review transactions and statements regularly. Unknown charges, however small, are the first sign: attackers test with small amounts before the big hit. Turn on spending alerts if your bank offers them.

3. **REACT — Fast and with professional help**
   If you discover you're a victim: consult a specialist urgently and act immediately to keep the problem from growing. Notify your bank, block your cards, change the passwords of linked accounts.

>> PROTECT YOUR MONEY DAY TO DAY

→ Shop online only on trusted sites
Verify the store's exact address before entering your card.

→ Never give banking details by message or phone
Your bank does not ask for passwords, tokens, or codes through these channels.

→ Keep your cards in sight
In stores and restaurants, never let the plastic leave your field of view.

→ Guard paper as much as digital
Receipts, bills, and statements contain data that can be used to impersonate you.

WHY IT MATTERS

Identity theft is very hard to recover from: they can run up debt and commit crimes in your name.

KIDS SAFE ONLINE: A GUIDE FOR PARENTS AND EDUCATORS

The goal is not to ban technology but to guide: kids may know more about technology than adults do, but not about its risks.

>> THE 3 RISKS YOU NEED TO KNOW

CYBERBULLYING

Peer harassment through digital channels. Ask them to report any harassment or request that feels strange or upsetting.

GROOMING

Adults posing as minors to gain their trust. Verify their contacts; make sure they don't talk to strangers or use their real names in game chats.

SEXTING

Intimate material in circulation. The rule has three parts: don't create it, don't share it, don't ask for it.

>> WHAT TO DO / WHAT TO AVOID

[+] DO

- » Parental controls and usage limits, especially with young children
- » Devices in shared areas of the home, not in bedrooms
- » Open dialogue at home and school about what they see and experience online
- » Teach the risks as part of their education
- » Lead by example: what you do on social media must match what you tell them

[−] AVOID

- × Denying them internet access: it's key to their learning and their future
- × Letting them share identifying data: address, phone number, school
- × Online money transactions before they have the age and judgment to do them safely
- × Assuming they "know more than you": they master the tool, not the danger
- × Monitoring without talking: control without dialogue pushes them into secrecy

>> BY AGE

−10 — **Young children**
Active parental controls, direct supervision, filtered content, limited screen time.

10+ — **Teenagers**
Guided autonomy: fewer filters, more conversation. Make sure they know they can tell you anything without being punished for speaking up.

PASS THIS ON

Take care of your present: in the future it will be your past, and if it's on the internet, anyone will be able to dig it up.

A HACKER'S SECURITY GUIDE // INFOGRAPHIC 07/08

BEEN HACKED? RESPONSE PROTOCOL

Account takeover, fraud, impersonation: what you do in the first hours defines how much damage you take. Follow this order.

1 **DON'T delete anything — preserve the evidence**

Don't delete or forward emails, messages, or any information about the incident. Keep everything that could serve as proof: screenshots, e-mails, conversations.

▼

2 **Report it as soon as possible**

File a report with the police department or prosecutor's office nearest you. A formal report enables the investigation and protects you if crimes are committed in your name.

▼

3 **Cut off the attacker's access**

Urgently change the compromised passwords and those of linked accounts (above all your main e-mail: everything else can be reset from there). Sign out of open sessions on all devices.

▼

4 **Contact the provider through official channels**

Use the service's form, support desk, or phone line. They'll ask for details to verify you're the owner: approximate creation date, frequent contacts, content of recent emails, folders and labels. On free services the response can take a while: be persistent.

>> WHAT NOT TO DO

[−] MISTAKES THAT MAKE EVERYTHING WORSE

- × Hiring a "hacker" to recover the account: it's illegal outside the provider's official channels, and it's usually just another scam
- × Forwarding or spreading the content of the incident
- × Waiting for the law to fix it on its own: the active role in your protection is yours

>> PREVENT TODAY TO RECOVER TOMORROW

TURN ON MFA | SET UP RECOVERY INFO | ADD A SECOND PROFILE ADMIN | BACK UP YOUR PROFILE (DOWNLOAD YOUR DATA)

THE RULE

Evidence first, report fast, new passwords now. In that order, without delay.

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

AWAY FROM HOME: PUBLIC WI-FI, CONNECTIONS, AND TRAVEL

Coffee shops, airports, and hotels are shared territory: networks you don't control and exposed devices. The right habits for each scenario.

>> THREE SCENARIOS, ONE RULE

CAFÉ / MALL

- × No online banking or shopping on third-party Wi-Fi unless you trust the network and its provider
- » When in doubt, use your mobile data
- » Never leave your device alone, not even for a minute

AIRPORT

- × Public USB charging ports: they can sync your data
- » Your own charger in a wall outlet, or charge-only mode with protection
- » Verify the exact name of the official network before connecting

HOTEL

- × Don't leave devices in plain sight in the room
- » Use the safe for whatever you don't carry with you
- » Sessions signed out and device locked at all times

>> BEFORE YOU TRAVEL: DEVICE CHECKLIST

1. **Full backup**
   If the device gets lost or stolen, your information still exists.
2. **Disk encryption enabled**
   An advanced security measure: without your key, the device's contents are unreadable.
3. **Find-my-device turned on**
   Tracking, locking, and remote wipe available from another device.
4. **Travel light on data**
   Carry only what you need on the device: what isn't there can't be stolen.

>> IN ANY PUBLIC PLACE

→ Prying eyes

A privacy filter on your screen, and care when typing passwords around other people: don't make it obvious.

→ Physical safekeeping

Stealing the device itself is still the most common attack. On you or under lock and key, no exceptions.

THE SHARED-TERRITORY RULE

On networks you don't control, behave as if someone were watching. Sometimes someone is.