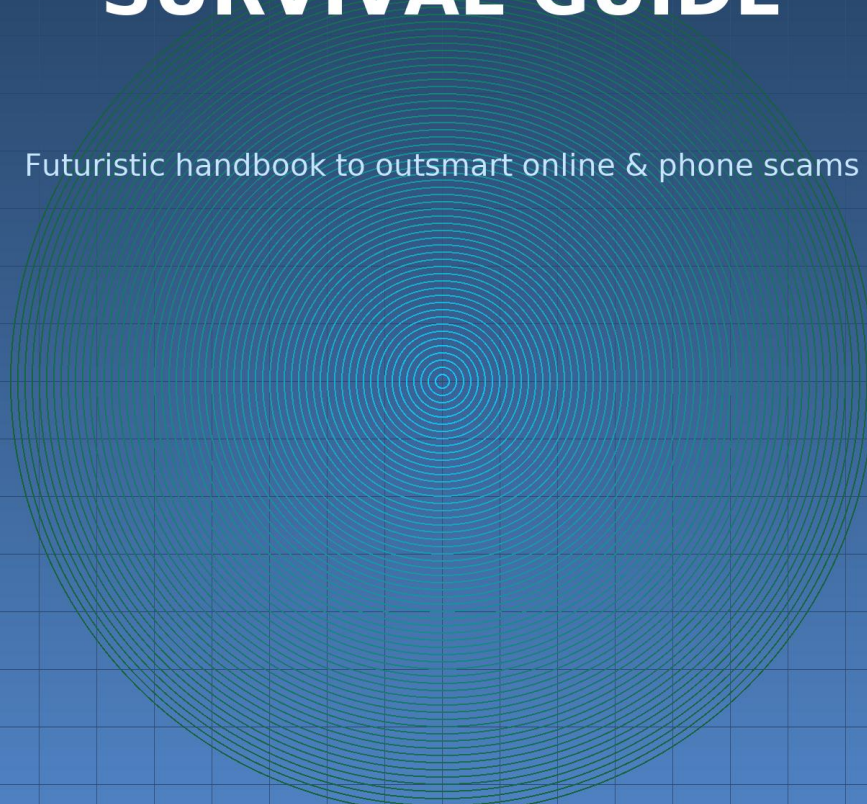


# ANTI-SCAM SURVIVAL GUIDE

Futuristic handbook to outsmart online & phone scams



# ANTI-SCAM SURVIVAL GUIDE

Written with the assistance of Artificial Intelligence  
2025

## Chapter 1 — Basic Security Mindset (How Scammers Think)

### 1.1 Why mindset matters

Most scams succeed not because technology is weak, but because **humans are predictable**. Attackers exploit psychology: fear, urgency, greed, trust, loneliness. Understanding **how scammers think** helps you recognize manipulation before it happens.

---

### 1.2 Core principles of the attacker

- **Opportunistic:** they don't need to know *you*, just that you have an email, a phone, a bank account.
  - **Scalable:** one phishing campaign can reach millions — they only need a tiny % of victims.
  - **Adaptive:** if a trick stops working (e.g., “Nigerian prince”), they rebrand (“parcel delivery,” “bank security alert”).
  - **Low cost, high reward:** sending 1 million scam emails costs less than €50.
  - **Emotion first, logic later:** they trigger panic or excitement so you act without thinking.
- 

### 1.3 Common psychological triggers

- **Urgency:** “Your account will be deleted in 24h!”
  - **Fear:** “Police warrant issued for your arrest unless you pay.”
  - **Greed:** “You won €1 million, claim now.”
  - **Authority:** “This is your bank/government/IT support.”
  - **Secrecy:** “Don't tell anyone, this is confidential.”
  - **Sympathy:** “I'm stranded abroad, please help me.”
- 

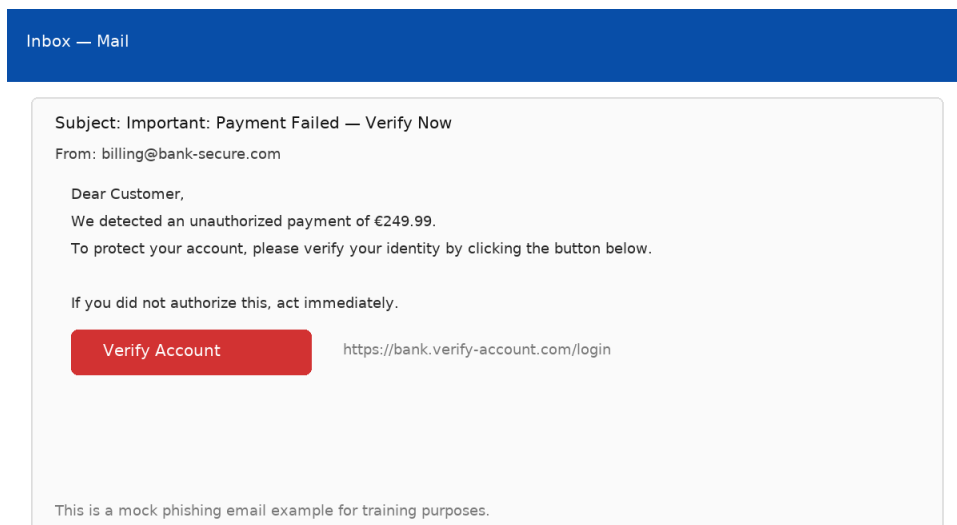
### 1.4 The “attack chain” explained

1. **Initial contact** — Email, SMS, phone call, social media message.
2. **Hook** — Emotional trigger (fear, greed, urgency).

3. **Action request** — Click link, open attachment, provide password, transfer money.
4. **Extraction** — Credentials stolen, malware installed, payment made.
5. **Exploitation** — Accounts hijacked, identity used for fraud, money laundered.

*Analogy:* Think of a phishing attempt like fishing:

- The bait = emotional message.
- The hook = malicious link.
- The catch = your password or money.



---

## 1.5 Key terminology

- **Phishing:** fraudulent messages designed to steal credentials.
- **Vishing:** voice phishing by phone calls.
- **Smishing:** SMS phishing.
- **Social engineering:** manipulating people into breaking normal security.
- **Credential stuffing:** using stolen username/passwords from one breach to try logging into other sites.
- **MFA bypass:** tricking you into giving 2FA codes or using fake login portals.

---

## 1.6 Real-world scam mindset

Example 1 — *Phishing email*:

“Dear customer, your PayPal account is locked. Log in here to restore access: paypal.com.”  
Attackers rely on you not noticing the “l” instead of “I” in the domain.

Example 2 — *Phone scam*:

“This is your bank. Fraud detected. Please confirm your card number and the SMS code we’ll send you.”

They exploit urgency and authority — banks never ask for codes by phone.

---

## 1.7 Defensive mindset

- **Slow down:** scammers want you to act fast — pausing ruins their plan.
- **Verify independently:** don’t trust contact info in the message, use official websites or numbers.
- **Assume attempts are normal:** you *will* receive scams, but awareness is armor.
- **Layer protection:** even if you slip once, MFA, unique passwords, and backups reduce damage.

---

## 1.8 Chapter summary — Takeaways

- Scammers think like marketers but with malicious intent: they sell fear or greed.
  - The attack chain always involves: **Contact → Hook → Action → Exploitation**.
  - Learn key terms (phishing, smishing, vishing, MFA bypass).
    - Adopt defensive habits: slow down, verify, expect scams.
-

## Chapter 2 — Accounts & Credentials

### 2.1 Why accounts are targeted

Your accounts are gateways:

- **Email** = master key (resets other passwords).
- **Banking** = direct money.
- **Social media** = reputation + identity theft.
- **Work accounts** = company data, potential for bigger fraud.

For attackers, **credentials = currency**. Stolen logins are sold on underground forums (“dark web”) for as little as a few dollars each.

---

### 2.2 How passwords get stolen

- **Phishing** — fake login page captures your input.
  - **Keylogging malware** — records what you type.
  - **Data breaches** — large companies hacked (LinkedIn, Yahoo, Adobe). Millions of emails + passwords dumped online.
  - **Credential stuffing** — using leaked passwords from one site to log into another.
  - **Brute force & dictionary attacks** — automated guesses of common passwords.
- 

### 2.3 What makes a strong password?

**Entropy** = randomness. The more unpredictable, the harder to crack.

- “P@ssw0rd!” → 10 characters, predictable substitutions → weak.
- “BlueCactus!movie7\_galaxy” → 24 characters, mixed categories → strong.

**Key rules:**

- Unique per account.
- 16+ characters for critical accounts (bank, email).
- Avoid personal data (birthday, pet names, phone number).

- Don't use common patterns ("123456", "qwerty", "Summer2024").
- 

## 2.4 Password managers

**Definition:** software that generates, stores, and auto-fills strong unique passwords. Vaults are encrypted and unlocked with a single **master password**.

**Benefits:**

- No need to remember dozens of logins.
- Prevents reuse.
- Can audit weak/duplicate passwords.

**Risks & mitigations:**

- If master password is weak → vault compromised. (Solution: use long passphrase + MFA.)
- Cloud-based vaults may be hacked. (Solution: choose reputable manager with zero-knowledge encryption.)

**Examples:** 1Password, Bitwarden, Dashlane, KeePass (local).

---

## 2.5 Multi-Factor Authentication (MFA)

**Definition:** extra step beyond password. Even if password is stolen, attacker can't log in without second factor.

**Types of MFA:**

- **SMS codes:** better than nothing, but vulnerable to SIM swap.
- **Authenticator apps (TOTP):** e.g., Google Authenticator, Authy. Generate time-based codes on device.
- **Push notifications:** e.g., Microsoft/Okta push approve/deny. Beware MFA fatigue (attackers spam until you click approve).
- **Hardware tokens (U2F/WebAuthn):** e.g., YubiKey, Titan Key. Strongest protection, phishing-resistant.

### Best practice order:

Hardware key > Authenticator app > SMS.

---

## 2.6 Account recovery hardening

Attackers often bypass login by resetting your password.

- Remove old recovery emails you no longer use.
  - Set recovery questions to **nonsense answers** stored in your password manager (e.g., “Mother’s maiden name” → “blue\_mango!47”).
  - Check if your email has unauthorized **forwarding rules** (attackers silently copy all mail).
- 

## 2.7 Real-world examples

- **Breached reuse:** If your email + password leaked from Adobe in 2013 and you reused it on PayPal, an attacker could log in years later.
  - **SIM swap:** Criminal convinces your mobile carrier to port your number → intercepts SMS 2FA → drains your bank.
  - **MFA fatigue:** Employee receives 20 login prompts, attacker hopes they click “approve” to stop notifications.
- 

## 2.8 Defensive checklist

- Use password manager for **all accounts**.
  - Enable MFA everywhere.
  - Prefer authenticator app or hardware key, avoid SMS if possible.
  - Rotate weak/reused passwords.
  - Audit accounts on **Have I Been Pwned**.
  - Regularly test account recovery options.
-

## 2.9 Chapter summary — Takeaways

- Passwords alone are **not enough** in 2025.
  - Password manager + MFA = baseline security.
  - Recovery settings are often overlooked but critical.
  - Attackers exploit the weakest link (your old Gmail, your reused Netflix password, your phone number).
-

## Chapter 3 — Email & Messaging (Phishing, SMS, WhatsApp)

### 3.1 Why this matters

Over 90% of successful cyberattacks start with an email or message. It's the easiest way for attackers to reach millions of people cheaply.

- **Email phishing** = fake emails that look like they come from trusted companies.
  - **Smishing** = phishing via SMS.
  - **Vishing** = voice phishing via phone calls.
  - **Messaging app scams** = WhatsApp, Telegram, Messenger with fake investment groups, fake friends, or cloned profiles.
- 

### 3.2 How phishing emails work

They exploit **trust in brand identity**: logos, formatting, sender names.

Steps of a phishing email:

1. **Spoofed sender address** — e.g., support@paypal-secure.com.
  2. **Urgent subject line** — “Your account will be closed in 24 hours.”
  3. **Body with fear/urgency** — “Suspicious login detected in Romania.”
  4. **Malicious link** — fake login page capturing credentials.
  5. **Attachment** — disguised malware (.zip, .docm with macros).
- 

### 3.3 Red flags in emails

- **Generic greeting**: “Dear customer” (banks usually use your name).
- **Strange domain**: paypal.com (with capital i) instead of paypal.com.
- **Misspellings/grammar errors**.
- **Suspicious links**: hover shows mismatch (https://secure-paypal.com instead of https://paypal.com).
- **Unusual attachments**: invoices, resumes, or shipping notices you never requested.

Subject: Important: Payment Failed — Verify Now

From: billing@bank-secure.com

Dear Customer,

We detected an unauthorized payment of €249.99.

To protect your account, please verify your identity by clicking the button below.

If you did not authorize this, act immediately.

Verify Account

<https://bank.verify-account.com/login>

This is a mock phishing email example for training purposes.

---

### 3.4 Realistic phishing email example

**Subject:** *Important: Payment Failed — Verify Now*

**From:** billing@bank-secure.com

**Body:**

Dear Customer,

We detected an unauthorized payment of €249.99. To protect your account, please verify your identity:

[Verify Account Button]

**Why it's malicious:**

- Wrong sender domain.
- Urgent language.
- Link points to bank.verify-account.com/login.

---

### 3.5 Smishing (SMS scams)

Scammers use **short URLs** (bit.ly, tinyurl) because phones don't show full links.

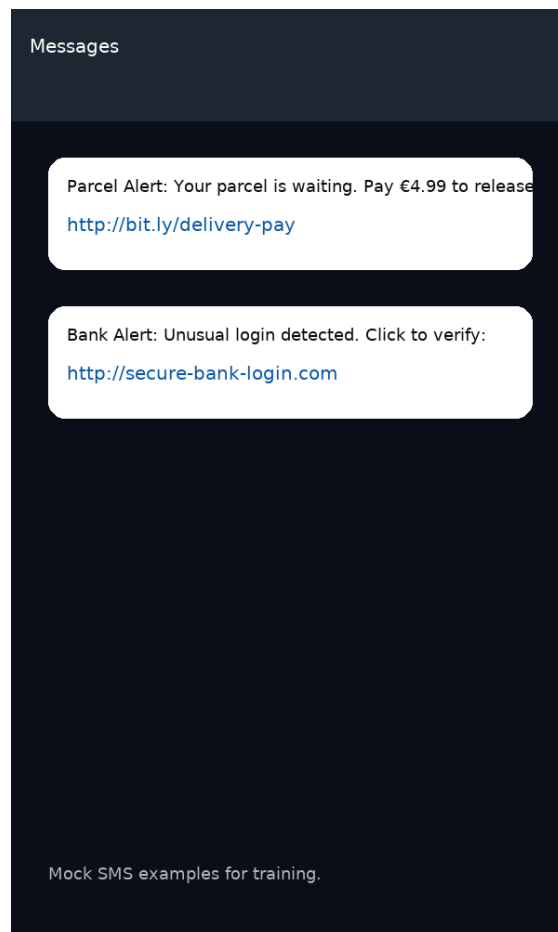
Examples:

- “Your parcel is waiting. Pay €4.99 here: <http://bit.ly/delivery-pay>.”

- “Bank Alert: Unusual login detected. Click <http://secure-bank-login.com>.”
- “Electricity Bill Overdue. Pay now to avoid cutoff.”

**Defense:**

- Don’t click links in SMS.
- Contact courier, bank, or utility via their official app/website.
- Block and report suspicious numbers.



---

### 3.6 WhatsApp & messaging scams

#### Fake investment groups

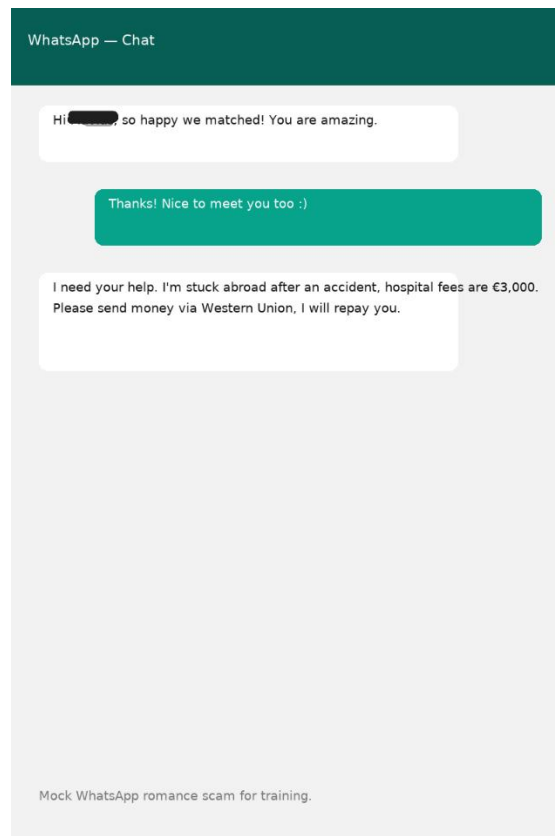
- You’re added to a WhatsApp/Telegram group with people showing fake profits.
- Admin claims “guaranteed 10% daily returns.”

- Victims send money → scammers disappear.

### Impersonation scams

- Attacker clones your friend's profile picture & name.
- Message: "Hey, I changed my number. Can you send me €200 quickly? I'll pay you back."

**Defense:** Always call the friend directly before sending money.



---

### 3.7 Vishing (voice phishing by phone)

Covered more deeply in Chapter 12, but common here:

- "This is your bank's fraud team. Confirm your card number + SMS code."
- "Police warrant — pay immediately to avoid arrest."

---

### 3.8 Advanced: spear phishing

- **Spear phishing** = targeted phishing using personal info.  
Example: “Hello Flavius, I saw your jewelry listings. Please open my attached catalog.”  
→ They researched your business on purpose.

---

### 3.9 Defense strategies

- **Don’t click links** — open official app/site yourself.
- **Don’t trust caller ID** — numbers can be spoofed.
- **Check with sender** — call/email using known contact, not reply button.
- **Verify attachments** — scan with antivirus, never enable macros.
- **Report** — forward phishing emails to your provider (e.g., phishing@company.com).

---

### 3.10 Key terms explained

- **Spoofing:** forging sender’s email or caller ID to look legitimate.
- **Typosquatting:** domains with small changes (micros0ft.com).
- **Macros:** small programs embedded in Office files, often abused to install malware.
- **Social proof:** fake testimonials in WhatsApp groups to build trust.

---

### 3.11 Chapter summary — Takeaways

- Most scams begin with a message — **email, SMS, or chat app**.
  - Learn to spot red flags: urgency, fake domains, suspicious attachments.
  - Defend by slowing down, verifying independently, and refusing to act under pressure.
  - If in doubt — **do nothing** until verified.
-

## Chapter 4 — Browsing, Downloads & Fake Sites

### 4.1 Why the browser matters

The web browser is your **daily gate** to banking, shopping, work, and entertainment. For attackers, it's the easiest entry point:

- Fake websites harvest passwords.
  - Malicious ads (malvertising) deliver malware.
  - Bad extensions spy on you.
- 

### 4.2 Typosquatting & lookalike domains

**Typosquatting** = registering domains that look like popular ones, hoping users mistype.

Examples:

- gooogle.com instead of google.com
- paypal.com (capital “i” instead of “l”)
- faceboook.net

**How to defend:**

- Always type carefully or use **bookmarks** for critical sites (bank, email).
  - Use a password manager: it auto-fills only on the correct domain.
- 

### 4.3 HTTPS padlock myth

- **Reality:** the padlock means the connection is encrypted, not that the site is trustworthy.
- Attackers can easily get free SSL certificates (Let's Encrypt) for fake sites.
- Example: <https://secure-paypal-login.com> may have a padlock but is still fake.

**Defense:** Check the **domain name**, not just the padlock.

---

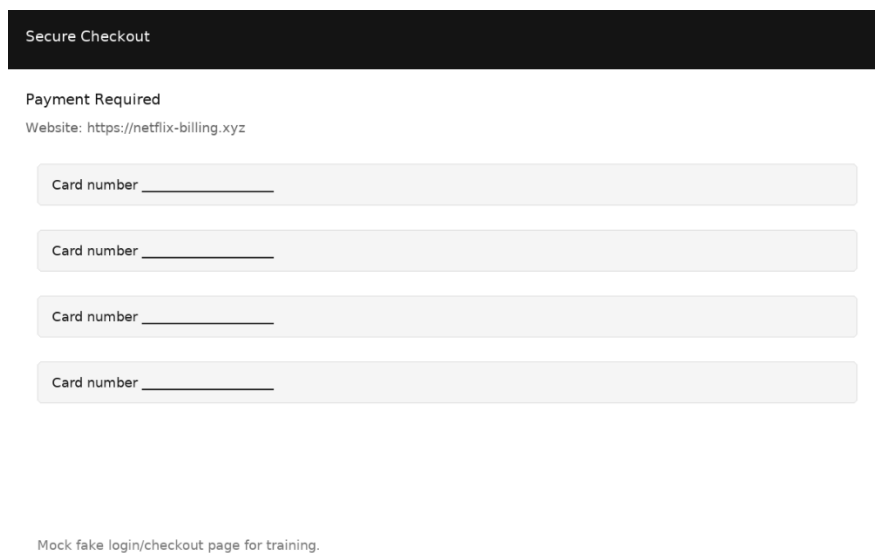
## 4.4 Fake login pages

Phishing sites mimic legitimate logins pixel by pixel.

Trick: they may ask for **extra details** a real site never requests:

- Both your **password and recovery codes**
- SMS 2FA code **and** your backup codes
- Or even ask you to forward codes via email/chat

⚠ Red flag: no real service ever asks you to share 2FA codes outside their app.



The image shows a mockup of a phishing page titled "Secure Checkout". Below the title, it says "Payment Required" and "Website: https://netflix-billing.xyz". There are four identical input fields, each labeled "Card number" followed by a line for text entry. At the bottom of the page, a small note reads "Mock fake login/checkout page for training."

---

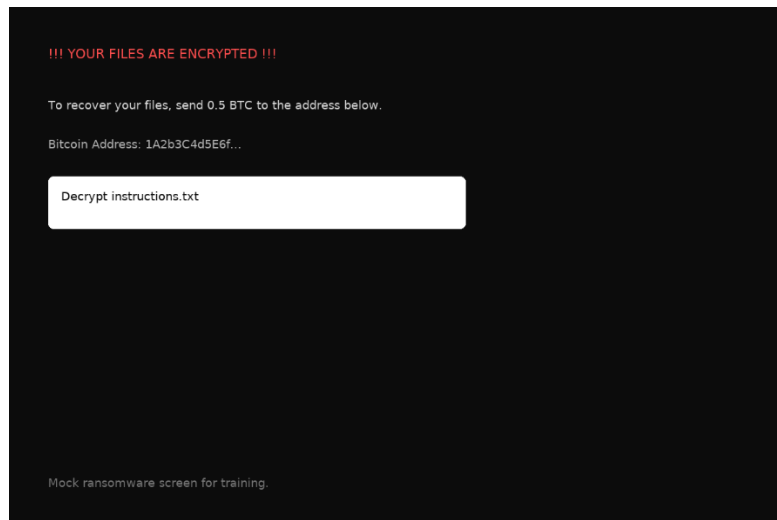
## 4.5 Browser hygiene

- **Remove unnecessary extensions.** Some extensions secretly collect data.
- **Keep browser updated.** Patches close zero-day vulnerabilities.
- **Use separate profiles:**
  - Profile 1 → Banking (no extensions, no history sync).
  - Profile 2 → Work.
  - Profile 3 → Casual browsing.

- **Private browsing ≠ anonymous.** It just doesn't save local history. Your ISP and sites still see you.
- 

#### 4.6 Safe downloads

- **Avoid downloading .exe or .scr** files from emails or untrusted sources.
- **Office files asking to “Enable Macros”** are a huge red flag — macros often install malware.
- **Scan downloads** with antivirus.
- **Mac/Linux** users are not immune — unsigned apps can also carry malware.



---

#### 4.7 Real-world examples

- **Fake Netflix login:** netflix-billing.xyz shows a padlock, looks identical, but steals credentials.
  - **Malvertising:** a fake “Flash Player update” ad delivers ransomware.
  - **Compromised extension:** Chrome extension “Downloader Pro” turned malicious after being sold to attackers.
-

#### 4.8 Key terms explained

- **Typosquatting:** fake domains mimicking real ones.
  - **SSL/TLS:** encryption of data in transit, but says nothing about trustworthiness.
  - **Malvertising:** malicious ads delivering malware.
  - **Macro malware:** malicious code inside Office documents.
- 

#### 4.9 Chapter summary — Takeaways

- Don't trust the **padlock** blindly — check the full domain.
  - Bookmark and use password managers for critical sites.
  - Treat downloads and macros with caution.
  - Segment browsing profiles to minimize exposure.
-

## Chapter 5 — Devices & OS Security

### 5.1 Why device security matters

Even if you have strong passwords and avoid phishing, a **compromised device = compromised everything**.

Attackers aim to:

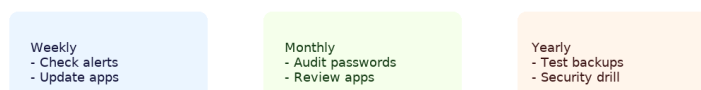
- Steal stored credentials (browsers often save them).
  - Install keyloggers to capture everything you type.
  - Encrypt your files (ransomware).
  - Turn your PC/phone into a bot for future attacks.
- 

### 5.2 Keep everything updated (patching)

- **OS updates** (Windows, macOS, Linux, Android, iOS) fix vulnerabilities.
- **App updates** (browser, office suite, messaging apps) prevent exploitation of old bugs.
- **Driver/firmware updates** close hardware-level flaws.

⚠ Example: *WannaCry ransomware (2017)* spread worldwide because people ignored a Windows patch released months earlier.

Security Routine Timeline



- ✓ Safe practice: Enable auto-updates where possible, or check manually **weekly**.
- 

### 5.3 Full-disk encryption (FDE)

**Definition:** Encrypts your device's storage so data is unreadable without your password.

- Windows → BitLocker
- macOS → FileVault
- iOS/Android → built-in encryption

Benefits:

- If your laptop/phone is stolen, attacker can't access your files.
- Protects sensitive work documents, banking files, saved sessions.

⚠ Without FDE, someone can remove your hard drive and read your data easily.

---

### 5.4 Lock screens & physical security

- Use strong device password/PIN (not 1234, not birthdate).
  - Set auto-lock after 1–5 minutes idle.
  - Avoid biometric-only unlock if someone can force you (finger/face). Combine with PIN.
  - Don't leave laptops/phones unattended in public.
- 

### 5.5 Anti-malware & Endpoint Detection (EDR)

**Anti-malware/antivirus** scans for known threats.

**EDR** (Endpoint Detection & Response) → advanced monitoring for suspicious behavior (used in enterprises).

⚠ Example: A free “cleaner app” on Android secretly recorded keystrokes.

✓ Safe practice: Stick to reputable security solutions (Windows Defender, Malwarebytes, Kaspersky, Bitdefender, etc.).

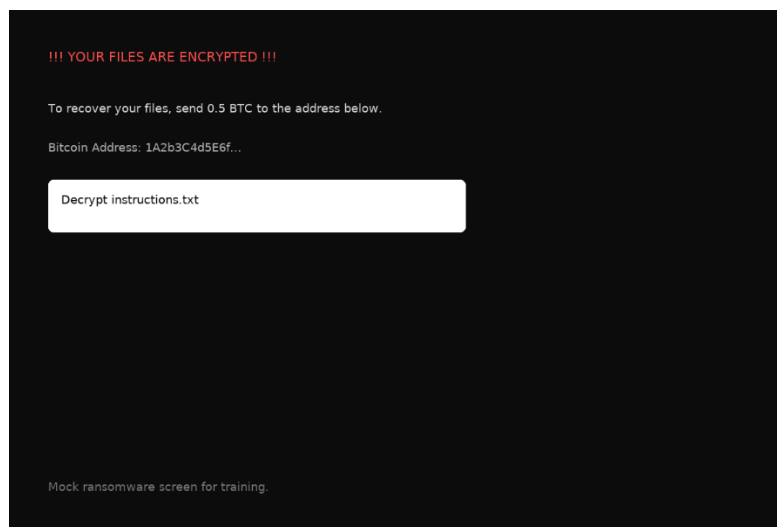
---

## 5.6 Backup strategy — the 3-2-1 rule

- **3 copies** of data: working + 2 backups.
- **2 different media**: e.g., external hard drive + cloud.
- **1 offsite**: in case of fire/theft.

Why: protects against ransomware, accidental deletion, hardware failure.

⚠ Example: Small businesses often pay ransom because backups were stored on the same PC → ransomware encrypted those too.



✅ Safe practice: Keep at least one offline or cloud backup disconnected from daily use.

---

## 5.7 App permissions & audits

On phones especially:

- Many apps request more than they need (flashlight app asking for contacts?).
- Review permissions every 3–6 months.
- Revoke microphone, SMS, camera if unnecessary.

⚠ Example: Some malicious Android apps used **accessibility permissions** to read bank app screens.

---

## 5.8 Key terms explained

- **Patch:** a software update fixing bugs or vulnerabilities.
- **Zero-day:** a vulnerability not yet patched but exploited in the wild.
- **FDE (Full-disk encryption):** encryption that covers entire storage, not just files.
- **Ransomware:** malware that encrypts your files until you pay.
- **EDR:** advanced security monitoring on endpoints (PCs/phones).

---

## 5.9 Chapter summary — Takeaways

- **Update everything:** OS, apps, firmware.
  - **Encrypt your devices** to protect data at rest.
  - **Back up with 3-2-1 rule** — and test restores.
  - **Review app permissions** regularly.
  - **Lock devices physically and digitally.**
-

## Chapter 6 — Payment & Money Safety

### 6.1 Why payment safety matters

When money leaves your account, it's often **gone forever** if you fall victim to a scam. Attackers know financial panic pushes people to act fast. They use:

- Fake invoices
- Investment opportunities
- Marketplace tricks
- Crypto schemes

Understanding safe payment practices drastically reduces risk.

---

### 6.2 Banks & transfers

- **Wire transfers:** fastest, hardest to reverse → scammers' favorite.
- **Red flag:** urgent transfer request via email/phone.
- **Defense:** verify via independent phone number before sending.

⚠ Example: Business email compromise (BEC) → CFO receives spoofed email “Send €25,000 to new supplier account.” Company pays → money laundered overseas.

✅ Safe practice: Always call vendor with the phone number already on file before changing payment details.

---

### 6.3 Credit cards vs debit cards

- **Credit cards:** stronger fraud protection, easier chargebacks.
- **Debit cards:** money comes directly from your account, harder to recover.
- **Virtual cards:** disposable card numbers for one-time purchases (many banks offer this).

⚠ Example: Scammer steals debit card → empties your checking account. Refund takes weeks (if at all).

✅ Safe practice: Use credit card for online purchases, enable alerts for every transaction.

---

## 6.4 Marketplace scams

Common tricks on classifieds (eBay, OLX, Facebook Marketplace):

- **Overpayment scam:** buyer “accidentally” sends too much, asks you to refund the difference. Their payment bounces, you lose money.
- **Shipping scam:** buyer insists on using their own “courier” → fake shipping site, you ship item, never get paid.
- **Too good to be true:** Rolex watch for €200.

⚠ Example: Fake ad for iPhone 14 Pro at half price, “payment upfront to reserve.” Seller disappears.

✅ Safe practice:

- Use **escrow** or built-in marketplace payment methods.
- Meet in person for high-value items (public place, cash/bank transfer on the spot).

---

## 6.5 Investment & Ponzi schemes

Scammers exploit **FOMO (fear of missing out)**:

- “Guaranteed 15% monthly returns.”
- Fake trading platforms with charts showing profits.
- Victims can “withdraw small amounts” early to build trust, then lose big when platform vanishes.

⚠ Example: “Crypto doubling scheme” → send 0.1 BTC, promised 0.2 BTC return. Money stolen instantly.

✅ Safe practice: If it sounds too good to be true, it is. Legitimate investments never guarantee profits.

---

## 6.6 Cryptocurrency-specific risks

- **Irreversible transfers:** no chargebacks like banks.

- **Fake token contracts:** scammers create lookalike tokens.
- **Phishing sites:** fake “MetaMask connect” popups drain wallets.
- **Exchange hacks:** if you keep funds on exchange, you risk losing them.

✓ Safe practice:

- Use **hardware wallets** (Ledger, Trezor).
  - Double-check wallet addresses (use QR, whitelist).
  - Never connect wallet to unknown dApps.
  - Store recovery seed **offline only**.
- 

## 6.7 Refunds & chargebacks

- If scammed via **credit card** → file chargeback quickly.
  - If via **wire transfer** → contact your bank immediately to request recall.
  - If via **crypto** → recovery is nearly impossible (unless scammer is caught).
- 

## 6.8 Key terms explained

- **Escrow:** third-party holds payment until buyer confirms goods received.
  - **Chargeback:** reversal of credit card payment due to fraud/dispute.
  - **Ponzi scheme:** scam where early investors are paid with later investors’ money.
  - **Rug pull:** crypto scam where developers vanish with investors’ funds.
- 

## 6.9 Chapter summary — Takeaways

- **Prefer credit cards** for online shopping, not debit or wire transfers.
- **Use escrow** in marketplaces, never pay outside the platform.
- **No guaranteed returns** — avoid Ponzi/investment scams.
- **Crypto = cash:** treat it as irreversible, protect with hardware wallets.
- Act **fast** if scammed: contact bank immediately.

## Chapter 7 — Social Engineering, Romance & Marketplace Scams

### 7.1 Why social engineering works

Social engineering = **hacking people, not machines.**

Instead of breaking encryption, scammers exploit:

- **Trust** (“I’m your colleague from IT”)
- **Authority** (“This is your bank/police”)
- **Emotion** (love, fear, sympathy)
- **Greed** (“Easy money, fast returns”)

⚠ Even well-trained people can fall for it if the scammer presses the right psychological button.

---

### 7.2 Common patterns in social engineering

1. **Building trust** — attacker engages in casual talk, slowly builds credibility.
  2. **Testing small favors** — “Can you do me a quick favor?”
  3. **Escalation** — once trust is built, comes the real request: money, login, or access.
- 

### 7.3 Romance scams

**How it works:**

- Scammer builds emotional bond on dating apps, Facebook, Instagram.
- Pretends to be a soldier, doctor, engineer abroad.
- After weeks/months of bonding, asks for money for “emergency” (hospital bills, travel, customs fees).

**Red flags:**

- Too much affection too soon (“love bombing”).
- Refuses to video call or meet in person.
- Always has an excuse why they can’t travel.

⚠ Example: A widow in the US lost over \$300,000 to a fake “US Army Captain” stationed overseas.

✅ Safe practice:

- Never send money to someone you haven’t met in person.
  - Verify photos (reverse image search).
  - Involve a trusted friend/family before sending money.
- 

## 7.4 Business Email Compromise (CEO fraud)

**How it works:**

- Attacker spoofs CEO’s email.
- Sends urgent request: “Wire €50,000 to new vendor immediately.”
- Employee obeys due to authority + urgency.

**Red flags:**

- Unusual payment instructions.
- CEO asking directly to bypass procedures.
- “Keep this confidential.”

⚠ Example: In 2020, Toyota subsidiary lost **\$37 million** due to BEC fraud.

✅ Safe practice:

- Always use **dual approval** for large payments.
  - Verify new vendor instructions via phone (using known number, not email).
  - Train staff to question unusual urgent requests.
- 

## 7.5 Job & recruitment scams

**How it works:**

- Fake job offer with high salary, minimal requirements.
- “We’ll hire you immediately, just pay €200 for training/equipment.”

- Or fake check fraud: they send you a check, ask you to deposit it and forward part of it → check bounces, you owe bank.

Jobs — HR

Subject: Immediate Hire — Work From Home (No Experience Needed)

From: hr@amazon-jobs.com

Congratulations! We are pleased to offer you a remote position.

To start, please pay a one-time training fee of €199 to cover setup.

Provide your bank details to receive the contract.

Mock fake job offer for training.

•

### Red flags:

- Job offers without interviews.
- Requests for upfront payments.
- Emails from free domains (gmail, yahoo) instead of corporate addresses.

⚠ Example: Thousands scammed by “Amazon work-from-home jobs” that required buying starter kits.

### ✅ Safe practice:

- Verify employer’s website & HR contact.
- Never pay to get hired.
- Use official career portals.

---

## 7.6 Marketplace manipulation (advanced scams)

- **Sympathy scam:** “Single mom selling laptop cheap, please help.”
- **Escrow fraud:** fake escrow websites created by scammers.
- **Rental scams:** scammers copy real apartment listings, ask deposit upfront.

⚠ Example: College students often lose security deposits to fake rental ads.

✅ Safe practice:

- Visit property in person before paying.
  - Use official marketplace escrow, not links sent by seller.
- 

### 7.7 Key terms explained

- **Social engineering:** psychological manipulation into giving access or money.
  - **Romance scam:** fraud exploiting love and loneliness.
  - **CEO fraud / BEC:** spoofed business emails ordering wire transfers.
  - **Advance fee scam:** asking small payments upfront for a larger promised reward (lottery, job, inheritance).
- 

### 7.8 Chapter summary — Takeaways

- Social engineering targets **emotions, not firewalls**.
- Romance scams: emotional manipulation → financial loss.
- CEO fraud: urgency + authority = big money losses.
- Job scams: if you must pay to get hired, it's fake.
- Always **verify independently** before sending money or sensitive info.

## Chapter 8 — Phone Scam Categories & Examples

### 8.1 Why phone scams are dangerous

Unlike email, phone calls feel **more personal and urgent**. Attackers exploit:

- **Trust in voice** (“it sounds official”).
- **Caller ID spoofing** (faking the bank/police number).
- **Pressure** (keep you on the line until you act).

⚠️ Victims often hand over sensitive info or money because they feel “they’re talking to a real person.”

---

### 8.2 Common categories of phone scams

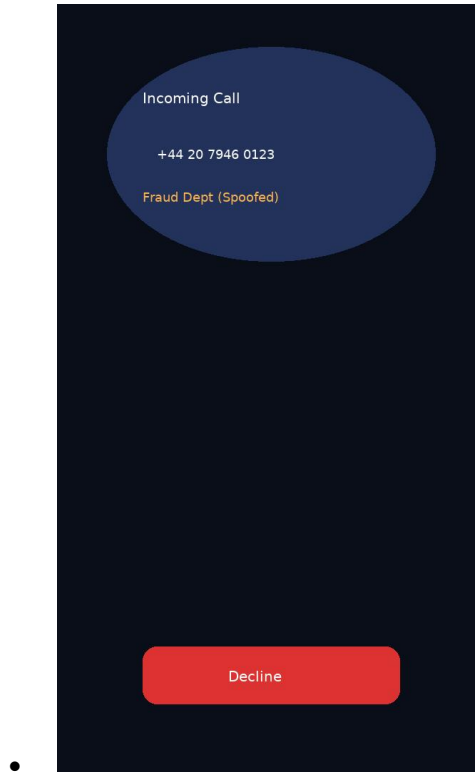
#### 1. Tech support scams

**How it works:** Caller pretends to be from Microsoft, Apple, or your ISP.

- “Your computer has a dangerous virus. If you don’t fix it now, you’ll lose all your files.”
- Asks you to install **remote access software** (TeamViewer, AnyDesk).
- Gains control of your device, installs malware, or demands payment.

#### ✅ **Defense:**

- Big tech companies never call you first.
- Never install remote software at a stranger’s request.
- Hang up immediately.



---

## 2. Bank or credit card fraud impersonation

**How it works:** Caller claims to be your bank's fraud department.

- “We detected a €2,500 transaction. To cancel, please confirm your card number and the SMS code.”
- Once you give the code, they drain your account.

✓ **Defense:**

- Banks never ask for **codes or full card numbers** by phone.
- Hang up, call the number printed on your card.
- Never read verification codes aloud.

---

## 3. Government / tax scams

**How it works:** Caller pretends to be IRS/ANAF/Tax authority.

- “You owe unpaid taxes. Police will arrest you today unless you pay.”

- Demands payment via gift cards, wire, or crypto.

✓ **Defense:**

- Authorities **send letters**, they don't threaten arrest by phone.
  - No government accepts iTunes/Amazon gift cards as tax payment.
  - Hang up and call the official tax agency.
- 

#### 4. Lottery / prize scams

**How it works:** Caller congratulates you:

- “You’ve won a car! Just pay €499 processing fee to claim your prize.”
- After payment, the scammer disappears.

✓ **Defense:**

- If you didn't enter, you didn't win.
  - Legitimate contests never require upfront payment.
- 

#### 5. Grandparent / family emergency scam

**How it works:** Emotional manipulation:

- “Grandma, it's me. I had a car accident, need €1,000 for bail. Don't tell mom.”
- Scammer may know real names from Facebook.

✓ **Defense:**

- Always verify by calling the family member directly.
  - Ask a personal question only the real relative would know.
- 

#### 6. SIM swap scam

**How it works:** Attacker convinces your mobile carrier to “transfer” your number to their SIM.

- Now they receive all your calls and SMS (including 2FA codes).

- Can reset your bank, email, crypto accounts.

✓ **Defense:**

- Ask carrier to add a **PIN/password** to your account.
  - Use **authenticator apps/hardware keys**, not SMS codes.
  - If your phone suddenly loses service, contact your carrier immediately.
- 

## 7. Investment / crypto phone scams

**How it works:** Aggressive cold calls promising huge returns.

- “Our clients earn 15% monthly guaranteed with crypto.”
- Directs you to a fake investment platform with charts showing fake profits.
- You invest more and more, then site vanishes.

✓ **Defense:**

- No legitimate investment guarantees returns.
  - Verify company registration with financial regulator.
  - Never invest based on a cold call.
- 

## 8.3 Common tactics across all phone scams

- **Urgency & fear:** “Act now or lose everything.”
  - **Authority:** “This is the bank / police / tax office.”
  - **Confidentiality:** “Don’t tell anyone, this is secret.”
  - **Isolation:** keep you on the line, prevent you from verifying.
  - **Payment pressure:** always ask for unusual methods (gift cards, wire, crypto).
- 

## 8.4 Defense strategies

1. **Don’t engage** — hang up. Scammers are trained manipulators.
2. **Verify independently** — call your bank/police/family directly.

3. **Block & report** — to your carrier or national fraud hotline.

4. **If info leaked** —

- Card → block immediately.
  - Code/password → change instantly.
  - Remote access granted → disconnect internet, scan/reinstall PC.
- 

## 8.5 Ready-to-use defense scripts

- **Bank scam call defense:**

“I don’t share details over the phone. I’ll call my bank directly. Goodbye.”

- **Tech support scam defense:**

“My IT department handles this. Don’t call again.” [hang up]

- **Family emergency scam defense:**

“I’ll call [relative’s name] directly to confirm.” [hang up]

---

## 8.6 Chapter summary — Takeaways

- Phone scams exploit **urgency + authority + fear**.
  - Caller ID can be faked — don’t trust it.
  - Never give out codes, passwords, or install software on request.
  - Verify independently via official channels.
  - The safest move: **hang up**.
-


## Chapter 9 — Public Wi-Fi, Routers & Home Network Hardening

### 9.1 Why network security matters

Your **network is the highway** all your data travels on.

If attackers control or spy on it, they can:

- Intercept logins and private messages.
- Inject fake sites (man-in-the-middle).
- Hijack devices (IoT, smart cameras, routers).


 A weak home network or unsafe Wi-Fi connection can undermine all your other security measures.


---

### 9.2 Risks of public Wi-Fi

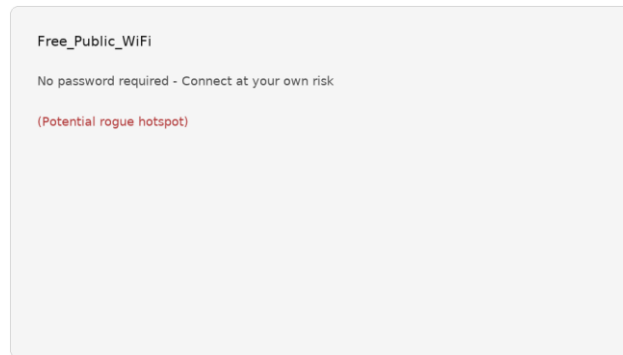
Public hotspots (cafés, airports, hotels) are convenient but risky:

- **Rogue hotspots:** attacker sets up “Free\_Airport\_WiFi” with no password.
- **Sniffing traffic:** unsecured connections expose logins, chats.
- **Session hijacking:** attacker steals cookies to impersonate you.

 Example: A hacker in a café can capture unencrypted logins from anyone using the same hotspot.

 Safe practices:

- Avoid banking or sensitive logins on public Wi-Fi.
- Use a **VPN** (Virtual Private Network) to encrypt traffic.
- Disable **auto-join** for open Wi-Fi networks.
- Turn off Wi-Fi/Bluetooth when not in use.



---

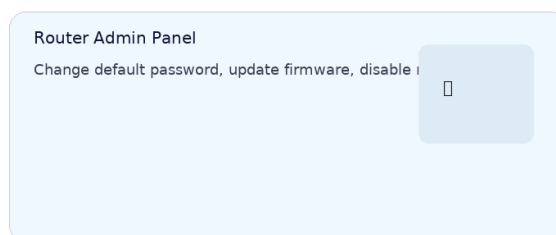
### 9.3 Home router hardening

Your router is the **front door** to your home network. Default settings are often weak.

Steps to secure:

1. **Change default admin password.** Attackers know “admin/admin” defaults.
2. **Update firmware regularly.** Manufacturers patch router vulnerabilities.
3. **Disable remote administration.** Prevents outside logins.
4. **Strong Wi-Fi encryption.** Use **WPA3** (best) or WPA2 with a long passphrase. Avoid WEP (obsolete).
5. **Unique SSID (network name).** Avoid default “TP-Link1234” → easier to target.

⚠ Example: The Mirai botnet (2016) hijacked millions of routers/cameras using default passwords.



---

## 9.4 Guest networks & segmentation

- **Guest network:** separate Wi-Fi for visitors and IoT devices (smart TVs, cameras, Alexa).
- **Segmentation:** if IoT is compromised, it can't access your laptop or bank accounts.

✓ Safe practice:

- Main network → personal devices (PC, phones).
- Guest/IoT network → smart bulbs, TVs, cameras.

---

## 9.5 DNS filtering & security

- **DNS = phonebook of the internet.** Attackers sometimes redirect DNS to fake sites.
- Use secure DNS providers (Cloudflare 1.1.1.1, Quad9 9.9.9.9, Google 8.8.8.8).
- Advanced: run your own DNS filter (e.g., Pi-hole) to block ads, malware, trackers.

⚠ Example: DNS hijack redirects facebook.com to a fake login page.

---

## 9.6 Key terms explained

- **Rogue hotspot:** fake Wi-Fi network set up by attacker.
- **Man-in-the-middle (MITM):** attacker intercepts traffic between you and the website.
- **Firmware:** software inside hardware devices like routers.
- **SSID:** Wi-Fi network name.
- **DNS hijacking:** attacker changes your DNS settings to redirect traffic.

---

## 9.7 Chapter summary — Takeaways

- Public Wi-Fi is **insecure by design** → avoid sensitive logins without VPN.
- Harden your home router: change defaults, update firmware, disable remote admin.

- Use WPA3/WPA2 with strong passwords.
  - Segment IoT devices into a guest network.
  - Use trusted DNS or filtering to block malicious domains.
-

## Chapter 10 — Privacy, Data Minimization & Digital Footprint Cleaning

### 10.1 Why privacy matters

Even if you never fall for a scam email, your **digital footprint** (all traces of your online activity) can be used against you.

Scammers and attackers:

- Collect personal info from social media (birthdays, relatives, address).
- Use it for **identity theft** or **password reset questions**.
- Build a profile to target you with tailored scams (spear phishing).

⚠ Example: Sharing your mother's maiden name on Facebook = free answer to a bank's "security question."

---

### 10.2 What is digital footprint?

Your **digital footprint** = the trail of data you leave online.

Types:

- **Active footprint:** what you post intentionally (social media updates, photos, blogs).
  - **Passive footprint:** data collected silently (cookies, trackers, IP logs).
- 

### 10.3 Risks of oversharing

- **Social engineering fuel:** attackers use personal details to sound convincing.
- **Identity theft:** with your full name, birthday, and address, scammers can open loans in your name.
- **Targeted ads / manipulation:** your browsing data is sold to advertisers and potentially misused.

⚠ Example: A scammer calls pretending to be your cousin abroad, mentioning your vacation from Facebook → feels real.

---

### 10.4 How to minimize exposure

1. **Social media hygiene:**

- Limit who sees your posts (friends only).
- Don't post real-time vacation details → signals empty house.
- Remove birthday, address, school details from public view.

## 2. **Data broker cleanup:**

- Many sites sell personal data (addresses, phone numbers).
- Use services like DeleteMe, Incogni, or request removal manually.

## 3. **Google yourself:**

- Search your name, email, phone number.
- Remove unwanted results (via site owner or Google removal request).

## 4. **Old accounts:**

- Close accounts you no longer use (forums, old emails).
- Less exposure = fewer breach risks.

---

### 10.5 Cleaning trackers

- Use **privacy browsers** (Firefox, Brave).
- Install tracker-blocking extensions (uBlock Origin, Privacy Badger).
- Periodically clear cookies/cache.
- Use private search engines (DuckDuckGo, Startpage).

---

### 10.6 Data breach monitoring

- Use **Have I Been Pwned** to check if your emails/passwords leaked.
- If yes: change password, enable MFA, don't reuse old ones.
- Consider **breach monitoring services** offered by password managers or credit bureaus.

---

### 10.7 Key terms explained

- **Digital footprint:** total online presence (posts, logs, data trails).
  - **Data broker:** company that collects and sells personal data.
  - **Doxxing:** publishing private info online to harm someone.
  - **Identity theft:** using someone's personal data to commit fraud.
- 

## 10.8 Chapter summary — Takeaways

- Attackers thrive on personal info. The less you expose, the safer you are.
  - Manage your social media privacy settings.
  - Remove data from brokers and old accounts.
  - Use tracker-blockers and check breaches regularly.
  - Treat your **personal info like money** — valuable, limited, to be protected.
-

## Chapter 11 — Incident Response: What to Do if You Were Scammed or Hacked

### 11.1 Why response matters

Even the most careful person can slip once. The difference between **losing everything** and **limiting the damage** is **how fast and structured you react**.

Think of incident response as a **fire drill**: panic less, act faster, contain the damage.

---

### 11.2 Step-by-step playbook

#### A. If your account was compromised

1. Use a **clean device** (not the infected one) to change password.
  2. Enable **MFA** immediately.
  3. Log out all sessions → most platforms have “sign out everywhere.”
  4. Check for **forwarding rules or filters** in email (attackers may copy all your mail).
  5. Notify contacts: “My account was hacked, ignore suspicious messages.”
  6. Run malware scan on the compromised device.
- 

#### B. If you sent money

1. Contact your **bank/credit card company immediately**.
    - Request **stop payment** or **recall**.
    - Provide transaction ID.
  2. If wire transfer → call receiving bank’s fraud department.
  3. If credit card → request **chargeback/dispute**.
  4. File a **police report** with all details (messages, screenshots).
  5. Save **every piece of evidence** (emails, chat logs, receipts).
- 

#### C. If your device is infected

1. Disconnect from the internet immediately.

2. Boot in **Safe Mode**.
  3. Run antivirus/anti-malware scan (Malwarebytes, Defender, etc.).
  4. If critical → **reinstall OS** from trusted media.
  5. Restore files only from **clean backup**.
  6. Change passwords only after system is clean.
- 

#### **D. If it's a phishing email/SMS (and you didn't click)**

1. Don't reply, don't click, don't open attachments.
  2. Report as phishing in your email client.
  3. Forward to provider's abuse address (e.g., phishing@paypal.com).
  4. Delete it.
- 

### **11.3 Copy-paste templates**

#### **1. Notify your contacts**

Hi, this is [Your Name]. My account was compromised earlier.

If you received strange messages or payment requests from me, please ignore.

I'm resolving the issue now. Thanks for your patience.

---

#### **2. Dispute a fraudulent transfer with bank**

**Subject:** Urgent — Fraudulent transaction dispute

Dear [Bank Name],

I did not authorize the transfer on [date/time] for [amount].

Please investigate and initiate reversal immediately.

Transaction ID: [ID].

I have filed a police report (ref: [number]) and can provide evidence (emails, screenshots).

Please confirm receipt and next steps.

Regards,

[Your Full Name]

---

### 3. Report phishing to provider

**Subject:** Phishing report — impersonation of [Service]

Hello,

I received a phishing email/SMS on [date] claiming to be from [company].

Sender: [address/number]

Malicious link: [URL]

It attempts to collect credentials/2FA codes.

Please investigate and take down.

Thank you.

---

### 11.4 If identity theft suspected

- Contact credit bureau → freeze your credit.
  - Check for new loans/accounts under your name.
  - File identity theft report with police.
  - Keep a log of every step for insurance/legal purposes.
- 

### 11.5 Incident response mindset

- **Speed is everything.** Every hour counts for recalls/chargebacks.
  - **Don't be ashamed.** Even experts fall for scams — what matters is acting.
  - **Document everything.** Screenshots, dates, names.
  - **Learn & harden.** After recovery, add missing protections (MFA, backups, alerts).
-

## 11.6 Chapter summary — Takeaways

- Don't freeze → follow the playbook step by step.
  - Notify bank, contacts, and authorities immediately.
  - Use templates to save time under stress.
  - After incident, audit and strengthen your defenses.
-

## Chapter 12 — Long Term: Detection, Recovery & Lessons Learned

### 12.1 Why long-term matters

Most people act only after a scam. But real digital resilience comes from **continuous detection & recovery planning**.

Think of it like health: one doctor visit isn't enough — you need regular checkups, prevention, and a lifestyle of protection.

---

### 12.2 Continuous monitoring

- **Account login alerts** → enable notifications for new device logins.
- **Bank/credit alerts** → SMS/email for every transaction.
- **Dark web monitoring** → password managers & credit bureaus often notify if your credentials are found in leaks.
- **Social media alerts** → watch for cloned profiles impersonating you.

 Safe practice: Review all alerts weekly, not just when you get a notification.

---

### 12.3 Periodic audits

Every **3–6 months**, perform a digital hygiene audit:

1. Check saved passwords → update weak ones.
  2. Review recovery options → remove old emails/phones.
  3. Audit app permissions (Google, Facebook, Microsoft).
  4. Remove unused accounts → old accounts = future breaches.
  5. Review payment methods stored online.
- 

### 12.4 Security drills

Just like fire drills, practice **security incident drills** once a year:

- Simulate losing access to your main email → can you recover?
- Pretend your phone is stolen → can you still log in with backups?

- Test restoring from backup → do files open correctly?

⚠ Many companies had backups they never tested — until ransomware hit, and the backups were corrupted.

---

## 12.5 Building resilience

- **Layered security** → password manager + MFA + encrypted devices + backups.
  - **Fail gracefully** → assume one layer might fail, others must protect you.
  - **Minimal trust** → always verify independently, even with colleagues/family.
- 

## 12.6 Learning from incidents

- After a scam attempt, ask:
    - How did they reach me (email, phone, social)?
    - What detail did they know about me?
    - What weak spot did I miss?
  - Adjust defenses accordingly.
  - Share lessons with friends/family → collective awareness = fewer victims.
- 

## 12.7 Security culture (personal & family)

- Teach children and elderly about common scams (grandparent scam, fake jobs, romance scams).
  - Create a family rule: “Never send money or codes without direct phone verification.”
  - Encourage openness → no shame in admitting you almost clicked a phishing link.
- 

## 12.8 Key terms explained

- **Dark web monitoring:** scanning leaked data dumps for your email/passwords.
- **Security posture:** your overall defense level (passwords, devices, habits).

- **Resilience:** ability to recover quickly from incidents.
  - **Defense in depth:** layering multiple protections so one failure doesn't cause disaster.
- 

## 12.9 Chapter summary — Takeaways

- Security is **not one-time**, it's ongoing.
  - Enable alerts for logins, transactions, and leaks.
  - Do regular audits and practice response drills.
  - Build resilience with layered defenses and backup strategies.
  - Share knowledge — collective defense helps everyone.
-

## Chapter 13 — Limitations, Residual Risk & Keeping the Guide Current

### 13.1 Why absolute security doesn't exist

No matter how many defenses you build, **risk can only be reduced, never eliminated.**

Attackers innovate constantly. A strategy that works today may fail tomorrow.

Think of cybersecurity like driving: seatbelts, airbags, and traffic rules reduce risk, but can't make accidents impossible.


---

### 13.2 Residual risks you must accept

- **Zero-days:** vulnerabilities unknown to the vendor, exploited before a patch exists.
  - **Human error:** tiredness, distraction, or stress may cause mistakes.
  - **Insider threats:** scams or leaks from people inside organizations.
  - **Social pressure:** highly convincing scams may bypass even trained individuals.
  - **Irrecoverable losses:** once crypto is transferred, or once wire leaves your account, chances of recovery are near zero.
- 

### 13.3 Trade-offs between security & convenience

- **MFA friction:** slows down logins but prevents account takeover.
- **Password managers:** centralize security but require trust in the software.
- **Backups:** take time and storage, but without them ransomware is devastating.
- **Privacy vs usability:** less data shared means less personalization and convenience.

 **Reflection:** Many users get scammed not because they lacked tools, but because they disabled them for convenience.

---

### 13.4 Keeping defenses up to date

- **Annual review:** revisit this guide once a year. Technology changes, scams evolve.
- **Subscribe to security news:** e.g., Krebs on Security, Schneier on Security, or CERT alerts in your country.
- **Follow trusted institutions:** banks, regulators, consumer protection agencies.

- **Continuous learning:** awareness is your best long-term weapon.
- 

### 13.5 Meta-Fix — keeping yourself future-proof

1. **Accept imperfection:** even if one layer fails, others should minimize damage.
  2. **Stay adaptive:** scams evolve; so must your defenses.
  3. **Teach others:** by sharing awareness, you create a safer environment for family, colleagues, community.
  4. **Document incidents:** your own experiences are the best lessons for the future.
- 

### 13.6 Chapter summary — Takeaways

- No system is 100% safe — goal is **risk management, not elimination**.
  - Accept residual risks: human error, zero-days, irrecoverable transfers.
  - Balance security with convenience, but **never disable protections completely**.
  - Keep defenses **updated and adaptive** through learning and annual reviews.
  - Share lessons — collective awareness strengthens everyone's defense.
-