# The Little Book of Scams

**⚠ Top 10 Scams That'll Empty Your Bank Account**

(And how to laugh in the scammers' faces)

CYBERAWARE UK • FREE RESOURCE

# Welcome, Future Scam-Proof Human

Let's be real — scammers are the used-car salesmen of the internet. They're annoying, they're everywhere, and they *really* want your money. But here's the thing: once you know how they operate, they're actually pretty predictable. Like pigeons in a conga line.

This little book lists the **top 10 scams doing the rounds in the UK right now**, how they work, and — most importantly — exactly what to do to ruin a scammer's day.

Plus we've thrown in a 🛡️ **How Not to Get Hacked** section because knowing the scams is one thing — locking your digital doors is another.

Share it with your nan, your mate who "just made a fortune in crypto" ( ), and anyone else who needs it.

### How to Use This Book

Each scam has: 😈 **The Scam** (how they trick you) → **The Joke** (because if we don't laugh we'll cry) → 🛡️ **The Fix** (what to actually do). Then flip to the **prevention section** for the boring-but-important stuff that keeps you safe.

# The Rogues' Gallery

## #1. Pig Butchering

***"The only pig being slaughtered here is your savings account."***

😈 **How it works:** A friendly stranger slides into your DMs. They're charming. They're interested in your hobbies. Eventually they show you a "sick crypto investment opportunity." You invest. It goes up. You invest more. Then one day — poof. They vanish. The whole "platform" was fake. You've been "fattened up" like a pig, then butchered.

**How to dodge it:**

If a stranger's crypto portfolio looks too good, it's not real — it's a screenshot from Google Images

No legitimate investment opportunity comes from a Tinder match

If you can't withdraw your "profits" — surprise, they were never there

Remember: you wouldn't trust a rando in a pub with your life savings. Same applies to WhatsApp.

## #2. Phishing

***"You've won £50 million! Just send us £99.99 to release the funds. 👍"***

😈 **How it works:** An email arrives. It looks like it's from your bank, or PayPal, or Netflix. It says something scary like "YOUR ACCOUNT HAS BEEN COMPROMISED" and asks you to click a link and "verify your details." The link goes to a fake website that looks real. You type in your password. Congratulations — you just handed your login details to Kevin from Nigeria.

**🛡 How to dodge it:**

- Banks don't send "verify your account" links. They already have your details. Duh.
- Hover your mouse over links before clicking — if the URL looks like "yourbank-secure-login.ru", it's not your bank
- Check for bad grammar: "Dear Customer, your account have been suspensed" — that's a scam, mate
- When in doubt, close the email and go directly to the website yourself (not via the link)

## #3. Smishing (SMS Phishing)

***"Your DPD delivery is waiting! (Said the scammer, definitely not DPD.)"***

😈 **How it works:** Same as phishing, but via text message. You get a text saying your parcel couldn't be delivered, or your account has been locked. Click the link to "reschedule" or "reactivate." The link steals your card details, your personal info, or installs malware.

**🛡 How to dodge it:**

- DPD, Royal Mail, Evri — none of them will ask for your bank details to deliver a parcel
- Never click links in unexpected texts. Go to the actual website and check there
- If you get a scam text, forward it to 7726 — it's free and helps catch the scammers

## #4. Vishing (Voice Phishing)

***"Hello, this is your bank's fraud department. We definitely need your full PIN and sort code. Trust us."***

😈 **How it works:** Your phone rings. Caller ID says it's your bank. A professional-sounding person tells you there's "suspicious activity on your account." They need you to "confirm your details" or "move your money to a safe account." The "safe account" actually belongs to criminals. Bye bye, savings.

**🛡️ How to dodge it:**

Your bank will NEVER ask you to move money to a "safe account." That's not a thing.
Hang up. Call your bank back on the number on the back of your debit card. Not the one they gave you.
If they pressure you or tell you to "stay on the line" — that's a scammer tactic
Remember: real banks don't mind if you take 5 minutes to verify. Scammers panic if you pause.

## #5. CEO Fraud

***"Your boss needs £2,000 in Amazon gift cards. Urgently. Don't tell anyone. — Definitely Your Boss"***

😈 **How it works:** A scammer pretends to be your CEO, director, or manager via email. They ask you to urgently transfer money, buy gift cards, or share sensitive data. The email address looks real — maybe it's slightly off (like "ceo@company.co" instead of "ceo@company.com"). You think it's urgent. You comply. The "CEO" was actually Gary from a basement in Birmingham.

**🛡️ How to dodge it:**

If your CEO really needs gift cards urgently, they'll walk over to your desk. Not email.
Always verify urgent financial requests by phone or in person — using a number you already know
Check the sender email address carefully. One letter off = 100% scam.
Implement a "two-person rule" for any payment over £500

## #6. Romance Scams

***"He's a handsome oil rig worker. She's a beautiful doctor. They both need £500 for a plane ticket to meet you."***

😈 **How it works:** You meet someone online. They're perfect. Funny, attractive, shares your interests. But they're "stuck overseas" for work. After weeks of chatting (and falling for them), they hit an emergency: a medical bill, a stolen passport, a broken laptop. Could you help with £500? Then £1,000? Then £5,000? The person you're in love with is actually a retired man in Lagos named Ade, running six other "relationships" at the same time.

**🛡️ How to dodge it:**

If they've never video-called you but always have an excuse —
Reverse image search their photos. Chances are they're stolen from someone else
Never send money to someone you haven't met in person. Period.
If their story sounds like a Hollywood movie plot, it's because it's made up

## #7. Shopping Scams

***"That £30 PlayStation 5? It's real! (It's a brick in a box. Enjoy.)"***

😈 **How it works:** You find an amazing deal on Facebook Marketplace, Instagram, or a random website. Designer trainers for £20. A PS5 for £30. An iPhone 16 for £50. You pay. Either nothing arrives, or you get a box of rocks. The seller vanishes. The website disappears the next day.

**🛡️ How to dodge it:**

If the price is £30 and it should be £500 — it's not a bargain, it's a scam. Simple.
Pay with a credit card (Section 75 protection) or PayPal Goods & Services — never bank transfer
Check Trustpilot reviews. If the site is 2 days old with no reviews — run.
If the website has more typos than a Year 3 spelling test, don't buy from it

## 💰#8. Investment Scams (aka "Get Rich Quick — For the Scammer")

***"Guaranteed 500% returns! All you have to do is give us your money first. What could go wrong?"***

😈 **How it works:** A slick website, Instagram ad, or WhatsApp group promises "life-changing returns." They show fake testimonials, fancy graphs, and "verified" profit screenshots. You invest £100. The dashboard shows it's now £150! You invest £1,000. Now it's £1,500! You try to withdraw — oh, there's a "technical issue." Or a "minimum withdrawal limit." Or they just disappear with your money. Classic Ponzi scheme.

**🛡 How to dodge it:**

- If someone guarantees returns, they're lying. Even Warren Buffett can't guarantee returns.
- Check if they're FCA-authorised on the FCA register. If not, it's illegal.
- Legitimate investments don't use WhatsApp groups or Instagram DMs to recruit
- Remember: if it sounds too good to be true, your granddad already told you it's a scam

## 🖥#9. Tech Support Scams

***"Hi, I'm calling from Microsoft. Your computer has 47 viruses. We definitely know this without looking at it."***

😈 **How it works:** A pop-up appears on your screen: "YOUR COMPUTER IS INFECTED!" Or your phone rings with "Microsoft Technical Support." They say your computer has viruses and they need remote access to fix it. Once you give them access, they "find" more "problems," charge you hundreds to "fix" them, and sometimes install actual malware or steal your passwords.

**🛡 How to dodge it:**

- Microsoft does not call you. Apple does not call you. No tech company calls you.
- Never give remote access to anyone who calls you unprompted
- That pop-up saying "call this number"? It's the pop-up itself that's the virus. Not your computer.
- Press Ctrl+Alt+Delete or restart your browser if you get a fake virus pop-up

## 🎙️ #10. AI Voice Cloning

***"Mum, I'm in trouble! I need money!" — said the AI, not your actual child.***

😈 **How it works:** Scammers grab 3 seconds of someone's voice from a TikTok, Instagram story, or voicemail. They run it through AI voice cloning software (£50, available online). Then they call you sounding exactly like your panicked child, partner, or parent saying they've been in an accident, arrested, or stranded abroad and need money urgently.

**🛡️ How to dodge it:**

- Have a family code word. If someone calls asking for money, ask for the code word.
- Hang up and call the person back on their real number — not the one that just called you
- Ask a question only the real person would know ("What did we have for dinner last night?")
- Don't post voice notes publicly on social media — that's free training data for scammers

### BONUS: The Golden Rule of Scams

**If someone contacts you out of the blue asking for money, personal details, or remote access to your computer — it's a scam. Full stop. No exceptions. No "but they sounded legit." No "but the website looked real." It. Is. A. Scam.**

⚠ Always report scams to **Action Fraud** (0300 123 2040) or via **actionfraud.police.uk**. If you've lost money, contact your bank immediately on their official number.

# 🏆 Scam Premier League

This week's **standing of the nastiest scams** doing the rounds in the UK. Green arrows? They're on the rise. Red arrows? Cooling off — but still dangerous. Like the Premier League, but with more Nigerian princes.

| # | SCAM | TREND | FORM |
|---|---|---|---|
| | 🎙️AI Voice Cloning ON FIRE | ▲3 | ⬆⬆⬆⬆⬆ |
| 2 | Phishing | ▲1 | ⬆⬆⬆⬆⬇ |
| 3 | Smishing | — 0 | ⬆⬆⬆⬇⬆ |
| 4 | Vishing | ▲2 | ⬆⬆⬆⬆⬆ |
| 5 | Shopping Scams | ▼2 | ⬇⬆⬇⬆⬇ |
| 6 | Pig Butchering HIGH VALUE | ▲1 | ⬆⬆⬆⬇⬆ |
| 7 | Romance Scams | ▼1 | ⬇⬆⬇⬇⬆ |
| 8 | 💰Investment Scams | — 0 | ⬆⬇⬆⬇⬆ |
| 9 | CEO Fraud | ▼3 | ⬇⬇⬇⬆⬇ |
| 10 | 🖥️Tech Support Scams | ▼1 | ⬇⬇⬆⬇⬇ |

▲ Rising ▼ Falling — No change  Hot trend

**🗣️ PUNDIT'S TAKE**

*"AI Voice Cloning has stormed the league! It's come from nowhere and topped the charts — terrifyingly easy and cheap to pull off. Phishing is the Man City of scams: always in the top 3, always dangerous. CEO Fraud is having a shocker — dropped 3 places as companies finally wised up to the 'gift card' trick. But don't let your guard down — one wrong click and they're back."*

# Seasonal Scams Calendar

Scammers love a calendar almost as much as they love your bank details. Every holiday, event, and religious celebration is a **fresh opportunity to trick you**. Here's what to watch for throughout the year.

### Valentine's Day

Fake dating profiles ramp up weeks before. "Can't video call but here's my heart (and my GoFundMe)."

**Never send money to someone you haven't met in person**

**Classic:** "I bought you a gift but it's stuck in customs — can you pay the £50 release fee?"

### Easter

Fake chocolate/Premier Inn deals, "Easter egg delivery" texts (you didn't order any), and charity scams for "Easter meals for kids."

**Only buy from known retailers. Charity scams spike 60% at Easter**

**Classic:** "Your Cadbury order has been delayed — click to reschedule" (from someone who is definitely not Cadbury)

### Ramadan & Eid

Fake charity appeals for "Eid meals for orphans," counterfeit designer clothes for Eid shopping, and phishing emails pretending to be from halal food delivery services.

**Check registered charities on the Charity Commission register. That WhatsApp appeal might not be legit**

**Classic:** "Help orphans in Gaza this Ramadan" link in a WhatsApp forward — goes to a fake donation page

### Back to School

Fake uniform suppliers, "free school meals application" phishing, and laptop/tablet deals that are too good to be true.

**School-related communications should come through the official school system, not random texts**

**Classic:** "Your child's free school meal application needs updating — verify your details here" link

### Christmas

The Super Bowl of scamming. Fake Santas, nonexistent toys, compromised charity pages, "delivery failed" texts from every courier ever, and gift card draining.

**If the toy is half price in November and it's the must-have of the year, it's fake. Full stop.**

**Classic:** "Your Amazon Christmas delivery is stuck — confirm your card to re-deliver" (you didn't order from Amazon)

### Black Friday / Cyber Monday

Fake e-commerce sites pop up like mushrooms. Prices that make no sense. Countdown timers to pressure you. "Only 2 left!" tactics invented by scammers.

**If you've never heard of the website, check Trustpilot AND howlong has that website been online (free tool)**

**Classic:** Facebook ad for a Dyson vacuum at £45 (real price: £350). Site takes your money. Nothing arrives.

## Mother's Day

Fake flower delivery sites, compromised "personalised gift" stores, and "your mum will love this" Instagram ads linking to scam shops.

**Order from florists you know. The cheap bouquet from "bestflowers-uk.ru" won't arrive**

**Classic:** "Your mum's flowers are out for delivery — pay £2.99 delivery fee to confirm" (the flowers don't exist)

## Father's Day

Same as Mother's Day but with tools, gadgets, and suspiciously cheap golf gear. Plus "dads deserve a treat" investment scams targeting older men.

**Tool deals that are 80% off are usually 100% scams. Power tools don't cost £15.**

**Classic:** "Premium whisky gift set — £19.99" ad on Instagram. You get apple juice in a fancy bottle.

**The Golden Rule: If a deal, email, or text mentions a holiday you didn't ask about, it's almost certainly a scam. Scammers surf the calendar. You surf with scepticism.**

# ⛓ The Dark Side: Scam Factories

You might think scammers are just dodgy blokes in hoodies. The reality is darker. **Massive organised crime syndicates** run fake call centres where **trafficked victims are held against their will** and forced to scam people around the world.

| 120,000+ | $75B+ | 50+ |
|---|---|---|
| people estimated trafficked into scam centres in SE Asia | annual revenue from forced-labour scam operations | countries whose citizens have been rescued from these centres |

## How It Works

**Step 1 — The Bait:** A "legit" job ad on social media: customer service rep, IT support, admin assistant. High salary. Free accommodation. Flights paid. The destination? Thailand, Cambodia, Laos, or Myanmar.

✈ **Step 2 — The Trap:** You arrive. They take your passport. You're taken to a guarded compound. Armed security. Barbed wire. No leaving. Welcome to the scam factory.

**Step 3 — The Work:** 14-hour shifts. Scripts for pig butchering, romance scams, crypto fraud. If you don't hit targets? Beatings, electric shocks, solitary confinement. Your "salary" is deducted for food and rent. You'll never see a penny.

**Step 4 — The Cycle:** Can't meet targets? You're "sold" to another centre. Family back home gets ransom demands. Some victims are forced to recruit their own friends. The syndicates are vast,跨国, and deeply connected to organised crime.

MYANMAR — GOLDEN TRIANGLE

### 🏴 Shwe Kokko & KK Park

The largest known scam compounds. Thousands of trafficked workers from across Asia, Africa, and Europe locked in fortified compounds running crypto and romance scams 24/7. Armed guards. Watchtowers. UN investigators have documented mass graves.

🌍 30+ nationalities | 💰 $10B+ stolen | Ongoing UN investigation

CAMBODIA — SIHANOUKVILLE

### 🏗 The Coastal Scam City

Once a tourist town, now dominated by high-rise casino-scam compounds. Workers lured by job ads, then held in buildings with barred windows. Cambodian authorities have raided multiple sites, rescuing hundreds of victims — including UK citizens.

UK victims rescued | 100+ compounds | 🕊 1,200+ rescued 2024-25

LAOS — GOLDEN TRIANGLE SEZ

### The New Frontier

Special Economic Zone that's become a haven for scam operations. Massive casinos surrounded by worker dormitories. Traffickers use debt bondage — victims are told they owe thousands and must "work it off" scamming. Impossible to ever repay.

⚠ Fastest-growing hub | Targets UK & EU | Highly fortified

### 🛡 What This Means for You

The person who just messaged you about a "great crypto opportunity" might not be a villain — they could be a victim, forced to type those messages at gunpoint. **The best thing you can do is not engage**, report the account, and warn others. Every time you ignore, the scam loses. Every time you educate someone, the syndicate loses a potential mark.

# ₿ Crypto Scams — The Wild West

Crypto is like the internet's back alley: exciting, unregulated, and full of people trying to sell you "the next Bitcoin." **Scammers love crypto** because there's no bank to reverse the payment and no regulator to call. Once your crypto is gone, it's gone forever.

**⚠ £300M+ lost to crypto scams in the UK in 2025**

Average loss per victim: £20,000+. Only 1 in 7 victims reports it. The real number is much higher.

🏗

### Rug Pulls

Developers create a shiny new coin, hype it up on social media, you buy in, and then — poof — they drain all the money and vanish. The coin was never real. You were the exit liquidity.

**New coin + anonymous devs + no audit = rug pull**

### Fake Airdrops & Giveaways

"Elon Musk is giving away 10,000 ETH!" No he's not. You send 0.1 ETH to "verify" your wallet and get nothing back. These are everywhere on X/Twitter and YouTube comments.

**The real Elon doesn't ask for your money**

### Fake Trading Platforms

You deposit money into an app that looks like Binance or Coinbase. It shows profits going up. You get excited. You deposit more. Then one day — the app is gone. The whole thing was fake.

**Only use exchanges you can verify are real — app store reviews, regulatory registration**

### Crypto Recovery Scams

Already lost money to a crypto scam? Someone will contact you offering to "recover" your funds — for a fee. They're the **same scammers**, double-dipping. There is no recovery. There's only more loss.

**No one can "recover" crypto. If they say they can, they're lying.**

| | |
|---|---|
| **Phishing (fake wallet sites)** | 41% of crypto losses |
| **Investment fraud (fake platforms)** | **31%** · highest £ loss per victim |
| **Romance + crypto hybrid (pig butchering)** | **18%** · fastest growing |

### The Golden Crypto Rule

If someone you've never met in person is trying to get you to buy crypto, invest in a "sure thing," or send crypto to a wallet address they control — **it's a scam, full stop**. Crypto doesn't make you rich overnight. Scammers do.

# Facebook Ad Scams

Facebook is not just for grandmas sharing minion memes. It is also the **biggest scam ad platform** on the planet. Why? Because targeting is easy, ads look legit, and Meta's automated systems miss most of them.

| 1 in 5 | £1.3B | 70% |
|---|---|---|
| UK adults scammed via social media ads | lost to online shopping scams in 2025 | of social media scams start on Facebook |

### Fake Shopping Ads

That "70% off North Face jacket" you saw in your feed? It's a screenshot of a real jacket. You'll get a polyester rag from China — or nothing at all.

**Check: is the website real? does Trustpilot exist? is the price believable?**

"Premium AirPods Pro — £19.99" → You get one earbud in a broken box

### Fake Celebrity Endorsements

Martin Lewis, Deborah Meaden, Elon Musk, and your local news presenter — all "endorsing" crypto schemes via deepfake videos. They never said that. Their face was stolen.

**If a celebrity is offering you free money, it's a deepfake. Delete and report.**

"Martin Lewis says this government crypto grant is real." (Martin Lewis has sued Facebook over this 5 times.)

### Fake Rental Listings

Beautiful flat, amazing price, landlord is "abroad" so can't show it. Send a deposit to secure it. You arrive — the flat either doesn't exist or is someone else's actual home.

**Never pay a deposit without viewing the property in person. No exceptions.**

"2-bed flat in Zone 1 London — £750/month. Landlord is in Ghana. Send £1,200 deposit to secure."

### Facebook's Problem

Meta makes money from ad views — not from vetting ads. Their automated systems approve millions of ads daily, and scammers slip through constantly. You can report a scam ad and it often stays up for days. **The best filter is your own scepticism.**

# Job Scams — When "Work from Home" Means "Work for Free"

Looking for a job is stressful enough without scammers making it worse. They post fake jobs on LinkedIn, Indeed, Reed, and Facebook — offering **great pay for minimal work**. Sounds amazing? That's the scam.

| £1,200 avg loss per victim | 70% increase in job scams 2025 | Most targeted: 20-35 year olds |
|---|---|---|

### "Pay Us to Get You a Job"

A "recruitment agency" offers you a great role — but you need to pay for "training," "certification," or "background checks" upfront. The job doesn't exist. The fee was the scam.

**Legitimate employers pay you. You don't pay them.**

"Pay £199 for our exclusive job portal access — guaranteed interviews with top companies!" (The portal is a Google Doc.)

### Reshipping / Parcel Mule Scams

"Earn £2,000/month from home! Just receive packages and resend them." You're receiving goods bought with stolen credit cards and shipping them to criminals. **You are now a money laundering accomplice.**

**If a "job" involves receiving and reshipping packages, it's a crime.**

"Admin Assistant needed — just repackage parcels from your home address." (The parcels are bought with stolen cards. You're the fall guy.)

### Mystery Shopper Scams

You're hired as a "mystery shopper." Your first assignment: evaluate a money transfer service. They send you a cheque for £2,000. You deposit it, keep £200 as your fee, and wire £1,800 to "the client." The cheque bounces. The £1,800 was your actual money.

**If they send you money and ask you to send some of it elsewhere, the original payment is fake.**

"We need you to rate Western Union's service. We've sent you £2,000 — send £1,800 to our evaluator and keep £200." (The cheque will bounce in 2 weeks.)

### The Golden Job Rule

Any job that offers huge pay for little work, asks you to pay upfront, involves handling money or packages for other people, or hires you without an interview — **is a scam**. Real jobs are boring. Scam jobs sound amazing. That's how you tell the difference.

# Rental Scams — That Dream Flat Is a Nightmare

Finding a place to rent is hard enough. Scammers know this and **prey on desperate renters** with listings that are too good to be true. Spoiler: they are.

**£1.5M+**
lost to rental scams in UK per year

**£2,300**
average loss per rental scam victim

**40%**
of tenants have encountered a fake listing

**London #1**
most-targeted city for rental fraud

### The Phantom Flat

Beautiful photos, amazing location, suspiciously cheap rent. The "landlord" is abroad, so you can't view it. Pay a deposit to secure it. You arrive — either the flat doesn't exist, or it's someone else's home and they have no idea it was "for rent."

**Never pay a deposit without viewing the property. In person. With a real human.**

"2-bed flat in Shoreditch, £750/month, bills included. Landlord is in Dubai. Send £1,200 deposit via bank transfer." — The flat is a stock photo from a hotel website.

### The Double Let

A genuine rental listing is copied from Rightmove/Zoopla and reposted on Facebook Marketplace or Gumtree at a lower price. Multiple tenants pay deposits for the same flat. One person gets the real flat. Everyone else is out of pocket.

**Check if the same property is listed elsewhere at a higher price — that's the real one.**

Real flat: £1,500/month on Rightmove. "Same" flat: £950/month on Facebook. The Facebook ad is a scam.

### The Key Exchange Trick

"I can't meet you, but I'll courier the keys once you pay the deposit." They send a tracking number. The parcel never arrives (or arrives with a random key that doesn't fit anything). The "landlord" ghosted you.

**Keys before cash. Always. No exceptions.**

"I'm in Scotland for work. Pay the deposit and I'll DHL the keys tomorrow." (The tracking number is fake. The keys don't exist. Your money is gone.)

### How to Rent Safely

1. **View the property** in person or have someone you trust do it. 2. **Use a licensed letting agent** — check they're registered with a redress scheme. 3. **Pay via credit card** (Section 75 protection) or bank transfer to a recognised deposit scheme. 4. **Google the address + "scam"** — see if others have been burned. 5. **If the price is too good to be true**, it's the scam, not the deal of the century.

# You've Been Scammed — Now What?

First thing: **this is not your fault.** Scammers are professionals who trick smart people every single day. Shame is what they rely on — it stops you from reporting it. Don't give them that gift. Here's exactly what to do, step by step.

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Contact your bank immediately | Change passwords | Report to Action Fraud | Tell someone |

### Step 1: Call Your Bank

Right now. Stop reading and call them. Use the number on the back of your card — not any number the scammer gave you. They can freeze accounts, flag transactions, and potentially recall payments made within hours.

**Number on your debit/credit card**

Most banks have 24/7 fraud hotlines. Call immediately — time is everything.

### Step 2: Change Your Passwords

Especially your email and banking passwords. If a scammer has access to your email, they can reset every other password. Use a different device if possible (in case yours is compromised). Turn on 2FA if you haven't already.

### Step 3: Report It

Action Fraud is the UK's national fraud reporting centre. Call them or report online. Even if they can't get your money back, your report helps them track patterns and shut down operations.

**0300 123 2040**

Mon-Fri, 8am-8pm • actionfraud.police.uk (online form 24/7)

Also report to **Cifas** — cifas.org.uk — to add protective registration to your credit file.

### Step 4: Talk to Someone

Scammers rely on shame and secrecy. Tell a friend, family member, or a support service. You are not stupid. You are not alone. Thousands of people get scammed every day — including lawyers, bankers, and police officers.

**Victim Support: 0808 168 9111**

**Free, confidential, 24/7**

Also: Citizens Advice consumer service on 0808 223 1133

### Step 5: Protect Yourself Going Forward

Place a **fraud alert** on your credit file with the three credit reference agencies (Experian, Equifax, TransUnion). This flags any new credit applications in your name so lenders will verify it's really you. Check your credit report for new accounts you didn't open.

**experian.co.uk • equifax.co.uk • transunion.co.uk**

You can check your credit report for free — never pay for it.

### A Message for You

If you've been scammed, you might feel embarrassed, angry, or ashamed. Please don't. The person who scammed you has done this hundreds of times. They know exactly which buttons to press. **You are not the first person they've tricked, and you won't be the last.** What matters now is what you do next: report it, protect yourself, and help someone else avoid the same trap. That's what makes you stronger than the scammer.

### Quick Numbers

**Action Fraud**: 0300 123 2040
**Your Bank**: Number on the back of your card
**Victim Support**: 0808 168 9111 (free, 24/7)
**Citizens Advice**: 0808 223 1133
**Cifas Protective Registration**: cifas.org.uk

# 🎭 Face Swapping & Deepfakes

Remember when photo editing was just giving your friend bunny ears in Photoshop? Now anyone can **swap faces in real-time video calls** using apps that cost less than a takeaway. The technology is terrifyingly good — and terrifyingly easy.

**3 seconds**
of video needed to clone a face

**£20**
cost of face-swapping app

**640%**
rise in deepfake fraud attempts (2024-25)

### How Easy Is It?

You download an app like FaceSwap, DeepFaceLab, or any of a dozen free tools. Upload a few photos of your target (social media gives you hundreds). The AI maps their face. You can now swap it onto a video of yourself in real-time — including on Zoom, FaceTime, or WhatsApp calls. **Total cost: £0-£50. Total time: 10 minutes.**

### What Scammers Do With It

They scrape your selfies, holiday photos, and profile pics from social media. Then they call your mum looking like you, saying you're in trouble and need money. Or they deepfake a CEO on a video call to authorise a fraudulent £200,000 transfer. Or they create fake pornographic content and blackmail you (this is called "sextortion").

**Every photo you post publicly is training data for a deepfake model**

### How to Protect Yourself

1. **Limit what you post** — make social media private. Fewer photos = less fuel for deepfakes.
2. **Use a family code word** — if someone calls looking like your child, ask for the word they'd never share online.
3. **Look for tells** — deepfakes often have weird blinking, mismatched lip sync, or odd skin texture around the edges.
4. **Call back on a known number** — if a "relative" video-calls asking for money, hang up and call their real number.
5. **Watermark your photos** — some tools break deepfake models when faces have watermarks overlaid.

"Mum, I've been arrested in Spain! I need £3,000 bail!" — The face is your son's. The voice is AI-cloned. The call is fake. Your son is at work.

### ⚖ The Law in the UK

Creating a deepfake of someone without consent can be **prosecuted under several laws**. The Online Safety Act 2023 made sharing deepfake intimate images a criminal offence (up to 2 years in prison). The new **Criminal Justice Bill (2025)** goes further — creating a sexually explicit deepfake of someone is now a crime, even if you don't share it. Fraud using deepfakes falls under the Fraud Act 2006 (up to 10 years). But the law is always playing catch-up. **Your best defence is your own awareness.**

# Help & Support Directory

Whether you've been scammed, think you're being targeted, or just want advice — **these organisations exist to help you, not judge you.** All free unless stated.

## 🚔 Reporting & Police

**Action Fraud**
UK's national fraud reporting centre
**0300 123 2040**
actionfraud.police.uk • Mon-Fri 8am-8pm

**Police (Emergency)**
If you're in immediate danger or the scammer is at your door
**999**
Non-emergency: 101

## Banking & Financial

**Your Bank's Fraud Team**
Call the number on the back of your card — they can freeze accounts and potentially recall payments
**Number on your debit/credit card**
Most have 24/7 fraud hotlines. Call immediately.

**FCA (Financial Conduct Authority)**
Check if a financial firm is authorised and report illegal schemes
**0800 111 6768**
fca.org.uk/register • Free

**Cifas Protective Registration**
Flags your credit file — makes it harder for scammers to open accounts in your name
**0330 100 0180**
cifas.org.uk • £25 for 2 years protection

**FSCS (Financial Services Compensation Scheme)**
You may be entitled to compensation if a regulated firm goes bust
**0800 678 1100**
fscs.org.uk • Free

**UK Finance — Banking Fraud**
The banking trade body coordinating fraud prevention across UK banks and payment systems
**ukfinance.org.uk**
Take Five campaign: takefive-stopfraud.org.uk

**Take Five to Stop Fraud**
National campaign backed by UK Finance — Stop, Challenge, Protect
**takefive-stopfraud.org.uk**
Follow #TakeFive on social media

## Emotional Support & Advice

**Victim Support**
Free, confidential support for anyone affected by crime — including fraud
**0808 168 9111**
victimsupport.org.uk • 24/7 • Free

**Citizens Advice**
Consumer advice, debt help, and scam reporting guidance
**0808 223 1133**
citizensadvice.org.uk • Free

**Samaritans**
If you're struggling emotionally after being scammed — they listen, no judgement
**116 123**
samaritans.org • Free, 24/7 • Confidential

**Mind (Mental Health)**
Support if the scam has affected your mental health — anxiety, depression, trauma
**0300 123 3393**
mind.org.uk • Mon-Fri 9am-6pm

## Cyber Security Advice

**NCSC (National Cyber Security Centre)**
Official UK government cyber security advice — how to stay safe and report issues
**ncsc.gov.uk**
Report phishing: report@phishing.gov.uk • Free

**Get Safe Online**
Practical guides on staying safe online — from passwords to social media privacy
**getsafeonline.org**
Free guides and resources

## Age-Specific Support

**Age UK**
Fraud advice and support tailored for older people — the most targeted age group
**0800 678 1174**
ageuk.org.uk • Free • 8am-7pm

**Stop Scams UK**
Partnership of banks, telecoms, and tech companies working to stop scams
**stopscamsuk.org.uk**
Resources and reporting tools

**Save this page.** Take a photo of it with your phone. If you or someone you know gets scammed, you'll have all the numbers in one place. **Share it with elderly relatives — they're most at risk.**

# How to Support a Scam Victim

Someone you know has been scammed. They're embarrassed, angry, and probably blaming themselves. **How you react matters more than you think.** Here's exactly what to do.

### Do Say

"This is not your fault — scammers are professionals"

"I'm glad you told me. That takes courage."

"What do you need right now?"

"Let's sort this out together, step by step"

"You're not alone — thousands of people get scammed every day"

### Don't Say

"How could you be so stupid?"

"I knew that was a scam from the start"

"Well, you should have been more careful"

"I would never fall for something like that"

"Let me see the messages so I can laugh at them"

1 **Listen First, Fix Second**

Don't jump into解决问题 mode. Let them tell the story. Let them feel their feelings. Most victims say the worst part isn't the money — it's the shame. **Your first job is to make them feel safe, not stupid.**

2 **Help Them Act Fast**

Once they've talked, gently move to action. Offer to sit with them while they call their bank. Help them find the fraud number. Write down what the bank says. The scammer relied on them being alone — your presence changes the power dynamic.

3 **Help Them Report It**

Offer to sit with them while they report to Action Fraud (0300 123 2040). The reporting process can feel overwhelming — having someone there makes it manageable. Don't pressure them if they're not ready. Some people need a few days.

4 **Don't Judge the Amount**

Whether they lost £50 or £50,000, the shame is real. Don't say "at least it was only £50" — that dismisses their pain. Don't gasp if it's a lot — that makes the shame worse. Just say "okay, let's work with what we've got" and move to action.

5 **Help Them Lock Things Down**

Walk through the basics: change passwords (starting with email), turn on 2FA, check credit reports, place a Cifas flag. Most victims don't know where to start. You don't need to be a tech expert — just follow the steps with them.

6 **Check In Later**

The shame doesn't go away after one conversation. Check in a week later. Ask how they're doing — not just about the scam, but about *them*. Scam victims often withdraw from friends and family. Don't let them.

7 **Know When to Get Professional Help**

If they're struggling to sleep, having panic attacks, or talking about suicide — this is beyond what you can handle alone. Encourage them to contact Victim Support (0808 168 9111), Samaritans (116 123), or Mind (0300 123 3393). This is not a sign of weakness. It's a sign that the scam did real damage, and real help is needed.

### The Most Important Thing

Being scammed is one of the most humiliating experiences a person can go through. The scammer didn't just take their money — they took their trust, their confidence, and their sense of safety. **Your kindness is the antidote.** A scam victim who feels supported is far more likely to report the crime, seek help, and recover emotionally. A victim who feels shamed withdraws, suffers alone, and often gets scammed again because they never told anyone. **You can break that cycle just by being kind.**

# 🔍 Weekly Deep Dive Investigations

Every week we pick **one scam** and go deep — real stories, dark web intel, victim interviews (anonymous), and exactly how the operation works from the inside. Think of it like a documentary in your pocket.

THIS WEEK'S INVESTIGATION

## Pig Butchering: Inside the Crypto Love Machine

How a wrong-number text turned into a £340,000 loss. We tracked the messages, the fake platform, and the trafficked workers forced to run the scam. Full dark web trace with screenshots.

### How We Investigate

Our system monitors dark web forums, Telegram scam channels, and leaked databases daily. When a new scam trend appears, we trace it from the initial hook (the first message you receive) all the way to the money flow. We map the infrastructure — fake websites, hosting providers, payment processors — and publish everything in plain English.

🗒️

### Previous Investigations

WEEK 1 **AI Voice Cloning** — Tested 3 voice cloning tools. Cloned a voice from a 6-second Instagram story. Called 10 people. 8 believed it was real.

WEEK 2 **Deepfake CEO Fraud** — Traced a deepfake Zoom call that cost a UK company £200,000. Interviewed their IT security team.

WEEK 3 **Smishing Ring** — Found the Telegram channel selling fake DPD/Royal Mail templates. Reported to NCSC. Channel shut down within 48 hours.

### Read the Full Investigations

Each deep dive is published on the CyberAware UK website with full evidence, screenshots, and practical takeaways. Also available as a podcast episode.

Website | Podcast | Twitter

# Phone Theft Protection

Your phone is a goldmine for thieves — access to your bank, email, social media, photos, and passwords. **Phone theft is exploding in the UK** (over 200 phones stolen every day in London alone). Here's how to lock yours down so a thief gets a brick, not a bank account.

200+ phones stolen daily in London | £2,300 average phone theft loss (device + data) | Enable these settings BEFORE you lose your phone

## iPhone — Apple Security (iOS 17+)

Apple has the best theft protection of any phone maker — but only if you turn it on. Here's what you need:

**Find My iPhone** — Settings > [Your Name] > Find My > Enable all three (Find My iPhone, Find My Network, Send Last Location). This lets you track, lock, and wipe your phone remotely.

**Stolen Device Protection** — Settings > Face ID & Passcode > Stolen Device Protection > ON (iOS 17.3+). This is the single most important setting. It requires Face ID for critical changes (passwords, turning off Find My, erasing). A thief with your passcode can't do any damage.

**Activation Lock** — Enabled automatically with Find My. Even if a thief factory resets your iPhone, they can't activate it without your Apple ID password. The phone is a brick.

**Remove SIM PIN** — Set a SIM PIN too (Settings > Mobile Data > SIM PIN). Stops thieves putting your SIM in another phone to get 2FA codes.

The passcode is the thief's best friend. Use a strong alphanumeric code (not 4 or 6 digits) and rely on Face ID for everyday unlocking.

## Android — Google Security (Android 15+)

Google has caught up fast. Android 15 introduces powerful theft protection features:

**Find My Device** — Settings > Google > Find My Device > Enable. Lets you locate, lock, or erase your phone remotely at google.com/android/find.

**Theft Detection Lock** — Android 15 uses AI to detect if someone snatches your phone and tries to run or drive away. It automatically locks the screen. Ensure this is enabled in Settings > Security.

**Offline Device Lock** — Locks your screen if a thief tries to disconnect the phone from the internet to prevent remote wiping.

**Remote Lock** — Even if you didn't set up Find My Device, you can still lock your phone by visiting android.com/lock and entering your phone number.

Samsung phones have extra protection in Galaxy Settings > Security & Privacy > Auto Blocker. Also enables "Maximum Restrictions" for stolen device scenarios.

## Critical Settings Everyone Should Check

**Use a strong passcode** — 4-digit PINs take seconds to brute force. Use a 6-digit or alphanumeric code. Face ID / fingerprint is fine for everyday, but your backup passcode needs to be strong.

**Disable lock screen notifications** — When your phone is locked, your texts and emails show on the screen. A thief can read your 2FA codes without unlocking it. Settings > Notifications > Show Previews > When Unlocked.

**Turn off Control Centre on lock screen** — Stops thieves turning on Airplane Mode (disabling Find My) without unlocking. (iPhone: Settings > Face ID & Passcode > Turn off Control Centre)

**Remove Face ID / fingerprint data** — You can quickly disable biometrics by pressing the power button 5 times (iPhone) or holding the power button (Android). This forces passcode entry and invalidates biometrics.

**Write down your IMEI number** — Dial *#06# to see it. This can be used by your network provider to blacklist the phone globally. Save it somewhere safe (not on the phone).

## Your Phone Is Stolen — Now What?

**Use Find My immediately** — Go to iCloud.com/find or google.com/android/find on another device. Put your phone in Lost Mode. It locks the screen with a message showing your contact number.

**Do NOT try to retrieve it yourself** — The police will tell you this too. Tracking an iPhone to a house and knocking on the door is how people get stabbed. Let the police handle it.

**Call your mobile provider** — They can bar the SIM and blacklist the IMEI. O2, Vodafone, EE, Three all have 24/7 lines for this.

**Change your critical passwords** — Especially your Apple ID / Google account, email, and banking apps. Do this from a different device.

**Report to the police** — Get a crime reference number. You'll need it for insurance claims.

**Remotely erase (as last resort)** — Only do this if you're sure you can't recover the phone. Once erased, you can't track it anymore. But Activation Lock still applies (iPhone) so the thief can't use it.

### Do This Right Now

Take 5 minutes. Go into your phone settings. Enable Find My / Theft Detection. Set a strong passcode. Turn off lock screen notifications. Write down your IMEI. **You'll never regret doing this. You might regret not doing it.**

# Lock Your Laptop — BitLocker & FileVault

You lock your front door. You lock your car. But what about your laptop? If it's stolen, the thief can just **pull out the hard drive and read everything** — your photos, tax returns, passwords, the lot. Encryption fixes this.

1 in 10 laptops will be lost or stolen | Without encryption = anyone can read your data | Encryption is free. Takes 2 minutes to turn on.

## Windows — BitLocker

WINDOWS PRO ONLY

BitLocker encrypts your entire hard drive. If someone steals your laptop, removes the hard drive, and plugs it into another computer — they see nothing but scrambled nonsense without your recovery key.

**Check if you have it:** Press Windows Key, type "BitLocker" and select "Manage BitLocker"

**Turn it on:** Click "Turn on BitLocker" next to your system drive (usually C:)

**Save your recovery key:** It will give you a 48-digit key. Save it to your Microsoft account (recommended) or print it. Never store it on the same laptop.

**No BitLocker?** If you have Windows Home, you can still use "Device Encryption" — Settings > Privacy & Security > Device Encryption. Slightly less fancy but still encrypts your data.

BitLocker runs in the background. Once turned on, you won't notice it. You just log in normally. The encryption happens invisibly.

## Mac — FileVault

BUILT INTO EVERY MAC

FileVault is Apple's full-disk encryption. It's actually even simpler than BitLocker — one toggle and you're done. Without it, someone with a few minutes and a screwdriver can read everything on your Mac.

**Turn it on:** System Settings > Privacy & Security > FileVault > Turn On

**Choose how to unlock:** Either your iCloud account (easier) or a recovery key (more secure). If you use iCloud, you can unlock via Apple's website if you forget.

**Encryption takes a few hours** — your Mac will still be usable while it encrypts. It only happens once. After that, it's instant.

**FileVault + Firmware Password:** For extra security, set a firmware password (Intel Macs only). This stops someone booting from a USB stick to bypass FileVault.

FileVault is already on many newer Macs by default. Check if yours is: look for a green "FileVault is turned on" message.

| Feature | Windows BitLocker | Mac FileVault |
|---|---|---|
| **Free?** | (Pro edition) | Every Mac |
| **Takes 2 mins to enable** | | **Even quicker** |
| **Protects against drive removal** | **Full disk** | **Full disk** |
| **Recovery key backup** | Microsoft account or print | iCloud or recovery key |
| **Performance impact** | Minimal (hardware-accelerated) | Minimal (Apple Silicon) |

## What Encryption Actually Does

Think of encryption like a **secret language**. Your laptop stores everything in English (readable). Encryption translates it all to gibberish. When you log in with your password, it translates back to English on the fly.

Without encryption: a thief removes your hard drive, plugs it into a USB dock on their laptop, and reads every file like it's a USB stick.

With encryption: that same hard drive looks like random noise. The thief gets nothing. **A £10 screwdriver and 5 minutes is all it takes to bypass a login password. Encryption stops them cold.**

## Important Warnings

**Don't forget your password/recovery key** — If you forget your password AND lose the recovery key, your data is gone forever. Not even Apple or Microsoft can recover it. That's the whole point.

**Write down your recovery key** — Not on a sticky note on your laptop screen. Write it on paper and keep it somewhere safe. Or save it in a password manager.

**Encryption ≠ backup** — Encryption protects your data if your laptop is stolen. It doesn't protect you if your hard drive dies. You still need backups (see the Backups section earlier in this book).

**Linux users** — LUKS (Linux Unified Key Setup) is the standard. Most Ubuntu/Fedora installers offer encryption during setup. Enable it. It works the same way as BitLocker/FileVault.

### Encrypt Now, Worry Later

Seriously — go to your settings right now and turn on BitLocker or FileVault. It takes 2 minutes. You'll never notice it's there until the day your laptop gets stolen — and on that day, you'll be very, very glad you did it.

🔍 DEEP DIVE INVESTIGATION

# The Journey of a Stolen Phone: From London to Shenzhen

Your iPhone gets snatched on Oxford Street. 72 hours later it's on a workbench in China having its brains scooped out. This is exactly how the stolen phone supply chain works.

### HOUR 0 — LONDON STREETS

A stolen iPhone is worth **£200-£300** to a thief (street price to a fence). The thief sells it within hours to a local buyer — often a shop that "doesn't ask questions" or a middleman working for a larger operation. Cash, no receipt, no questions.

**£200-300 street value · Sold within 4 hours**

### DAY 1 — THE CONSOLIDATOR

The phone moves up the chain to a **consolidator** — a warehouse that collects stolen phones from dozens of thieves. Here they're sorted by model, condition, and iCloud status. Phones without Activation Lock are worth more. iCloud-locked phones go to the parts pile. A container with 500+ phones is assembled and prepared for shipping.

**500-1,000 phones per shipment · Deactivated phones worth 3x more**

### DAYS 2-30 — THE CROSSING

The phones are shipped in cargo containers, often mislabelled as "electronics parts" or "recycled goods." Major ports: Felixstowe (UK) → (transit) → Hong Kong or Shenzhen (China). Some go via Dubai or Vietnam as intermediary stops to avoid detection. Customs checks are minimal for container freight — too many boxes, not enough inspectors.

**£500k-£1M value per container · <5% inspected by customs**

### ARRIVAL — SHENZHEN, CHINA

Welcome to Huaqiangbei — the world's largest electronics market. Your stolen iPhone arrives in a district where you can buy anything electronic, no questions asked. The phone is immediately assessed: if it's iCloud-locked (Activation Lock), it goes to **parts harvesting**. If it's unlocked, it gets a new case, new screen, new box — and sold as "refurbished."

**Huaqiangbei market: 2 sq km of electronics · 50,000+ shops**

### PARTS HARVESTING (ICLOUD-LOCKED PHONES)

If Activation Lock is on, the phone can't be reused as a phone. But its parts are worth a fortune. The screen (£150-300), the camera module (£40-80), the battery (£20-40), the logic board (£100-200 for its gold and rare earth metals). Each part is tested, sorted, and sold to repair shops across Asia and Africa. **Your data is safe** — the NAND chip (where your data lives) is wiped, but the rest of the phone lives on as spare parts in a thousand different devices.

**Parts value: £400-700 per phone · Screens are the goldmine**

### THE ICLOUD REMOVAL INDUSTRY

There's an entire grey-market industry dedicated to **removing iCloud locks**. Methods range from phishing the original owner (fake Apple emails), social engineering Apple support agents, brute-forcing passcodes, or replacing the logic board's serial number with one from a donor phone. Some "unlockers" charge £50-200 per phone. If they succeed, the phone's value jumps from scrap parts to £400+ as a fully functional device sold in developing markets like Nigeria, Pakistan, and Brazil.

**iCloud removal: £50-200 fee · Unlocked phones worth 5x more**

## What This Means for You

**Encryption and Activation Lock work.** A stolen iPhone with a strong passcode and Find My enabled is worth far less to thieves than an unlocked one. The entire economics of phone theft shifted when Apple introduced Activation Lock — stolen phone values crashed by 50%+ because thieves couldn't resell them as working devices. **Your best defence: strong passcode, Stolen Device Protection ON, Find My ON, lock screen notifications OFF.** And back up your data — because if your phone ends up as spare parts in Shenzhen, at least you won't lose your photos.

Sources: Metropolitan Police organised crime reports, UNODC transnational crime data, Huaqiangbei market research, dark web iCloud removal forums (investigated for research purposes only).

# Car Key Theft — Signal Relay Attacks

Your car key fob is basically a tiny radio transmitter. When you press unlock, it sends a code. **Gangs have learned to amplify that signal from inside your house** and use it to open your car parked outside — without your keys, without breaking a window, without any sign of entry. It's called a **relay attack**, and it's the #1 method cars are stolen in the UK.

| 3 min | 70% | £12,000 |
|---|---|---|
| average time to steal a keyless car | of stolen cars taken without keys | average car theft insurance claim |

## 📢 How a Relay Attack Works

### Step 1: One Thief Walks to Your Front Door

They hold a **relay box** (a radio amplifier, about the size of a phone) against your front wall, near where your keys are — hallway table, coat hook, kitchen counter. This device picks up your key fob's signal from up to 30 metres away, even through walls.

### Step 2: Signal Beamed to the Car

The relay box transmits your key's signal to a **second device** held by another thief standing next to your car. The car thinks the real key is right there. **Click.** Doors unlock. Engine starts. They drive away in 60 seconds.

⚠ NO ALARM TRIGGERED · NO GLASS BROKEN · CCTV SHOWS NOTHING UNUSUAL

### The Equipment (Scarily Cheap)

Relay attack devices are available online for as little as **£50-200**. They look like walkie-talkies or game consoles. Some are sold openly as "key fob testers" — but everyone knows what they're actually for. The technology has been around since 2017 and has only gotten cheaper and smaller.

## How to Protect Your Car

**Faraday Pouch**
£5-15
Lined with metal mesh. Put your keys inside and the signal can't escape. Test it: put keys in pouch, try to unlock car — if it works, the pouch is fake.

**OBD Lock**
£15-30
Thieves often access your car's OBD port (under the dashboard) to program a blank key. A simple lock stops them.

**Steering Wheel Lock**
£20-60
Old school but effective. Visible deterrent — thieves move on to an easier target. The bright yellow ones are best.

**Ghost Immobiliser**
£150-300
Requires a secret button sequence (using your car's existing buttons) before the engine can start. Even if they have your key signal, they can't drive away.

### Simple Habits That Make a Difference

**Keep keys away from doors and windows** — Place them in a metal tin or a Faraday pouch at night. Front-hall hooks are the most vulnerable spot.

**Check if your key fob goes to sleep** — Some newer fobs (Ford, BMW, Mercedes) have motion sensors. If the key hasn't moved for a few minutes, the signal switches off. Test yours.

**Turn off keyless entry overnight** — Some cars let you disable passive entry in the settings menu. Check your owner's manual or Google "[your car model] disable keyless entry".

**Fit a tracking device** — An AirTag hidden somewhere in your car costs £35. Thieves know to look for them, but if you hide it well (inside trim panels, under carpets), it could help police recover the car.

**Use aftermarket security** — A Thatcham-approved alarm or immobiliser can reduce insurance premiums and make your car significantly harder to steal.

### Check Your Car Right Now

Go to your car with your key fob. Stand next to the driver's door and press lock. Now walk into your house and put the keys where you normally keep them. Go back to the car and try the door handle. If it opens — **you are vulnerable to a relay attack.** Get a Faraday pouch tonight.

# 🛠 Hacker Gadgets — The Tools of the Trade

You've seen them in movies. Here they are in real life — **the actual gadgets criminals and pentesters use**. Some are sold on Amazon. Some on Telegram. All of them are cheaper than you'd think. Knowing what they look like is your first defence.

HOT

**Flipper Zero**

£150-200

A dolphin-shaped multi-tool that can read RFID access cards, clone garage remotes, control IR TVs, emulate NFC tags, and spam Bluetooth. **Most famous for:** opening hotel doors, changing petrol station prices (digitally), and cloning office keycards. Sold openly on Amazon.

Use RFID-blocking wallets. Disable unused Bluetooth/NFC on your phone.

Wi-Fi

**WiFi Pineapple**

£100-300

A rogue access point that tricks your phone/laptop into connecting to it instead of the real Wi-Fi. Once connected, it can intercept passwords, inject fake websites, and steal session cookies. **Most famous for:** the "Evil Twin" attack — creating a fake Starbucks Wi-Fi that looks identical to the real one.

Use a VPN. Don't auto-connect to open Wi-Fi. Forget networks you don't use.

KEYS

**USB Rubber Ducky**

£50-80

Looks like a normal USB drive. But when plugged in, your computer recognises it as a keyboard. It types pre-programmed commands at superhuman speed — installing malware, exfiltrating files, or adding backdoor accounts. **Most famous for:** "I just found a USB stick in the car park" attacks.

Don't plug in unknown USB drives. Use USB blockers on work laptops.

📻 RF

**HackRF / SDR**

£200-400

A software-defined radio that can transmit and receive any radio signal from 1MHz to 6GHz. Can clone car keys, spoof GPS, intercept Pager messages, and even replay garage door signals. **Most famous for:** intercepting aircraft ADS-B signals and cloning key fobs.

Rolling-code fobs help. Faraday pouches block signal sniffing.

USB-C

**OMG Cable**

£50-150

A phone charging cable that looks completely normal but contains a hidden implant. When you plug it into your computer, the cable acts as a keyboard and runs payloads. It can also connect to Wi-Fi and let the attacker remotely control it. **Most famous for:** looking exactly like an Apple Lightning cable.

Only use charging cables you trust. Avoid public charging stations (juice jacking).

⌚ WATCH

**WiFi Deauther (Watch)**

£20-60

A programmable smartwatch that can kick any device off Wi-Fi by sending deauthentication packets. Can also create fake access points and capture handshakes (which can be cracked to reveal the Wi-Fi password). **Most famous for:** being worn on the wrist like a normal watch while taking down café Wi-Fi.

WPA2/3 encryption. Use a VPN. Deauther can't crack strong passwords easily.

💳 ATM

**Skimmer / Shimmer**

£30-200

A device placed over ATM card slots or inside card readers. The skimmer reads your card's magnetic stripe; a hidden camera or overlay keypad captures your PIN. **Shimmers** are ultra-thin inserts that go inside the card slot and read the chip data. **Most famous for:** being almost indistinguishable from a real ATM slot.

Check the card reader — if it wiggles or looks bulky, don't use. Cover your PIN.

🏷️ RFID

**Proxmark3**

£150-300

A device specifically for reading, cloning, and emulating RFID tags — the kind used in office keycards, hotel room keys, and contactless payment cards. Can read a card from several feet away and write the data to a blank card. **Most famous for:** cloning office building keycards in seconds.

Use RFID-blocking wallets. Ask your office about MIFARE DESFire (harder to clone).

⚠ **Important Note**

Most of these gadgets are **dual-use** — they're sold for security research, penetration testing, and education. Owning one isn't illegal. Using one to commit a crime is. The best protection is awareness: **knowing what these devices look like and what they can do.** A Flipper Zero in the office doesn't mean someone's hacking you. But a Flipper Zero pressed against your office door reader? That's a problem.

# Property Fraud — Stop Thieves Selling Your Home

Yes, this is a real thing. Criminals forge your ID, pretend to be you, and **apply to sell your house** while you're on holiday. No mortgage, no chain — just a quick sale to a cash buyer they've lined up. By the time you get back, the house has a new owner and the criminal has disappeared with the money. **Property fraud is rare, but when it happens, it's devastating.** Here's how to protect yourself.

### Real Case: The £2.3M Disappearing House

In 2023, a London couple returned from holiday to find their house had been sold without their knowledge. A fraudster had used forged documents to register as the owner, then sold the property to an unsuspecting buyer. The real owners spent years in legal battles to get their home back. HM Land Registry has since seen a 350% increase in property fraud attempts.

## How to Protect Your Property

1. **Sign Up for HM Land Registry Property Alert**
   This is the single most important thing you can do. It's **completely free**. You register your email and the addresses you want to monitor. If anyone applies to change the register (e.g., selling, mortgaging, or adding a name), you get an instant email alert.
   gov.uk/property-alert

2. **Restrict the Title Register**
   You can ask HM Land Registry to add a **restriction** to your property's title. This means the property can't be sold or mortgaged without your solicitor certifying that the application is genuine. It costs **£15-30** but is the strongest protection available. Ask your solicitor to do this.

3. **Check Your Title Register Regularly**
   You can view your property's title register online for £3 from the Land Registry. Check it once a year to make sure nothing has changed without your knowledge. Any unexpected entries could be a sign of fraud.
   gov.uk/get-information-about-property-and-land

## Who Is Most at Risk?

**Empty properties** — Second homes, holiday homes, rental properties you don't live in. Criminals target these because you won't notice for months.

**Unmortgaged properties** — If you own your home outright with no mortgage, there's no bank to flag suspicious activity. Mortgaged properties have an extra layer of scrutiny.

**Properties where the owner is abroad** — Extended holidays, working overseas, or living abroad makes you a prime target.

**Elderly homeowners** — Particularly those with dementia or in care homes. Family members should monitor their property.

**Properties with multiple owners** — Disputes can create opportunities for one owner to fraudulently sell without others' knowledge.

## How Criminals Do It

**Identity theft** — They steal your passport, driving licence, or utility bills (postal theft, data breaches, phishing).

**Forged documents** — They create fake IDs in your name and use them to "prove" they're you to conveyancers and Land Registry.

**Fake solicitor** — Some fraud rings set up fake law firms that handle the "sale" on paper. The buyer has no idea they're dealing with criminals.

**Quick cash sale** — They sell at below-market value for a fast cash completion. The buyer thinks they got a bargain. The real owner comes home to a nightmare.

### Do This Today

Go to **gov.uk/property-alert**. It takes 3 minutes to register. Add your home address. Add any properties you own. Add your elderly parents' homes. It's completely free. You'll get an email alert within minutes confirming your registration. That's it — you're now protected. **3 minutes today could save you years of legal hell tomorrow.**

# 💳 Card Skimming — How They Steal Your Card Details

Your debit card is a goldmine. And criminals have got **absurdly creative** at stealing the details off it. From fake ATM slots to hidden cameras to devices that read your card through your wallet — here's every method, and exactly how to spot it.

**ATM Skimmer**
Fake card reader placed over the real slot — reads your magnetic stripe

**Hidden Camera**
Tiny camera pointed at the keypad to capture your PIN

**Shimmer**
Ultra-thin device inserted inside the card slot — reads chip data

**Digital Pickpocket**
Handheld RFID reader that scans contactless cards through wallets

### Traditional ATM Skimmers

A fake card slot is placed over the real one. It has a built-in magnetic stripe reader that captures your card number. Usually paired with a tiny pinhole camera on top of the machine (disguised as a brochure holder or in the ATM canopy) to film you entering your PIN. The skimmer and camera are retrieved later by the criminal, who now has everything needed to clone your card.

**Check: Wiggle the card reader. If it moves, don't use it. Real ATM readers are fixed solid.**

### Shimmers — The Invisible Reader

Shimmers are thinner than a piece of paper and slide **inside** the card slot. You can't see them, wiggle them, or detect them by looking. They intercept the chip data as your card communicates with the terminal. Chip data can't be cloned into a magnetic stripe, but shimmers are becoming more sophisticated. **Best defence: use contactless or Apple/Google Pay whenever possible.**

**Tap to pay is safer than inserting your card. Use it whenever you can.**

### Digital Pickpocketing (Contactless Theft)

A criminal stands close to you on the Tube or in a crowded street with a handheld RFID reader (£20 on Amazon). The reader scans your contactless card through your wallet, pocket, or bag — capturing the card number and expiry date. **But they can't get your CVV and can't make large purchases with just the contactless data.** Still, they can make small contactless payments until you cancel the card.

**Use an RFID-blocking wallet or sleeve. Pockets tin foil (yes, really) works in a pinch.**

### Fuel Pump Skimmers

Petrol station pumps are a favourite target. Criminals open the pump panel (many have universal keys), install a skimmer inside the card reader, and replace the panel. The skimmer collects card data for weeks before being retrieved. **Pay at the kiosk** or use Apple/Google Pay inside the app — it's much safer than swiping at the pump.

**Use the chip reader inside the kiosk, or pay with your phone. Outdoor pumps are less secure.**

### How to Protect Yourself

**Cover your PIN** — Always use your other hand to cover the keypad when entering your PIN. Even if there's no camera, someone might be watching.

**Use contactless / Apple Pay / Google Pay** — These use one-time tokens, not your real card number. A skimmed terminal captures nothing useful.

**Wiggle the card reader** — Before inserting your card at an ATM, try to wiggle the reader. If it feels loose, it's probably a skimmer on top of the real one.

**Check for cameras** — Look at the ATM keypad area, the top screen bezel, and anywhere a tiny pinhole could hide. If something seems out of place, find another ATM.

**Use ATMs inside banks** — Thieves target outdoor ATMs (cash machines on the street) more often because they can install skimmers without being seen. Inside a bank is safer.

**Get an RFID-blocking wallet** — Stops digital pickpocketing. They cost £10-20 on Amazon. Or wrap your card in foil as a temporary solution.

**Monitor your statements** — Check your bank statements regularly. Flag any unrecognised transactions immediately. The earlier you spot fraud, the easier it is to get your money back.

**Quick Test**

Take your debit card out of your wallet. Try tapping it on the card reader at the shop (without paying). If it works through your wallet, a digital pickpocket can read it too. Get an RFID-blocking wallet.

# SIM Swapping — When Your Phone Number Gets Stolen

You wake up one morning and your phone has no signal. Your mobile just says "No Service." You try to call yourself — someone else answers. **Your number has been stolen.** A criminal convinced your phone provider to transfer your number to a SIM card they control. Now they're getting your 2FA codes, your "forgot password" texts, and your banking alerts. This is **SIM swapping** — and it's terrifyingly effective.

| £10,000 | 3 min | 50%+ |
|---|---|---|
| average loss from SIM swap attack | phone call to social-engineer a provider | of crypto thefts involve SIM swapping |

## 🔗 How SIM Swapping Works

1

**Information Gathering**

The scammer collects personal details about you — often from data breaches, social media, or phishing. They need your full name, date of birth, address, and maybe your mother's maiden name or last 4 digits of your bank card.

2

**The Call**

The scammer calls your mobile network (EE, Vodafone, O2, Three) pretending to be you. They say they've lost their phone and need a new SIM. They provide your personal details to "verify" their identity. The call centre agent processes the request.

3

**Your Number Is Gone**

Your old SIM deactivates. The scammer's new SIM activates with your number. You lose signal. Meanwhile, the scammer goes to your email, types "forgot password," gets the reset link sent via SMS — which now goes to THEIR phone. Then your bank. Then your crypto exchange. Then your social media. All in 10 minutes.

## How to Protect Yourself

**Set a SIM PIN or account password** — Call your mobile provider and ask to add a **dedicated account password** or a **SIM PIN** that must be provided before any account changes. This is the single most effective protection. Without it, no porting, no new SIM, no changes.

**Use an authenticator app, not SMS** — Stop using SMS for 2FA wherever possible. Use Google Authenticator, Authy, or Microsoft Authenticator instead. App-based 2FA can't be SIM-swapped. Most major services (Google, Facebook, banking apps, crypto exchanges) support app-based 2FA.

**Don't use SMS for "forgot password"** — If a service ONLY offers SMS for password resets, consider whether it's worth using. Use a backup email or hardware security key (YubiKey) as alternative recovery methods.

**Keep your personal info off social media** — Don't post your DOB, mother's maiden name, pet's name, or address publicly. That's the exact data scammers use to social-engineer call centre agents.

**Add a recovery phone to your accounts** — Have a secondary number (e.g., a partner's phone or a PAYG SIM you keep at home) as a backup recovery option.

## Your Number Is Stolen — Now What?

**Call your mobile provider immediately** — Use another phone. Tell them your SIM has been swapped fraudulently. They can deactivate the new SIM and restore your old one.

**Call your bank** — Freeze your accounts. Tell them you've been a victim of SIM swap fraud. They can flag your accounts for extra verification.

**Check your email** — See if password reset emails were sent. Secure your email account first (change password, revoke sessions, enable app-based 2FA).

**Check your crypto exchanges** — If you hold crypto, check your accounts immediately. SIM swap + crypto = disaster. Enable withdrawal whitelists if available.

**Report to Action Fraud** — 0300 123 2040. Get a crime reference number.

### Do This Today

Call your mobile provider right now. Ask them to add a **dedicated account password** or **SIM PIN** that must be given before any SIM changes. It takes 5 minutes. Without this, anyone with your name and DOB can steal your number. **Don't wait until you wake up with no signal.**

# Scams Targeting the Elderly — A Guide for Carers & Families

**People over 65 are the most targeted demographic for scams.** Not because they're "gullible" — because they grew up in a world where people kept their word, door-to-door salesmen were legitimate, and the nice person on the phone was actually who they said they were. **Scammers exploit this trust.** If you have elderly parents, grandparents, or neighbours, this section is the most important one in this book.

**The "I'm Calling About Your Computer" Scam**
Someone calls claiming to be from Microsoft, BT, or your internet provider. They say your computer has a virus and they need remote access to fix it. Once connected, they show fake "problems," charge hundreds for "fixes," and steal personal data.
**What they say:** "Hello, this is Susan from Microsoft Technical Department. Your computer has sent us an error report. Please turn on your computer and I'll help you fix it."
🛡 Microsoft, Apple, and BT will NEVER call you about your computer. Hang up.
🚔
**The "Police" or "Bank" Phone Call**
A caller claims to be from your bank's fraud team or even the police. They say there's suspicious activity on your account and you need to move your money to a "safe account." They may send a courier to collect your bank card. The "safe account" belongs to criminals.
**What they say:** "This is Detective Miller from Scotland Yard. We've arrested someone using your card. To protect your savings, we need you to transfer everything to this secure account number I'll give you."
🛡 The police and banks will never ask you to move money or send a courier for your card. Hang up and call 101 or your bank on the number on your card.

**Doorstep Scams**
Someone knocks on the door offering driveway repairs, roof cleaning, gardening work, or "leftover tarmac" from a nearby job. They pressure for cash payment upfront, do shoddy work (or none), and disappear. Some even return later to burgle houses they've identified as occupied by elderly people living alone.
**What they say:** "We're working on a job down the road and have leftover tarmac — we can do your driveway for £200 cash, today only." (The tarmac is cold mix that washes away in the first rain.)
🛡 Never pay upfront for doorstep work. Get three written quotes. Ask to see public liability insurance. If they pressure you, say no and close the door.

📣

**Lottery & Prize Draw Scams**

Letters, emails, or phone calls claiming you've won a large sum of money — but you need to pay a "fee" or "tax" to release it. The scammer may call repeatedly, becoming increasingly urgent. Some victims lose thousands over months as the "prize" gets bigger and the "fees" mount up.

**What they say:** "Congratulations! You've won £500,000 in the European Lottery! To release your winnings, please pay the £2,500 insurance fee via bank transfer. Hurry — the prize expires in 24 hours!"

🛡 You cannot win a lottery you didn't enter. No legitimate prize draw asks you to pay money to receive your winnings.

**Romance & Friendship Scams**

Loneliness is a vulnerability scammers ruthlessly exploit. They befriend elderly people online or by phone, build a "relationship" over weeks or months, then ask for money — for a plane ticket to visit, a medical emergency, or a business opportunity. Many victims lose their life savings and are too ashamed to tell anyone.

**What they say:** "I'm an American engineer working on an oil rig in the North Sea. I've fallen for you. But my daughter is sick and I need £3,000 for her operation. I'll pay you back when I visit England next month."

🛡 If you've never met someone in person and they ask for money, it's a scam. Full stop. Tell a family member immediately.

## 🤝 What Families & Carers Can Do

1

**Have the conversation before it happens**

Talk openly with elderly relatives about scams. Tell them it's okay to be suspicious. Give them permission to hang up on anyone asking for money or personal details. Many elderly people are too polite to hang up — and scammers exploit this.

2

**Set up a family password**

Create a simple code word that only close family knows. If someone calls claiming to be a relative in trouble, ask for the code word. No code word = hang up. This stops the "Grandparent Scam" (fake grandchild needing bail money).

3

**Add their phone to your accounts**

Add your phone number as a secondary contact on their bank accounts if they're comfortable with it. You'll get alerts about unusual activity. Also consider registering their property on gov.uk/property-alert — see the Property Fraud section.

4

**Register with the Telephone Preference Service**

TPS (tpsonline.org.uk) is a free service that stops most legitimate sales and marketing calls. It won't stop scammers directly, but it reduces the number of calls overall, making scam calls more noticeable. Also consider call-blocking phones specifically designed for elderly users.

**The Golden Rule for Elderly Relatives**

Give them permission to be "rude." Scammers rely on politeness and trust. Teach them: **"If someone calls out of the blue and asks for money, personal details, or access to your computer — hang up. You are not being rude. You are being safe. Anyone legitimate will understand."**

# Protecting Your Children Online — A Parent's Guide

Your child knows how to use a phone before they know how to tie their shoelaces. They're growing up in a world where strangers can slide into their DMs, fake friends ask for "nudes," and the "free Robux" website steals your credit card details. **Scammers target children too** — differently, but just as ruthlessly. Here's what every parent needs to know.

31%
of 8-17yr olds have been scammed online

12
average age a child first gets a phone

75%
of parents don't monitor online activity

🎮

**"Free" In-Game Currency & Item Scams**

"Free Robux!" "Free V-Bucks!" "Free Minecraft skins!" These are the most common scams targeting children. Fake websites, YouTube videos, and Discord messages promise free in-game currency. Children enter their parent's credit card details — or worse, download malware that steals everything from the family computer.

There is no such thing as free Robux. Teach your child: if it says "free" in a game, it's probably a scam.

"Enter your username and your mum's credit card to get 10,000 free Robux!" — The Robux never arrive. The card details are stolen.

**Fake Friends & Grooming**

Scammers pose as children the same age on gaming platforms (Roblox, Fortnite, Minecraft) and social media (TikTok, Instagram, Snapchat). They build trust over days or weeks, then ask for personal information, explicit photos, or money. This is how online grooming starts. **One in five children have been approached by strangers online.**

Talk to your child about stranger danger online the same way you do about stranger danger in the park. The same rules apply.

**Fake Competitions & Giveaways**

"Follow me and share this post to win an iPhone!" — Influencer-style scams that trick children into clicking malicious links, sharing personal data, or completing surveys that sign them up for expensive subscriptions. Children don't spot the red flags because the offer looks exactly like real influencer giveaways.

Teach your child: never click "claim prize" links, never share your real name/age/address online, and always ask a parent before entering any competition.

**Sextortion — The Fastest Growing Cybercrime Against Children**

A scammer pretends to be a romantic interest, persuades a child to send an intimate photo, then immediately threatens to share it with their friends, family, and school unless the child pays money (often via gift cards or crypto). **The NSPCC reports a 257% increase in sextortion cases targeting boys aged 11-15.** Children are terrified, ashamed, and often too scared to tell anyone. This is not your child's fault. This is a crime.

If your child comes to you with this: do NOT get angry. Do NOT blame them. Report it to the police immediately. The images can often be removed through the Internet Watch Foundation (iwf.org.uk).

**What to say to your child:** "If anyone ever asks you for a photo and then threatens you — stop talking to them, tell me immediately, and I will not be angry. You are the victim. The criminal is the only one who did something wrong."

## Practical Steps for Parents

1

**Keep devices in shared spaces**

No phones, tablets, or laptops in bedrooms overnight. Charge devices in the kitchen or living room. This isn't punishment — it's protection. Most online grooming and sextortion happens late at night when parents are asleep.

2

**Use parental controls — but don't rely on them alone**

Set up Screen Time (iPhone) or Family Link (Android) to restrict app downloads, content access, and screen time. But controls are not a substitute for conversation. A determined child can bypass most parental controls. Education beats restriction every time.

3

**Have the "no is not rude" conversation**

Children are taught to be polite. Scammers exploit this. Teach your child: **"If someone online asks you to keep a secret from your parents, that person is dangerous. If someone asks for a photo or your address, you don't have to be polite — you say no and tell me immediately."**

4

**Check their privacy settings together**

Sit down with your child and go through their social media privacy settings together. Make accounts private. Turn off location sharing. Disable DMs from strangers. Explain why — not just "because I said so" but "because there are people online who pretend to be kids to hurt other kids."

### The Most Important Thing You Can Do

**Create a culture of safety, not secrets.** If your child knows they can come to you about anything that happens online without being punished, shouted at, or having their devices taken away — they will. If they're scared of your reaction, they'll suffer in silence. **Be the person they can tell.** Visit **thinkuknow.co.uk** for age-appropriate resources from the National Crime Agency.

# 🎓 Student Scams — University Life, Scammer Targets

Starting university is overwhelming enough without getting scammed. But **students are prime targets** — you're managing your own money for the first time, you're desperate for accommodation and jobs, and you're constantly online. Scammers know this. Here's what to watch for.

60%
of students targeted by scams in first year

£1,800
average loss per student scam victim

£20M
lost by UK students to scams annually

🏠

**Fake Student Accommodation**

You find a perfect flat near campus — great price, amazing photos. The "landlord" says demand is high and asks for a deposit (£500-1,000) to secure it. They're "abroad" so you can't view it. You pay. You arrive. The flat doesn't exist or is someone else's home. The "landlord" is gone.

Never pay a deposit without viewing the property. Use accredited letting agents. Check the university accommodation office for legitimate listings.

"2-bed flat near City Campus — £450/month all bills included. Landlord is in Spain. Send £650 deposit to secure." — The photos are from a hotel website.

**Fake Student Jobs**

"Earn £200/week as a brand ambassador! Just pay £50 for your starter pack!" Or the classic reshipping scam: "Receive parcels at your student address and forward them overseas — earn £2,000/month!" You're now a money laundering accomplice. The parcels are bought with stolen credit cards.

No legitimate job asks you to pay to work. No legitimate job involves receiving and reshipping packages.

"Student Marketing Rep needed — £500/week, flexible hours. Just pay £99 for your training materials and welcome pack." (The welcome pack is a PDF. The job doesn't exist.)

📚

**Fake Tuition Fee Emails**

An email arrives that looks exactly like your university's finance department. "Your tuition payment has failed — click here to re-verify your card details." The link goes to a fake university login page. You enter your details. The scammer now has your university login and your bank details.

Universities send payment reminders — they never ask you to click a link to "verify" your card. If in doubt, walk to the finance office in person.

**Social Media Hacking & Account Takeover**

"Hey, click this link and vote for me in this competition!" — A friend's Instagram or TikTok account has been hacked and is now DMing everyone with a phishing link. Students lose their accounts weekly to these scams. Once hacked, the scammer uses the account to message your family asking for money, or posts content designed to blackmail you.

If a friend sends you a strange link, message them on a different platform to check. Turn on two-factor authentication on every social media account.

"OMG I can't believe I won! Vote for me: www.voteforme-competition.co.uk/login" — The site steals your Instagram login. The friend was hacked. Now you are too.

**Student Discount Scams**

Fake UNiDAYS, Student Beans, or TOTUM discount pages. A Facebook or Instagram ad promises "80% off everything with this student discount code" — but you need to enter your card details to "verify your student status." The discount code doesn't exist. Your card details are now being used for fraud.

Only use the official UNiDAYS, Student Beans, or TOTUM apps. Never enter card details on a third-party site for a "discount."

**Online Shopping — Fake Goods & Medication**

Cheap vaping products, prescription medication (ADHD meds, anxiety meds) sold without prescription on Instagram and Telegram. You pay. You get counterfeit goods, dangerous chemicals, or nothing at all. Ordering prescription medication without a prescription is illegal and dangerous.

If an Instagram account is selling prescription medication without a prescription, it's a crime. You are buying from criminals.

## Student Survival Tips

1

**Use your university's accommodation office**

Most universities have an accommodation service with verified listings. Use it. Private Facebook groups for student housing are full of scammers.

2

**Turn on 2FA on everything**

Email, Instagram, TikTok, banking, university portal. Use an authenticator app, not SMS. See the SIM Swapping section for why.

3

**Beware "too good to be true" at Freshers' Fair**

Scammers set up fake stalls at Freshers' Fairs offering amazing deals. If they want cash or bank details upfront, walk away.

4

**Talk to your flatmates**

Share scam warnings with your housemates. If one of you spots something, tell the others. Scammers target groups — protect each other.

**🎓 Share This Page With Every Fresher You Know**

60% of students are targeted in their first year. Most are too embarrassed to tell anyone they've been scammed. Send this to your younger siblings, your uni group chat, and anyone starting university this year. **A 5-minute read could save them £1,800.**

# Insider Threats — When the Enemy Works Next to You

Not all data breaches come from hoodie-wearing hackers in basements. Sometimes they come from **the colleague who sits next to you**. Insider threats happen when an employee — deliberately or accidentally — exposes company data. And it's more common than you think.

60%
of data breaches involve insiders

£15M
average cost of insider threat incident

3 in 4
insider breaches are accidental, not malicious

### The Three Types of Insider Threat

😈
Malicious

😐
Negligent

🕵
Compromised

😈
**Malicious Insider — The One Selling Passwords**

A disgruntled employee, someone approached by criminals, or someone in financial trouble sells their access. Common targets: IT admins with system-level access, sales staff with customer databases, finance staff with payment systems. Passwords are sold on dark web forums for £50-£5,000 depending on access level. **An IT admin's credentials can sell for £5,000+.**

Warning signs: employee suddenly living beyond their means, expressing anger at the company, or accessing files they don't need for their role.

A systems administrator at a UK telecoms company sold admin credentials to a criminal group for £3,500. The group accessed customer data for 6 months before detection. The admin was sentenced to 5 years.

😐
**Negligent Insider — The One Who Means Well But Messes Up**

Someone leaves their laptop on the train. Clicks a phishing email they shouldn't have. Shares a spreadsheet with customer data on a public link. Uses "Password123" for their work accounts. **75% of insider threats are accidental.** No malicious intent — just human error with catastrophic consequences.

Training, not punishment, is the answer. A culture of security awareness prevents more accidents than strict policies ever will.

An NHS employee emailed a spreadsheet containing 500 patients' medical records to their personal email to work from home. The email was intercepted. The employee was dismissed. The trust was fined £500,000.

🕵

**Compromised Insider — The One Whose Account Got Stolen**

Someone's work account is hacked — usually through phishing or credential stuffing (using a password leaked from another site). The criminal now has access to the company network as that employee. They move laterally, escalate privileges, and exfiltrate data. **The employee had no idea their account was compromised until IT called.**

2FA would have prevented most of these. If your employer doesn't require 2FA, ask why.

A marketing employee at a law firm reused their personal password (leaked in a 2022 data breach) for their work account. A criminal used it to log in, then spent 3 weeks quietly downloading client contracts worth millions. The firm lost 3 major clients.

## 🛡 How to Protect Your Workplace

1

**Enforce 2FA everywhere**

No exceptions. Not even for the CEO. If a criminal gets a password, 2FA stops them. This is the single most effective control against compromised insider attacks.

2

**Use the principle of least privilege**

Employees should only have access to the data they need for their job. No more. If a salesperson doesn't need access to HR files, they shouldn't have it. This limits the damage of both malicious and compromised insiders.

3

**Monitor for unusual access patterns**

If an employee logs in at 3am from an IP in a different country, or downloads 10,000 files in an hour, the system should flag it. Most insider threats are detected by behaviour, not by passwords.

4

**Create a culture where people speak up**

Employees should feel safe reporting a colleague who seems to be acting suspiciously, or admitting they clicked a phishing link without fear of being sacked. Fear drives secrecy. Secrecy drives breaches.

5

**Have an exit checklist for leavers**

When an employee leaves, revoke all access within 24 hours. Disable accounts, collect badges, wipe company devices. Many insider breaches happen in the notice period when a disgruntled employee still has full access.

**For Employers & Employees Alike**

**If you're an employee:** Never share passwords. Never reuse work passwords for personal accounts. Report suspicious behaviour to IT. **If you're an employer:** 2FA is not optional. Least privilege is not bureaucracy — it's security. Your biggest threat might not be a hacker. It might be someone who already has a key to the building.

# How NOT to Get Hacked

Knowing scams is half the battle. The other half? **Locking your digital doors so hackers can't even try.** Good news: you don't need to be a tech wizard. Most of this is just... common sense with a sprinkle of paranoia.

## 1. Use a VPN

***"Free public Wi-Fi at the coffee shop? Lovely. Also lovely for the bloke stealing your passwords from 3 tables away."***

A VPN **encrypts everything you do online** into a secret tunnel. Anyone on the same Wi-Fi — including hackers at the airport, hotel, or café — sees nothing but gibberish. Without a VPN, your banking logins, emails, and passwords fly through the air in plain text for anyone to scoop up. Yes, really.

**What to do:**

Get a reputable VPN (ProtonVPN has a solid free tier; NordVPN, Mullvad for paid)
Turn it on any time you're not on your home Wi-Fi
Don't use free VPNs — if you're not paying, you're the product
Bonus: a VPN also hides your browsing from your internet provider

## 2. Passwords: Stop Using "Password123"

***"Your password is 'iloveyou'? Aww. The hacker loves you too — especially your bank balance."***

Hackers use automated tools that try millions of passwords per second. "Password1", "123456", your dog's name, your birthday — cracked in milliseconds. And if you reuse the same password everywhere? One leaked password means ALL your accounts are toast.

**What to do:**

Use a password manager (Bitwarden is free, 1Password is great). You only need to remember ONE master password
Every account gets a unique, randomly-generated password — the manager fills them in for you
Your email and banking passwords should be the strongest. If those get hacked, you're in trouble
Write your master password on paper and keep it somewhere safe. Yes, paper. It can't be hacked.

## 3. Turn On 2FA (Two-Factor Authentication)

***"2FA is like having a second lock on your door. The hacker picks the first one and finds... another lock. Annoying for them. Great for you."***

Even if a hacker gets your password, 2FA blocks them with a second check — usually a code sent to your phone, or generated by an app like Google Authenticator. Without that code? They're locked out. **On average, 2FA blocks 99.9% of automated attacks.**

**What to do:**

Turn on 2FA on EVERY account that offers it — email, banking, social media, the lot

Use an authenticator app (Google Authenticator, Authy, Microsoft Authenticator) rather than SMS if possible

SMS 2FA is better than nothing, but can be bypassed via SIM swapping (see Scam #11... ok that's not in this book, just know it's a thing)

## 4. Update Your Bloomin' Devices

***"You know that 'Update Tonight' pop-up you've been ignoring for 6 weeks? Hackers love it when you do that."***

Software updates aren't just for new emoji. They patch security holes that hackers actively exploit. The moment a vulnerability is announced, hackers race to build tools that target unpatched devices. Every day you delay an update is a day you're walking around with a gaping hole in your digital armour.

**What to do:**

Turn on automatic updates on your phone, laptop, and tablet. Let it update overnight while you sleep

Don't ignore system update notifications for more than a day or two

This includes your router, smart TV, and any smart home gadgets — they can be hacked too

## 5. Back Up Your Data

***"Ransomware encrypted all your photos? That's cute. Did you back them up? No? Ah. That's a shame."***

Ransomware is malware that locks your files and demands payment to unlock them. If you have backups, you can wipe your device, restore, and tell the hacker to jog on. If you don't... you either pay up (never guaranteed to get your files back) or lose everything.

**What to do:**

Follow the 3-2-1 backup rule: 3 copies of your data, 2 different types of storage, 1 stored off-site

Use a cloud backup service (Backblaze, iCloud, Google Drive, OneDrive — something automated)

Also keep an external hard drive backup at home for important stuff (photos, documents)

Test your backups! A backup you've never tested is a prayer, not a plan.

## 🔍 6. Think Before You Click

***"That link promising a free iPhone? If you click it, the only thing that's free is the malware you just installed."***

Most hacks don't involve genius-level code-breaking. They involve **tricking you into clicking something**. A link, an attachment, a "FREE GIFT CARD" image. One click can install malware, steal your cookies (the digital kind), or redirect you to a fake login page.

**What to do:**

Hover over links before clicking — check the actual URL, not just the text on screen

If something seems urgent, exciting, or too good to be true — pause. That pause is your superpower.

Never download attachments from unexpected emails — even if they look like they're from someone you know

If a friend sends you a weird link on WhatsApp, message them separately to check if it was really them

## 🕵️ 7. Lock Down Your Social Media Privacy

***"Posting your holiday photos while you're still on holiday? You just told the world your house is empty. Great work, detective."***

Scammers mine your social media for personal info: your date of birth, pet's name, where you went to school, your mum's maiden name. These are the exact answers to "security questions." You're giving them the keys and wondering why your accounts keep getting broken into.

**What to do:**

Don't post your date of birth publicly on social media. Ever.

Make your profiles private — strangers don't need to see your holiday snaps or your cat's name

Don't share your location in real-time. Post that beach photo when you're already home

Use lie-answers for security questions (password manager can store them). Your first pet wasn't really "Fluffy" — it was "XylophoneBanana42"

Never post photos of your boarding pass, work ID, or credit card — yes, people actually do this

## 8. Common Sense — The Greatest Antivirus

***"All the tech in the world can't save you from that little voice that says 'hmm, this seems dodgy'. Listen to it."***

The best security tool you own is your brain. Scammers rely on you acting without thinking. They create urgency, fear, excitement — anything to bypass your rational brain. If something feels off, **it is off**. Trust your gut.

**The Golden Rules:**

No legitimate person or company will ever ask for your password. Ever. Period.

If someone calls you and claims to be from your bank, hang up and call the number on your card

Free USB drives left at conferences or mailed to you? Don't plug them in. It's called "USB dropping" and it works.

Don't plug random phones or devices into your computer's USB port — they can act as keyboards and take over

Cover your laptop camera with a sticker. Mark Zuckerberg does it. You're not more important than Zuck.

If a deal seems too good to be true, your wallet is about to learn an expensive lesson

# Quick Rescue Card

Stuck on a call with a scammer? Getting suspicious texts? Tear your eyes away from this card.

## STOP. Don't Do Anything.

⏸ Pause. Scammers rush you.

Hang up or close the message.

🔍 Verify using official channels.

Tell someone. Scams thrive in secrecy.

## Who to Call

🚨 Action Fraud: 0300 123 2040

Your bank (use number on your card)

Forward spam texts to 7726

Report phishing: report@phishing.gov.uk

## Red Flags

URGENCY — "Do it now!"

💳 Asking for card/PIN/password

"Too good to be true" offers

"Don't tell anyone" ( )

Bank transfer only (no card protection)

# The Little Book of Scams

Share it with your friends, family, and that one mate who keeps "almost" falling for pyramid schemes. Education beats fear — every time.

**cyberawareuk.co.uk**

𝕏 @CyberAware_UK • Spotify: CyberAware UK