Beginner's Guide To Phishing Scams

Guide · How Phishing Works Psychologically, The Patterns Across Every Variant, And The Verify-Before-You-Click Flow.

Who this is for: anyone who's clicked a sketchy link before — or worried they will. Phishing is the #1 cause of account takeovers. This guide explains how it works, why it works, and how to train your eye so it stops working on you.

What Phishing Is, And Isn't

Phishing is when an attacker pretends to be a trusted entity (your bank, your boss, Apple, the IRS) to trick you into doing something you wouldn't normally do — clicking a link, downloading a file, sharing credentials, sending money. It's not technical: phishing exploits human psychology, not software vulnerabilities. That's why it works on smart people. That's also why awareness is the only real defence.

The Phishing Family Tree

- **Phishing** — generic, usually email-based, mass-distributed.
- **Spear phishing** — targeted at a specific person or company, customised with real details.
- **Whaling** — phishing aimed at executives or high-value individuals.
- **Smishing** — phishing via SMS / text message.
- **Vishing** — phishing via phone call.
- **Quishing** — phishing via QR code (newer; QR codes hide the destination URL).
- **Clone phishing** — copying a legitimate email and replacing one link.

Why Phishing Works

Phishing exploits cognitive biases that all humans share. Recognising the bias the attacker is targeting is half the defence:

Bias / Trigger	How Attackers Use It
Authority	Pretend to be your bank, IRS, CEO, or law enforcement.
Urgency	'Act now, your account will be suspended in 24 hours.'
Scarcity	'Limited offer, claim your refund before it expires.'
Fear	'Suspicious activity detected, verify immediately.'
Reciprocity	'We've already started your refund — just confirm details.'
Social proof	'Most customers have already updated their info.'
Curiosity	'You won't believe what they're saying about you online.'
Loss aversion	'Tax penalty unless you respond by Friday.'

12 Universal Red Flags

1. **Urgency.** 'Act within 24 hours,' 'final notice,' 'account suspended.'
2. **Mismatched sender.** Display name says 'Apple,' but email is at apple-billing-support.help.
3. **Generic greeting.** 'Dear customer' instead of your name from a service that knows your name.
4. **Hovering shows different URL.** Mouse over the link — the destination doesn't match what's displayed.
5. **Slightly wrong domain.** arnazon.com, paypa1.com, microsoft-secure.com.
6. **Unexpected attachment.** Especially .zip, .iso, .htm, or 'invoice.pdf.exe'.
7. **Asks for credentials.** No real company emails you a login form.
8. **'Verify your account' link.** Even if it looks genuine, type the URL yourself.
9. **Threats.** Lawsuit, arrest, IRS, deportation, account closure.
10. **Too good to be true.** Refund, lottery, inheritance, package you didn't order.
11. **Tone mismatch.** Coworker / friend writing in a way that doesn't sound like them.
12. **Spelling and grammar errors.** Especially in supposedly corporate communications.

The Verify-Before-You-Click Flow

1. **Stop.** Don't click. Don't reply. Take 30 seconds. Real urgency is rare.
2. **Inspect.** Sender domain, link destination, attachments, tone. Look for the red flags.
3. **Verify out-of-band.** Open the app or website directly. Call the company at a number you find on their official website or the back of your card — never the number in the suspicious message.
4. **Report.** Gmail: Report Phishing. Outlook: Report → Phishing. Forward to reportphishing@apwg.org.

Modern Variants Worth Knowing

AI / Deepfake Phishing

AI-generated voice clones can impersonate family members in a 'grandchild emergency' scam, requesting urgent money. Defence: family verify-word system. Pick a word your family uses to authenticate any urgent money request. If a voice can't say it, it's a scam, even if it sounds like them.

Romance Scams

Long-running phishing campaigns where the attacker builds an emotional relationship over weeks/months before introducing a money request. Often involves moving the conversation off the original platform. Defence: never invest based on a relationship that started online; reverse-image-search profile photos.

MFA Fatigue

Attacker who has your password tries to log in repeatedly, sending dozens of MFA push notifications hoping you'll tap 'Approve' to make them stop. Defence: switch to number-matching push (Microsoft) or use authenticator-app codes that require active entry.

Quishing — QR Code Phishing

A QR code in an email or printed in a public place leads to a phishing site. The QR hides the URL until you scan, so you can't preview before commitment. Defence: prefer typed URLs or known apps over QR codes for anything sensitive.

If You Already Clicked Or Replied

1. Disconnect Wi-Fi if you downloaded anything.
2. Change passwords on any account you submitted credentials for, immediately, from a clean device. Enable MFA.
3. Run a malware scan.
4. Notify your bank if any financial info was shared. Consider a credit freeze.
5. Report at reportfraud.ftc.gov and to the platform where the scam reached you.

Train The Whole Family

Phishing succeeds because people fall for it before they learn to recognise it. Build a family library of real scams you've encountered — forward the analysed messages to everyone in the household with the red flags called out. Real examples are dramatically more memorable than abstract advice.

Where To Go Next

- **Use the Phishing Red Flags Cheat Sheet** — quick visual reference.
- **Use the Scam Warning Signs Cheat Sheet** — universal patterns across all scams.
- **Try the Phishing Email Test** — quiz yourself on real-world examples.