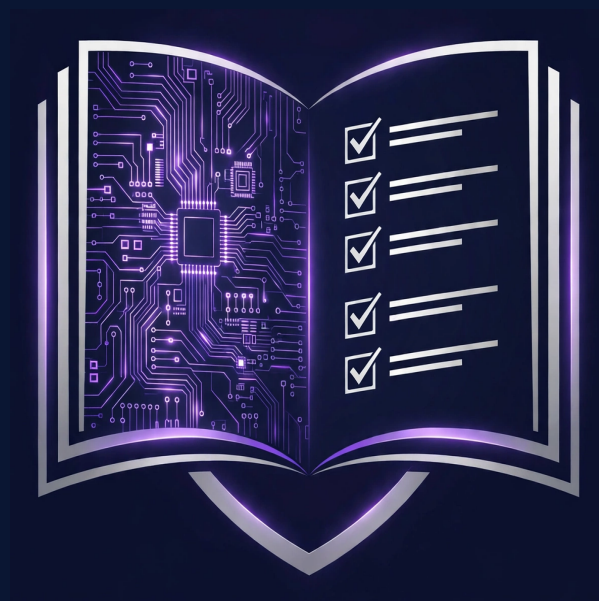




PLAYBOOK

Phishing Response Playbook

Cybersecurity & GRC, in Plain English

A free resource from Cyber By The Book
cyberbythebook.com • Houston, TX



PLAYBOOK

Phishing Response Playbook

Phishing is the #1 way small businesses and families get hacked — not by breaking in, but by tricking you into opening the door. Part 1 helps you spot it. Part 2 is your step-by-step plan if you already clicked.

Part 1 — Spot it in 10 seconds

- ☐ The sender: does the email address really match the company? One changed letter means fake
- ☐ The rush: 'Your account will be closed TODAY!' — real companies don't threaten you by text or email
- ☐ The link: hover, or press and hold, before you tap — if the address looks strange, don't open it
- ☐ When in doubt, don't click: open the company's real app or website yourself and check there

Part 2 — If you clicked or typed something

- ☐ Step 1: If you downloaded a file, disconnect that device from Wi-Fi right away
- ☐ Step 2: On a clean device, change the password for the account involved — then anywhere you reused it
- ☐ Step 3: Turn on 2FA for that account before you do anything else
- ☐ Step 4: Check your bank and card accounts for charges you don't recognize
- ☐ Step 5: Run a full antivirus scan on the device you clicked on
- ☐ Step 6: Warn your family and coworkers — the same message may have gone to them too

Part 3 — If you entered card or banking details

- ☐ Call your bank immediately using the number on the back of your card — not a number from the message
- ☐ Ask the bank to watch or freeze the card, and note the time you called
- ☐ Report the phish: forward suspicious texts to 7726, and phishing emails to reportphishing@apwg.org

Print this and keep it where anyone in the house or office can find it. The first 10 minutes after a click matter most.

More free checklists, playbooks, and controls: cyberbythebook.com