



Spot It. Stop It. Fix It.

A plain-English workshop on the email, text, and online scams targeting people today.

Scams aren't aimed at the careless anymore — they're aimed at everyone, and they're getting convincing. The good news: almost every one follows the same handful of patterns. Once you can read those patterns, you can shut them down in seconds. **This workshop teaches you exactly how.**

1 SPOT

Learn the tells that give away a fake — the urgency, the odd sender, the link that's almost right — across every channel scammers use.

2 DEFEND

Build a few simple habits — slow down, verify, go direct — that stop the vast majority of scams before they ever cost you anything.

3 REMEDIATE

Know exactly what to do in the first hour if something slips through: how to limit the damage, who to call, and what to ignore.

THE SCAMS YOU'LL LEARN TO READ

EMAIL — “PHISHING”

- “Your account is locked” login-stealers
- Fake invoices & subscription renewals
- The boss / CEO “quick favor” wire request
- Fake delivery & shipping notices
- Attachments that quietly install malware

TEXT — “SMISHING”

- Bank “fraud alert” asking you to confirm
- Package “redelivery fee” links
- Toll, DMV, or tax “unpaid fine” notices
- One-time passcode theft (“read me the code”)
- “Wrong number” chats that become investment pitches

ADS & WEB — “MALVERTISING”

- Fake stores with prices too good to be true
- Sponsored results impersonating real brands
- “Your PC is infected” support pop-ups
- Lookalike login pages, one letter off
- Fake giveaways, coupons & crypto “doubblers”

ANATOMY OF ALMOST EVERY SCAM

1 — THE HOOK

Something that grabs your attention: a delivery, a prize, a warning, or a name you recognize and trust.



2 — THE PRESSURE

Urgency or fear, so you act before you think: a deadline, a threat, a “limited-time” window, a secret to keep.



3 — THE PAYLOAD

What they're really after: your login, a payment, a one-time code, or a single click that installs malware.

Break any one of these three links — slow down past the pressure, verify before the payload — and the scam falls apart. **That's the whole game, and it's learnable in an afternoon.**

CONTINUED → YOUR TAKE-HOME FIELD GUIDE



Your Take-Home Defense

Two things to remember long after the workshop ends: a quick gut-check for any suspicious message, and a calm plan for the moment something slips past you.

THE 3-SECOND GUT CHECK — PAUSE IF A MESSAGE...

- ☐ Creates **urgency or fear** — “act now or else”
- ☐ Arrived **unexpectedly**, even from a name you know
- ☐ Asks for a **password, one-time code, or payment**
- ☐ Pushes you to a **link** instead of the real app or site
- ☐ Sounds **too good to be true** — because it is
- ☐ When in doubt: **stop and verify** through a channel you trust

IF A SCAM GETS THROUGH — ACT FAST

- 1 Stop and disconnect.** Don't send more, click more, or reply. If you suspect malware, get the device off the network.
- 2 Secure your accounts.** Change the password from a device you trust and turn on MFA. Reset anywhere you reused that password.
- 3 Call your bank or card issuer.** Use the number on your card — freeze the card, flag the charge, and reverse what you can.
- 4 Report it.** File at reportfraud.ftc.gov, and ic3.gov for online crime. Reporting protects your record and warns others.
- 5 Watch for round two.** Scammers resell “who paid” lists. Expect a follow-up “recovery” scam — and ignore it.

Prepared by Hacker Watchdog as a free security-awareness resource. Share it freely with family, colleagues, and anyone with a phone and an inbox.