TACTICAL TIPS: AFTER YOU'VE BEEN COMPROMISED

Quick-reference guide for responding to phishing, scams, and cyber attacks

Take a deep breath. Don't be embarrassed. It happens to everyone.
The FBI received 880,418 cybercrime complaints in 2023 with losses exceeding $12.5 billion.

1

DISCONNECT FROM THE INTERNET

Why: If you clicked a malicious link or downloaded an attachment, malware may be trying to contact hackers or exfiltrate your data.

Action: Unplug your Ethernet cable or turn off Wi-Fi/cellular data immediately.

2

CHANGE PASSWORDS (FROM A DIFFERENT DEVICE)

Why: If your computer is infected, hackers can see you typing your new password.

Action: Use a clean phone or tablet to change passwords. Use a password manager. If you reused that password anywhere, change those too.

3

ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Why: Even if hackers have your password, MFA stops them without your phone or authenticator app.

Action: Enable immediately for email, banking, and social media accounts.

4

CONTACT YOUR FINANCIAL INSTITUTIONS

Why: If you shared banking info, act fast to prevent unauthorized transactions.

Action: Call your bank's fraud department. Ask to freeze the account or cancel compromised cards.

5

PLACE A FRAUD ALERT

Why: This makes it harder for scammers to open new accounts in your name.

Action: Contact ONE of the three major credit bureaus (Equifax, Experian, TransUnion). They must notify the others.

6

SCAN YOUR DEVICE FOR MALWARE

Why: Your device may have been infected with malicious software.

Action: Run a full antivirus scan before reconnecting to the internet. If concerned, have a professional wipe and reinstall the OS.

7

CHECK EMAIL FORWARDING RULES

Why: Hackers often set up forwarding rules to receive copies of your emails even after you change your password.

Action: Go to email settings → Forwarding and POP/IMAP. Remove any unknown email addresses.

Report incidents to: ic3.gov (FBI) • identitytheft.gov (FTC) • Your local police department