Five Warning Signs of a Digital Scam

Pause. Check. Protect yourself.

Scammers count on urgency, not your lack of intelligence.

A convincing message can catch anyone off guard. Scammers imitate banks, delivery companies, employers, friends, and even government agencies. Their goal is to push you into acting before you have time to verify what is happening.

1. Someone wants you to act immediately

Messages such as 'Your account will close in 10 minutes' or 'A loved one is in danger' are designed to create panic. Real problems can be urgent, but urgency alone is not proof that the sender is legitimate. Pause and verify through a channel you choose.

2. You are asked to share a password or verification code

A caller may say they need the one-time code that just appeared on your phone. That code may allow someone else to access your account. Do not share passwords, passkeys, or one-time sign-in codes with unexpected callers or messages.

3. The payment instructions are unusual

Be cautious if someone insists on gift cards, cryptocurrency, wire transfers, or payment through an unfamiliar link. A demand for secrecy or a specific irreversible payment method is an especially strong warning sign.

4. A link or sender address looks almost right

Fraudulent messages may use a familiar logo and a web address with one extra letter, an odd domain, or a misleading subdomain. Instead of tapping the link, open the company's official app or type its known address yourself.

5. Someone asks for remote access to your device

Unexpected 'tech support' calls or pop-ups may claim your computer has a virus and ask you to install remote-access software. Close the message and contact support using a number or website you independently verify.

A simple response plan

STOP before clicking or paying. VERIFY using a trusted number or app you opened yourself. PROTECT your accounts: if you already shared information, change the affected password from a trusted device, enable multifactor authentication, and contact the relevant institution promptly.

If you think you were targeted

In the United States, report scams at ReportFraud.ftc.gov. For suspected internet crime, you can also submit a report at ic3.gov. If money was sent, contact the bank or payment provider immediately; speed may matter.

Try this with your family

Ask: 'What is the first thing you would do if a text said your bank account was frozen?' Practice answering: 'I would open my bank app or call the number on my card—not the number in the message.'