

Stop. Switch. Confirm.

A simple response to AI phishing, cloned voices, fake video, and urgent requests.

STOP

Do not click, pay, share a code, send documents, or reply while a message is pushing urgency.

SWITCH

Leave the message. Open the real app, saved contact, or known website yourself.

CONFIRM

Verify the request with a person you already know using contact information you already trust.

Do

- Call back using a saved number.
- Check important facts against a trusted source.
- Use approved tools and approved accounts.
- Report suspicious messages and accidental clicks quickly.

Don't

- Trust a voice, face, logo, email display name, or caller ID by itself.
- Use the phone number, link, or QR code provided by a suspicious message.
- Pay by gift card, wire transfer, cryptocurrency, or payment app because a caller demands it.
- Paste confidential, personal, financial, health, legal, employee, or client information into an unapproved AI tool.

RECOGNIZE THE PATTERN

Phishing may look polished now

AI can remove the spelling mistakes people once relied on. Watch what the message is trying to make you do.

Signal	What it looks like
Unexpected	The message arrives without normal context.
Urgent	It says act now, keep it secret, or skip approval.
Sensitive	It asks for passwords, codes, money, documents, or personal data.
Off-channel	It pushes you to a new number, app, QR code, or shortened link.
Almost right	The domain, invoice, title, or signature is close but not exact.
Borrowed authority	It claims to be a boss, bank, vendor, police officer, or government agency.

Phone calls and voice messages

A cloned voice can sound like someone you know. Hang up. Call the saved number. Ask a private question or use a family/team code word set before an emergency.

Remember

A real emergency can survive a 60-second verification. A scam depends on preventing it.

If you clicked or shared information

1. Stop interacting with the message.
2. Contact your organization, bank, or account provider using a known channel.
3. Change affected passwords and protect accounts with multifactor authentication.
4. Report fraud at [ReportFraud.ftc.gov](https://www.ftc.gov/ReportFraud); report internet crime at [IC3.gov](https://www.ic3.gov).

AI Without Fear | ai-wf.org