AI Scam Pause-and-Verify Checklist

A calm response card for suspicious emails, cloned voices, urgent requests, and exposed details

Pause

- [ ] Do not click, reply, pay, move the conversation, or share a code while the request feels urgent.
- [ ] Save the message, phone number, voicemail, or screenshot only if doing so is safe.
- [ ] Do not call the number, use the link, or follow the contact instructions inside the suspicious message.

Verify outside the message

- [ ] Use a phone number, app, bookmark, statement, or official website you already trust.
- [ ] Ask the person a private question or use a family safe word for an apparent emergency.
- [ ] For a workplace request, contact the colleague or approver through the normal channel.
- [ ] Check the full sender address, domain, request, attachment, destination, and payment method.

If you already acted

- [ ] Contact the bank, payment provider, employer, or affected service using an official channel.
- [ ] Change an exposed password from a trusted device and change reused passwords too.
- [ ] Revoke sessions, reset recovery methods, and tell trusted contacts if the account may send messages.
- [ ] Report the incident to the relevant platform and local authority; preserve evidence.

Family or team plan

- [ ] Safe word or verification question location: _____
- [ ] Primary trusted contact: _____ Backup: _____
- [ ] Bank or IT security number source: _____
- [ ] Rule: no payment, password, or one-time code based only on an incoming message or call.

A convincing voice, polished email, or familiar name is not identity proof. Verify through a channel you choose.

Continue on H5W

Source guide: https://www.h5w.com/how-to-spot-an-ai-phishing-email/

Spot an AI phishing email: https://www.h5w.com/how-to-spot-an-ai-phishing-email/

Avoid AI voice scams: https://www.h5w.com/ai-voice-scams/

Information last verified: October 18, 2026. This resource is general educational guidance. Check current official rules and professional advice when the decision is high impact.