



UNAUTOMATED
THE HUMAN INTELLIGENCE PROJECT

PRACTICAL GUIDE 003

THE DEEPPAKE VERIFICATION FIELD GUIDE

A practical pause, verify, document guide for parents,
educators, managers, and everyday life.

FREE EDUCATIONAL RESOURCE

Plain language. Practical tools. Human judgment.

unautomated.org

The Deepfake Verification Field Guide

Synthetic audio, images, video, messages, and documents can now imitate people and events with enough realism to create confusion before anyone has time to investigate. This field guide is designed for moments when something feels urgent, emotional, unusual, or difficult to verify.

HOW TO USE THIS RESOURCE

Use the PAUSE. VERIFY. DOCUMENT. sequence whenever a message, call, image, video, or instruction could cause money to move, credentials to be shared, a person to panic, a reputation to be damaged, or an important decision to be made.

The core rule

PAUSE. VERIFY. DOCUMENT.

Urgency is often part of the attack. Slow the decision down. Verify through a channel you choose. Preserve enough information to understand what happened.

PAUSE

Do not send money, share passwords, disclose private information, click an unfamiliar link, transfer funds, change banking instructions, or make a high consequence decision simply because a message sounds urgent. Emotion is a signal to slow down.

VERIFY

Contact the person or organization through a trusted channel that you already know. Use a saved phone number, official website, known email address, established family code word, internal directory, or another independent source. Do not rely on the contact information supplied in the suspicious message.

DOCUMENT

Save the message, email, voicemail, image, video, caller information, time, account details, and what action was requested. Screenshots and notes can help your organization, financial institution, school, platform, insurer, or law enforcement understand what occurred.

One page verification flow

1	STOP	Is the message asking for money, credentials, secrecy, urgency, a change in procedure, or an emotional reaction?
2	SEPARATE	Move away from the message. Do not use its links, reply address, phone number, or payment instructions to verify it.
3	VERIFY	Contact the real person or organization through a trusted independent channel.
4	CHALLENGE	Ask something the impersonator would not reasonably know, or use an established code word or internal verification process.
5	CHECK	Look for corroboration. Does the request fit normal behavior, timing, policy, location, and context?
6	DOCUMENT	Preserve the suspicious content and record what you did.
7	ACT	Only proceed after independent verification. If verification fails, report and contain the incident.

Four situations where verification matters

A parent receives an emergency call

A caller sounds like a child or grandchild and says they are hurt, arrested, stranded, or in danger. The caller may plead for secrecy or immediate payment. End the call. Contact the family member directly through a known number. Contact another family member if necessary. Do not let the voice alone become proof.

An employee receives executive instructions

A message or voice call appears to come from an owner, CEO, manager, or vendor asking for a wire transfer, gift cards, payroll information, credentials, or a change in payment instructions. Follow the organization's independent verification procedure before taking action.

An educator receives a damaging image or video

A synthetic image, audio clip, or video may falsely depict a student, teacher, or parent. Do not amplify it while trying to determine whether it is real. Preserve the original, limit circulation, document the source, and involve the appropriate safeguarding, administrative, or law enforcement resources when needed.

A manager sees a viral clip

A video or screenshot may appear to show an employee, customer, public official, or organization doing or saying something consequential. Before responding publicly or taking disciplinary action, seek the original source, independent reporting, context, metadata when available, and direct confirmation.

Signals that should increase caution

- Unexpected urgency, secrecy, fear, embarrassment, or pressure to act before checking.
- A request to bypass normal payment, approval, security, or communication procedures.
- A new bank account, payment destination, phone number, email address, or messaging account.
- Audio or video that is persuasive but arrives without reliable context or provenance.
- A familiar person behaving in an unfamiliar way, especially around money or sensitive information.
- A request for one time codes, passwords, account recovery information, or remote access.
- Claims that discourage independent verification, such as 'do not call anyone else' or 'I cannot talk again.'

What technology can and cannot tell you

Detection tools can sometimes identify signs of synthetic media, but no single detector should be treated as final proof. Compression, editing, screen recording, poor lighting, new generation techniques, and ordinary artifacts can produce false positives and false negatives. Verification is strongest when it combines technical clues with independent human confirmation, trusted channels, provenance, records, and context.

THE HUMAN QUESTION

Am I about to treat something as true because it looks or sounds convincing, or because I have actually verified it?

Build a family or workplace verification habit

- Choose a family code word or workplace challenge procedure before an emergency.
- Require a second channel for unusual financial instructions.
- Use saved contacts and official directories rather than numbers supplied in urgent messages.
- Teach people that ending a suspicious call is not rude. It is a security step.
- Make it normal to verify unusual requests from leaders, relatives, vendors, and colleagues.
- Document suspicious incidents so patterns can be recognized later.

If there is immediate danger: Use an independently verified emergency or official contact. Do not rely only on instructions contained in the suspicious message.