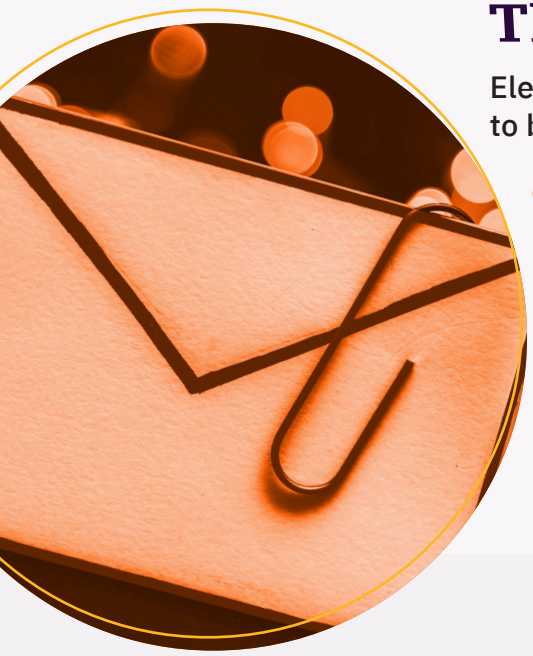
Phishing Threats

ESSENTIALS FOR SAFEGUARDING ELECTION INFRASTRUCTURE

ELECTION SECURITY *Exchange*

Phishing is a type of cyberattack where criminals trick people into giving away sensitive information, like passwords, voter data or access to election systems. They do this by pretending to be a legitimate or trustworthy entity. This often happens through emails, text messages, phone calls or fake websites that look or sound real but are designed to fool you.



Threats to Election Infrastructure

Election officials are frequent targets of phishing attacks or attempts due to both the sensitive information you handle and the nature of your work.

- As part of their job, election officials must frequently open emails from strangers. It is challenging to know if the email that you are opening is from a UOCAVA voter or from an attacker.
- Downloading attachments is part of the job. Critical UOCAVA documents, FOIA requests and files from vendors, frequently come as attachments, which attackers could exploit.
- Election vendors frequently distribute critical files as attachments, creating even more opportunities for attackers to exploit.

Methods of Phishing

Phishing is not just about email. Attackers can use several variations to trick people into giving up information or access.

Spearphishing. A targeted attack where the attackers use personal details like your name, job title or recent activity to make the message look real. There is also something called *whaling*, where the attacker targets the "big phish" like CEOs, chief election officials, etc.

Vishing. Phishing, but over the phone (voice phishing). Attackers call, pretending to be from a trusted organization, and try to build trust to either get access to information or systems.

Quishing. Phishing through QR Codes, where scanning the QR code takes the user to a fake website that steals information or installs malware.

Smishing. Phishing via text message. The attacker might send a text with a link, ask the user to download an app, or start a conversation.

Red Flags

Recognizing phishing is the first step to mitigating the risk. The warning signs of a phish might include:

- Urgency implied by security changes, pushing you to act quickly
- Sender's address is unknown or looks slightly different than what you would expect—coming from a .com instead of .gov or the use of the number 1 instead of letter "l"
- Generic greeting, no personalization; using terms like "Dear Customer" instead of your name
- Awkward phrasing, poor grammar or misspelling

With the rise of AI, attackers are creating phishing emails that are more polished and believable than ever before.

Additional warning signs include:

A link does not go to the same website as displayed

There is an attachment when you don't expect one

The attachment type does not match the extension (e.g., looks like a Word document but ends in *.exe*)

Mitigations

POINT 1: *Check the file extension and hyperlink*

- Attackers mask the website a link is sending you to, so hover over the links to view the hyperlink. If it doesn't match, do not click.
- Attackers disguise malicious files as commonly used file types, so do not download any documents that do not match the type of file expected.
- Always check with IT before downloading any executable (.exe) file type.
- Contact your IT department about any attachment that you're unsure about.

POINT 2: *Verify the sender*

- Don't trust display names alone. If it's from a generic Gmail or Yahoo account instead of the vendor's domain, stop and verify.

POINT 3: *Pause for urgency*

- Urgency is a classic phishing tactic. If it seems urgent, pause, take a breath and assess if it seems out of the ordinary.

POINT 4: *Use an alternate channel*

- Don't reply to the suspicious email or stay on the same call. Instead, use a different communication channel. For example, if they send an email, follow up with a call or text.

POINT 5: *Sandbox when possible*

- If your jurisdiction has a sandbox or IT security team, submit the file for analysis before opening it.