SECURE OUR WORLD

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

OUTSMART online outlaws

Avoid Phishing Scams with Three Simple Tips

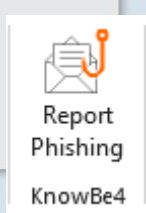
Phishing scams are online messages designed to look like they're from a trusted source. We may open what we thought was a safe email, attachment or image only to find ourselves exposed to malware or a scammer looking for our personal data.
The good news is we can take precautions to protect our important data. Learn to recognize the signs and report phishing to protect devices and data.

1 Recognize the common signs

- Urgent or emotionally appealing language
- Requests to send personal or financial information
- Unexpected attachments
- Untrusted shortened URLs
- Email addresses that do not match the supposed sender
- Poor writing/misspellings

2 Resist and report PHISHING SPAM

Report suspicious messages by using the "Report Phishing" feature.
Once you click the "Report Phishing" button, the email is moved to your Deleted Items folder and a report is sent to the Security Operations Center team within MaineIT to investigate.



3 Delete

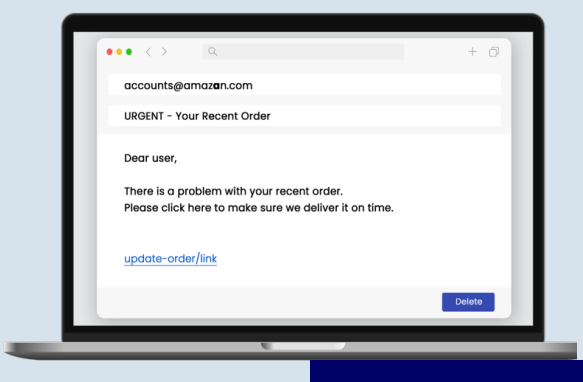
Delete the message. Don't reply or click on any attachment or link, including any "unsubscribe" link. The unsubscribe button could also carry a link used for phishing. **Just delete.**

DELETE

If a message looks suspicious, it's probably phishing.

But even if there's a possibility it could be real, don't click any link, attachment or call any number. Look up another way to contact a company or person directly:

- Go to a company's website to find their contact information
- Call the individual at a known number and confirm whether they sent the message



CYBERSECURITY AWARENESS MONTH

maine OIT

MaineIT
Information Security Office