



501CISO

501C CYBERSECURITY LEADERSHIP

Powered by ClearTone Consulting, LLC

DIGITAL DECEPTION: STRENGTHEN YOUR DEFENSES

Phishing attacks are a prevalent form of cybercrime where attackers masquerade as trustworthy entities to steal sensitive information. Nonprofits and associations, often handling valuable data, need to be vigilant and knowledgeable to thwart these threats.

Identifying Suspicious Emails

Check the Sender's Address:

Red Flags: Misspellings, unfamiliar domains, or addresses that don't match the supposed sender's organization.

Action: Cross-reference email addresses with previous correspondence or official contact information.

Look for Urgent or Unusual Language:

Red Flags: High-pressure tactics, threats, or language that creates a sense of urgency.

Action: Treat any email evoking urgency with suspicion, especially if it requests sensitive information.

Avoid Clicking on Unknown Links or Attachments:

Red Flags: Unexpected attachments or links, especially from unsolicited emails.

Action: Hover over links to preview the URL before clicking and avoid opening attachments from unknown sources.

Verifying Requests for Sensitive Information

Double-Check Requests:

Why It Matters: Phishers often impersonate officials to extract information.

How to Verify: Contact the sender directly using known and trusted contact information, not the details provided in the suspicious email.

Use Alternative Communication Channels:

Best Practice: If an email requests sensitive information, confirm its legitimacy through a different communication method, like a phone call.

Additional Best Practices

Regular Staff Training:

- Educate staff and volunteers on recognizing and responding to phishing attempts.
- Conduct mock phishing exercises to test awareness.

Implement Email Filters:

- Use email filtering solutions to help detect and block phishing emails.

Update and Patch Regularly:

- Keep your systems and software up-to-date to protect against phishing scams exploiting vulnerabilities.

Awareness and proactive measures are key in protecting your organization from phishing attacks. By educating your team and implementing best practices, you can significantly reduce the risk of falling victim to these deceptive tactics.

For more info, contact: info@501ciso.com



501CISO
501C CYBERSECURITY LEADERSHIP

