University of
CINCINNATI

Phishing

Phishing involves a malicious actor deceiving you into interacting with a suspicious email, making it one of the foremost cyberattack methods.

What are some signs of a phishing email?

- Be cautious of emails requesting sensitive information like passwords or Social Security numbers.
- Exercise caution when encountering suspicious attachments or links within the email.
- Pay attention to email content with bad grammar and misspelled words.
- Maintain skepticism regarding offers or deals that appear excessively advantageous.

How do I report a phishing email?

- Identify a suspicious email from the Red Flags listed above.
- Click the **"Report"** button in Outlook or forward the suspicious email to infosec@uc.edu.

How can I avoid phishing attacks?

- Be skeptical of unsolicited emails. Avoid opening emails from unknown senders.
- Verify email addresses. Check the sender's email address carefully.
- Don't click on suspicious links. Hover your mouse over links in emails to preview the URL before clicking.
- Don't share personal or financial information.
- Use Multi-Factor Authentication (MFA) to add an extra layer of security, such as Duo Mobile Security.

For any Cyber Security questions, please visit the Office of Information Security or email us at infosec@uc.edu