COMPLIANCE CLIPS

Resource Companion

Click to View

DON'T GET
HOOKED
Recognize & Avoid Phishing Attacks

This resource summarizes key highlights presented in the associated Compliance Clips video. Click Here for other compliance related resources.

WHAT IS PHISHING?

Phishing (also known as social engineering), refers to a technique that is often used to trick people into giving up their personal information.

Phishing attacks typically come in the form of fraudulent email messages that appear to have come from a legitimate source, such as your university or bank. Phishing emails will usually direct to a spoofed website or trick the receiver into divulging personal information like account passwords, credit card information, etc.

WHAT TO LOOK FOR?

While not contained in every phishing email, the following common signs and cues may serve as possible red flags.

Scare tactics / urgent requests	Phishing attacks are known for attempting to induce panic in the receiver and cause the person to act without verifying the legitimacy of the claim or the request
Spoofed link text	Because the actual destination of hyperlinks can be hidden behind spoofed link text, be sure to carefully scrutinize the actual URL address. **Note**: This may not be the case at UConn since Microsoft Advanced Threat Protection is used. As a result, destination links may appear garbled.
Bad spelling or grammar	Phishing messages are notorious for containing misspelled words or poor grammar.
Mismatched email address information	Remember to check the sender's name to view the actual "reply-to" email address
Generic signature lines	Review the message for an official UConn Health or UConn signature to indicate the message is from a trustworthy sender.
Unexpected requests	Be cautious about unexpected requests regarding personal information. Always be suspicious of any unsolicited communication or requests from contacts you did not initiate.

HOW TO RESPOND TO A PHISHING SCAM?

Recognize Red Flags – Start by reviewing the email for common warning signs, such as those outlined herein.

Take Action – If you suspect that you have receive a phishing email, immediately report it and delete it from your inbox.

Report Phishing Emails by forwarding them to:

UConn	reportphishing@uconn.edu
UConn Health	servicedesk@uchc.edu

If you clicked on a phishing email or shared personal information, immediately:

Change your password directly through the following official UConn or UConn Health website.

UConn	netid.uconn.edu
UConn Health	remote.uchc.edu

Review account statements and activity. Note: ITS monitors for suspicious activities associated with phishing attacks.

Run a virus scan on your computer to detect and remove any potentially harmful software downloaded on your system after clicking on a link.

UCONN RESOURCES

- UCONN PHISHING EDUCATION WEBSITE
- REPORT PHISHING AT UCONN
- NETID HOMEPAGE (PASSWORD RESET)

UCONN HEALTH RESOURCES

- CYBER SECURITY AWARENESS MATERIALS
- REPORT PHISHING AT UCONN HEALTH
- SERVICE DESK (PASSWORD RESET)

Office of University Compliance
Individual Responsibility • Institutional Success

UCONN