COVID-19 Phishing Scams

Attackers are taking advantage of the COVID-19 pandemic by sending phishing emails that look like important IT notifications, charities or legitimate awareness training.

Remember the ways to identify an email as a phishing scam.

Some red flags include:

- Urgent requests originating from outside of Uconn Health. Phishing attacks attempt to induce panic in the receiver and cause the person to act before investigating the authenticity of the request.
- Bad spelling or grammar. Phishing messages are notorious for containing misspelled words or poor grammar.
- Mismatched email address information. Make sure the email address displayed in the From: field matches address listed in behind mailto:.
- Generic signature line. A university message is typically signed by a university official, whose name you can verify, and have credible contact information.
- Unexpected requests regarding personal information. Be extremely wary of following links or answering questions from contacts you did not initiate.

Below are actual Phishing emails Uconn Health has received during this crisis:

*** Attention: This is an external email. Use caution responding, opening attachments or clicking on links. ***
Message sent from a system outside of UConn.

Office 365 ***Coronavirus Review***

Recent Update on Coronavirus disease (COVID-19)
COVID-19 ID: #NIPH

CASE ID: Coronavirus
EMMERGENCY NO: 911 - 112
EMAIL ID: EDCARN@ who.int

REVIEW NOW;:

Review on how to recover from covid-19.

De : GILLIS Bernadette
Envoyé : lundi 23 mars 2020 12:37
Objet : COVID-19 Mail Upgrade

Today, March 2020, we are upgrading our email system to Microsoft Outlook Web App 2020 due to the ongoing COVID-19. This service offers more storage space and easier access to the COVID-19 update. Click the link below to update your account and enter your activation information.

Click here to activate it.

If you are unable to complete the information, your account will be deactivated.

Thank you very much.
Advice center,
(@) 2020. All rights reserved.

From: Yinka Lowe <Yinkalowe@outlook.com>
Sent: Friday, March 20, 2020 6:12 PM
Subject: UNICEF: COVID-19

Hello there,

Due to the pandemic going on you have an important email from UNICEF. **CLICK HERE** and sign in with your school ID to read.

Regards

Always remember, if it looks suspicious, report it to IT Security using the Phish Alarm button in your Outlook toolbar: