



Phishing



Don't take the bait

91% of successful cyberattacks begin with a phishing scam

What is Phishing?

Phishing is a cyber attack that uses email messages trying to trick people into performing specific actions - clicking on a malicious link or attachment - or willfully providing sensitive information like usernames and passwords.

Spear Phishing is where the scam message is customized for a particular person or department. A common spear phishing scam targeting campus is the Gift Card Scam where you're asked to buy gift cards for your boss and reply back with the activation codes.

The image below shows some of the common signs that a message could be a phishing attempt.

Social Engineering Red Flags

- FROM**
 - I don't recognize the sender's email address as someone I ordinarily communicate with.
 - This email is from someone outside my organization and it's not related to my job responsibilities.
 - This email was sent from someone inside the organization or from a customer, vendor, or partner and is very unusual or out of character.
 - Is the sender's email address from a suspicious domain (like microsoft-support.com)?
 - I don't know the sender personally and they were not vouched for by someone I trust.
 - I don't have a business relationship nor any past communications with the sender.
 - This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I haven't communicated with recently.
- TO**
 - I was cc'd on an email sent to one or more people, but I don't personally know the other people it was sent to.
 - I received an email that was also sent to an unusual mix of people. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addressees.
- DATE**
 - Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.?
- SUBJECT**
 - Did I get an email with a subject line that is irrelevant or does not match the message content?
 - Is the email message a reply to something I never sent or requested?
- ATTACHMENTS**
 - The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
 - I see an attachment with a possibly dangerous file type. The only file type that is always safe to click on is a .txt file.
- CONTENT**
 - Is the sender asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?
 - Is the email out of the ordinary, or does it have bad grammar or spelling errors?
 - Is the sender asking me to click a link or open up an attachment that seems odd or illogical?
 - Do I have an uncomfortable gut feeling about the sender's request to open an attachment or click a link?
 - Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

KnowBe4
Human error. Conquered.

What should I do?

If you think you have received a phishing message:

- Do not respond
- Forward the message to **spam@uwindsor.ca**
- Delete it

If you clicked on a link or opened an attachment:

- Contact the ITS Service Desk at **ext. 4440**
- Change your UWinID password by going to the University of Windsor website and click on "Manage UWin Account" in the footer at the bottom of the page and then select "Change Your Password".

PRINT & POST THIS FLYER

We're here to help!

IT Services is happy to answer questions about cybersecurity on campus: **ext. 4440** or open a ticket for service here: **uwindsor.ca/itshelp**. More information on cybersecurity issues facing campus: **uwindsor.ca/cybersecurity**