Signs of Spear Phishing

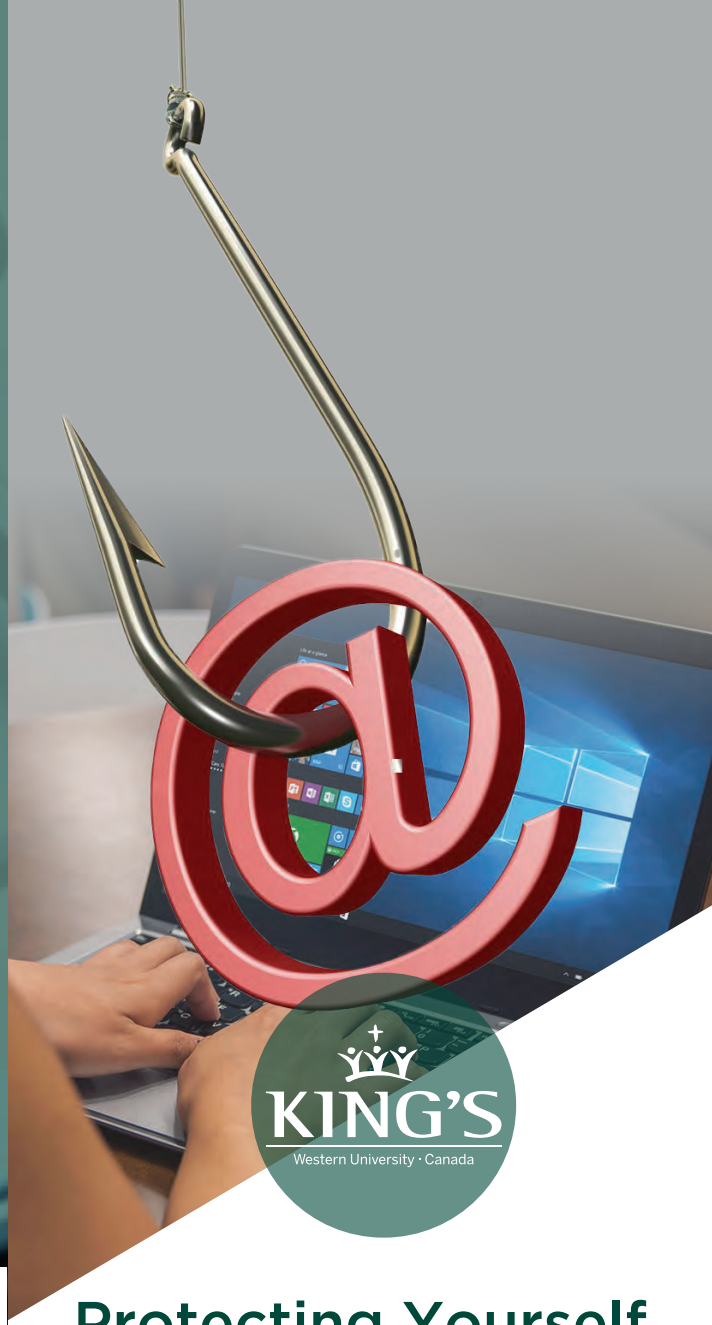
- **"Are you available" or "Are you at your desk"** - This type of email generally does not include any clear indicators of Spear Phishing. It is an attempt to fool you into responding. Once the attacker has you engaged in a conversation, further emails will be designed to compromise
- **"In a meeting Its Urgent" or "Need help fast"** - The sender is too busy to talk and only available via email. Urgency is implied within the subject or body of the email
- **Email "From" and "Reply To"** - Either do not match or the spelling of the email address is slightly different than expected. (e.g. Instead of jmortas37@uwo.ca the address might be jmortas37@uwo.co or jmortas37.uwo.@gmail.com)
- **Authoritative Sender** - These types of email appear to have come from someone known to yourself and in a position of authority. (Manger, Director, Professor, Dean, AVP, VP etc.) The intent is generally to get you to pay an invoice, transfer funds, purchase something etc.
- **Email Thread is Legitimate** - Hijacking of email threads, whereby an attacker embeds themselves into an already ongoing conversation, masquerading as the original person you were communicating to, are becoming more prevalent.

Protecting Yourself

- Develop the habit of scrutinizing every email for key indicators.
- Do NOT supply your King's/Western credentials (Username and Password) to any email request, link, or website unless certain it is for a legitimate King's/Western purpose. (King's/Western will NEVER ask for your password)
- Do NOT click on links embedded anywhere in suspicious email.
- Do NOT open attachments in suspicious email
- When in doubt if an email or its content are malicious, call the helpdesk at 519-433-3491 x.4441
- If the email requires action on your part, find an alternative method of communication to verify with the sender that the request is legitimate.
- Take some time to participate in learning and awareness programs offered by King's and Western.
- If you suspect that you have already participated in, clicked on, or opened; a conversation, a link, or an attachment, please contact support@kings.uwo.ca immediately.

CONTACT US

Phone: 519.433.3491 x.4441
Email: support@kings.uwo.ca
Website: www.kings.uwo.ca/cyber-awareness



Protecting Yourself and King's from Phishing

Spear Phishing Indicators

FROM

- This email was sent from someone of authority inside Western, but appears unusual or out of character.
- This email was unexpected or is from someone I wouldn't normally communicate with.
- This email is from outside of King's from someone I do not recognize or is not related to my job responsibilities.
- Is the sender's email address correct or does it contain small inconsistencies or a wrong domain? (Hover your mouse over the sender's name to see the actual address)

SUBJECT

- The subject does not match or is irrelevant to the message content.
- The subject contains wording to indi-cate importance, urgency or confidentiality.
- How likely is the subject to be true?

ATTACHMENTS

- Would this sender ordinarily include attachments?
- Does the name of the attachment make sense and are there any spelling inconsistencies?
- If in doubt, have someone scan the attachment before opening it.

LINKS

- The link is asking you to login or provide your Western credentials. (Never give up your credentials or private information without absolute certainty of legitimacy)
- Does the hyper-link point to a legitimate source? (Hover your mouse over the hyper-link to view it's real destination.)
- @kings.uwo.ca email links automatically re-direct through our link scanner for security

CONTENT

- Is the sender asking me to click on a link or open an attachment, possibly to gain something of value or avoid a negative consequence?
- Do the spelling and grammar align with expectations?
- Does the email contain an unusual amount of hyperlinks ?
- Do I have an uncomfortable feeling about this particular email?

SIGNATURE

- If the sender is a legitimate Western employee, does the signature match expectations?
- Does the senders role match expectations?
- Real logos and names alone, do not constitute legitimacy