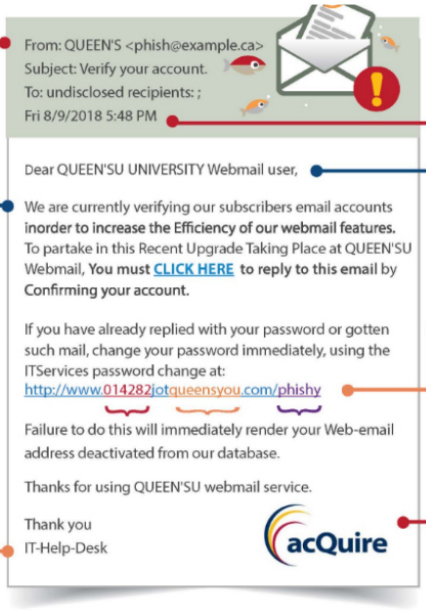
Learn to Identify a Phishing Email

SENDER
Is the email unexpected or from an unknown sender?
Does the display name match the email address?

BODY/CONTENT
Am I being asked to submit or verify confidential information? (e.g. passwords, account, or credit card information)
Am I being asked to click a link or open an attachment to avoid negative consequences? Is there a sense of urgency to the message?
Does the email have spelling errors or bad grammar?

SIGNATURE
Does the sender match the signature and use proper titles and department names?



DATE AND TIME
Is the timing of the email suspicious? (e.g. after business hours, on weekends)

SALUTATION
Is there a generic, inappropriate, inaccurate salutation? (e.g. Dear Customer)

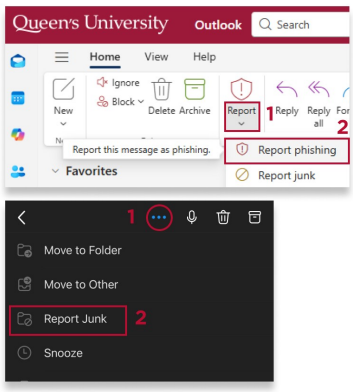
LINK
Does the URL start with a number, contain mispellings, or have an odd ending?

LOGO
Brands and logos can be easily copied.

What do I do if I get a phishing email?

DO NOT:

- **Respond** to the email.
- **Click** any links.
- **Open** any attachments.
- **Provide sensitive info.**



REPORT

the email using the "Report" button on Outlook (desktop) or "Report Junk" on Outlook (mobile) to advise IT Services of the phishing attack.

What do I do if I've put myself at risk?

SCAN

your system for viruses and apply outstanding system updates. Report results to the IT Support Centre by calling (613) 533-6666.

CHANGE

your NetID password securely and modify your security questions and answers by visiting **netid.queensu.ca**

REMEMBER

Support Centres, legitimate businesses, and financial institutions will never ask you for personal or confidential account credentials via email.

Need help? IT Services has you covered!

(613) 533-6666
queensu.ca/its
Mackintosh-Corry Hall B205
Online Help Form
queensu.ca/its/helpform