

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?

From: QUEEN'S <phish@example.ca>
Subject: Verify your account.
To: undisclosed recipients ;
Fri 8/9/2018 5:48 PM



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 misspellings, or have an odd ending?

LOGO

Brands and logos can be easily copied.

Dear QUEEN'SU UNIVERSITY Webmail user,
We are currently verifying our subscribers email accounts in order to increase the Efficiency of our webmail features. To partake in this Recent Upgrade Taking Place at QUEEN'SU Webmail, **You must [CLICK HERE](#) to reply to this email** by Confirming your account.

If you have already replied with your password or gotten such mail, change your password immediately, using the ITServices password change at:

<http://www.014282jotqueensyou.com/phishy>

Failure to do this will immediately render your Web-email address deactivated from our database.

Thanks for using QUEEN'SU webmail service.

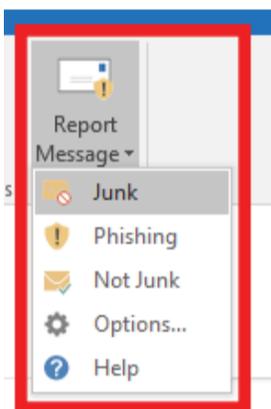
Thank you
IT-Help-Desk



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 Message" button in Outlook to advise IT Services and Microsoft of the phishing attack.

Note: if you are on a mobile device, you can report the email by forwarding it to abuse@queensu.ca

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
Monday - Friday:
8:00am - 4:30pm



queensu.ca/its



Online Help Form
queensu.ca/its/helpform



Mackintosh-Corry Hall B205
Monday - Friday: 9am - 4pm