Queen's University

IT SUPPORT SERVICES
queensu.ca/its/security

HOW TO SPOT A PHISHING EMAIL

SENDER
Is the email unexpected or from an unknown sender?

From: QUEEN'SU UNIVERSITY
Subject: Verify your account.
To: undisclosed recipients: ;
Fri/8/9/2018 5:48 PM

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

SALUTATION
Is there a generic salutation (i.e. Dear Customer)

Dear QUEEN'SU UNIVERSITY Webmail user,

We are currently verifying our subscribers email accounts inorder 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.

BODY/CONTENT
Does the email have spelling errors or bad grammar? (i.e. inorder, QUEEN'SU.)

BODY/CONTENT
Am I being asked to submit or verify personal or confidential information. (i.e passwords, account information or credit card information)?

Am I being asked to click a link or open an attachment to avoid a negative consequence?

If you have already replied with your password or gotten such mail, change your password immediately, using the ITServices password change at:
http://www.014282jotf0rm.com/queensyou

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

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

Thanks for using QUEEN'SU webmail service.

Does the sender match the salutation and use proper titles?

Thank you
IT-Help-Desk

If you answer YES to ONE OR MORE of these questions, then it's most likely a PHISHING EMAIL!

WHAT SHOULD I DO?

If you think you have RECEIVED A PHISHING EMAIL:

1. Do not respond
2. Forward the email to abuse@queensu.ca for action
3. Delete the email

If you HAVE CLICKED ON THE LINK or opened an attachment in the phishing email:

1. **Scan your system** for viruses and report any findings to your local IT Admin Rep. or the IT Support Centre (613-533-6666)
2. **Change your NetID password** by going to **netid.queensu.ca**
   - Click on **Login to manage your account**
   - Change your password
   - Modify your security questions and answers
3. **Contact the IT Support Centre** at (613) 533-6666 if you have not already done so

QUEEN'S UNIVERSITY WILL NEVER ASK FOR YOUR NETID PASSWORD THROUGH EMAIL OR PHONE

ITS
INFORMATION TECHNOLOGY SERVICES

Protecting Your Data and Devices

Information Technology Services
queensu.ca/its

HOW CAN I STAY SAFE?

We live in a world that is more connected than ever before. With all the benefits of the internet there are also dangers, but these dangers can be reduced by being cautious and employing cybersecurity. Help keep your data and devices safe.

PROTECT YOUR DATA

When using a personal or public computer, remember to log out and close the browser.

- Look for secure website using "https", and a closed lock icon in your browser's address bar.
- Never enter confidential information on a website that doesn't use secure encryption.
- Some, (but not all) websites may even display green text or a green shade in the address bar. This indicates enhanced security.
- Never save your password on a public computer.

Secure your mobile devices and browser from unwanted intruders.

- Use a password or pin to lock your device when not in use
- Never leave computers unattended.
- Encrypt any private data and install anti virus on your device.

Make sure to back it up.

- Keep a copy of important files on remote services or external drives. This way, if your device is hit with a Ransom Attack, you have a back up.
- Queen's offers 1 TB of storage on OneDrive for Business. Storing your files here ensures they will be secure and accessible from anywhere, anytime.

Cybersecurity and safe computing are high priority issues for the university. As a higher education institution, Queen's is a target for malicious attacks seeking to obtain unauthorized access to information or systems.

Cybersecurity is a shared responsibility!

PROTECT YOUR DEVICES

Use a strong password on all of your accounts.

- Choose a password that is difficult to guess by using a combination of letters, numbers and special characters.
- Never save passwords in browsers or applications, or share them with anyone else.

Use antivirus and anti-malware software.

- Install antivirus on your computer and mobile devices. Keep it current and scan regularly. (Check out the PC Magazine's ratings and reviews of the top 10 antivirus software protection for 2017.)

Install Updates.

- Stay up-to-date by installing updates for your operating system, browsers and other applications as soon as they become available.

When using wireless, always choose a secure connection.

- On campus use the QueensuSecure_WPA2 network.
- Avoid performing important activities like banking or shopping over a public Wi-Fi.
- When using Bluetooth, make sure security modes are enabled to avoid any chance of a security breach while in public.
- Wi-Fi is considered secure when you need to have an account to access it.

Never leave your computer or device unattended.

- Lock your screen. Always use a screensaver with password protection.
- When finished, log out of all your applications, close your browser and shut down your computer.