Phishing

Version 19

Published 9/24/2021 by Jennifer Kim Last updated 10/2/2024 1:55 PM by Elias Abatneh

---

Phishing emails appear to be legitimate but are trying to trick you. Criminals may try to obtain your private information to conduct identity theft to commit crimes in your name, harm your family or friends, or steal from you.

Phishing emails always try to do these two things:

1. Convey urgency: claim there's an urgent problem that only you can fix, or that you can win a prize if you act without delay
2. Convince you to act: encourage you to click a link, open an attachment, log on to an untrustworthy website, or volunteer your personal information

Phishing emails will often pretend to originate from a company you recognize, government authority, or even Seneca specifically. They can appear to be convincing, but phishing emails often have important differences from legitimate ones:

- The sender does not match the content of the email (e.g., an IT request comes from an unrelated department or faculty)
- Poor grammar and spelling
- Sloppy formatting
- Suspicious claims that only you can solve a problem
- Discourages you from contacting the company to verify
- Language does not match previous emails from the sender (e.g., asking you to purchase iTunes cards, or fix an IT problem)

If you get the feeling that the email you are reading may not be legitimate, examine it more closely to see whether it matches some of these characteristics.

Spam and phishing email protection

Students are safeguarded by Seneca's spam and phishing email protection system. This

service provides additional defence against email threats such as phishing and malware.

Seneca's email protection system provides the following primary benefits:

- Emails with malicious content or attachments will be deleted automatically
- Senders of malicious emails will be automatically blocked from contacting you

While automated email security systems do make email safer to use they are not a replacement for due diligence. Please exercise caution and follow the advice on this page to avoid the harms of malicious email.

What to do if you receive a suspicious email

Do not reply to suspicious emails and do not click any links, including an "unsubscribe" link. If you click a link in a suspicious email please Contact ITS immediately without delay; it's much better to report a potentially harmless activity than to hope nothing bad will happen.

If you're uncertain whether an email is legitimate, verify using another channel. For example, if you receive a suspicious email from a classmate, call them - do not reply to the email itself as it may go to a criminal instead of the intended recipient. Likewise, if you receive a suspicious email from a company, contact them via their website or telephone number - do not reply to the suspicious email.

If you receive a phishing email on your Seneca email address please report it by clicking the **report phish** (red fish) button in MySeneca webmail, the Microsoft Outlook software for Windows and MacOS, and in the Microsoft Outlook app for Android and iOS (other email apps are not supported at this time).

For more information visit the report an it security incident page.

MySeneca webmail

1. Click the email in your mailbox that you wish to report phish.
2. Click the **...** button at the top right corner of the email message preview.
3. Click the **report phish** button on the top ribbon.
4. Read the message that appears in the message frame on the right side and click **OK** to report phish the email.

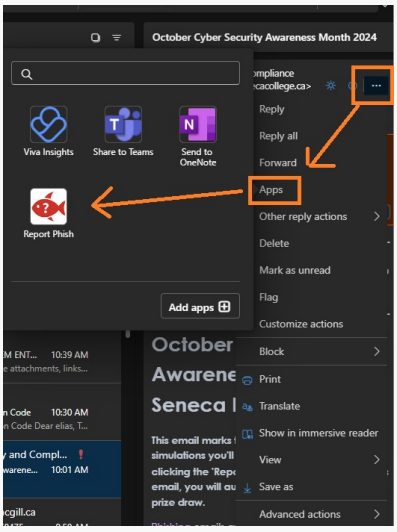
Microsoft Outlook for computers

1. Tap the email in your mailbox that you wish to report phish.
2. Click the **report phish** button.
3. Read the message that appears in the message frame on the right side and click **OK** to report phish the email.

Outlook Smartphone App

1. Tap the email in your mailbox that you wish to report phish.
2. Tap the **...** button at the top right corner of the email message preview.
3. Tap the **report phish** button at the bottom of the screen.
4. Read the message that appears in the message frame on the right side and tap **OK** to report phish the email.

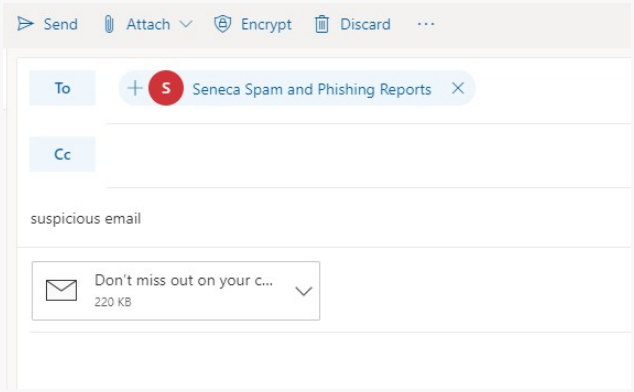
Not seeing the red phish button? Put your browser into full screen display mode or alternatively click on Apps under the 3 dots.



Alternatively, if the **report phish** button is not available, you may forward the email (preferably as an attachment) to ItIsSpam@senecapolytechnic.ca:

1. Click the **New message** button.
2. Type "ItIsSpam@senecacollege.ca" in the To field.

3. Click and hold the mouse button on the suspicious email and drag it into the new email.
4. Write a brief description of the threat in the subject and body of the email.
5. Click the **Send** button.



If you receive a phishing email on your personal (non-Seneca) email address, we recommend sending a copy to the Canadian Anti-Fraud Centre.

Telephone scams

Similar to phishing emails, criminals may pose as legitimate businesses (such as Microsoft or Dell) or government agencies (such as the Canada Revenue Agency or the police) to trick you into giving up your private information.

Never give your personal information to someone who has called you. If this happens, ask for the name and company of the caller, hang up, look up the main number for the company yourself (don't trust any number they give you), and ask for that person. If they can connect you back to the caller you can verify whether the request is legitimate.

Contact us

If you have any further questions please Contact ITS for assistance.

tags : email-protection, it-security, phishing-emails, spam-emails, suspicious-email, telephone-scam