



# Have you received a phishing email?

If you're unsure, watch out for these signs:



1. Sender is an unknown email contact OR sender is a known email contact, yet the message and/or links contained are out of the ordinary.



2. The overall content seems odd, unexpected and/or conveys a false sense of urgency.



3. Contains instructions to click a link, download an attachment, enter your credentials and/or send money or gift cards.



4. Includes phony links (tip: hover over link(s) with your cursor to see where they actually lead).



5. Has spelling or grammatical errors, yet beware that many sophisticated attackers will use professional language too.

   @ITSUOFT | @UOFTCYBERAWARE

**SECURITYMATTERS.UTORONTO.CA**



**Cyber Security  
Awareness Month**  
ONE TEAM. ONE GOAL. October 2019



UNIVERSITY OF  
**TORONTO**

## If you suspect a phishing attempt or attack, keep calm and take the following measures:



1. If you suspect your password may have been compromised, immediately change it at [www.utorid.utoronto.ca/cgi-bin/utorid/changepw.pl](http://www.utorid.utoronto.ca/cgi-bin/utorid/changepw.pl).



2. Immediately report phishing messages to: [report.phishing@utoronto.ca](mailto:report.phishing@utoronto.ca).



3. When in doubt, call or ask the sender in person to confirm the email was really from them.



   @ITSUOFT | @UOFTCYBERAWARE

[SECURITYMATTERS.UTORONTO.CA](http://SECURITYMATTERS.UTORONTO.CA)