SECURITY MATTERS

How to spot a phish

Display name

Verify details in the “From” line. Hover over a display name and check if the address reflects who the person claims they are and where they’re from by matching the domain (@utoronto) to the organization (University of Toronto). When in doubt, call the sender to confirm.

Attachments

Are you expecting attachments or links from this person? Typical phishes are unexpected and you should never open unexpected attachments or links. Remember to report suspicious email activity to: **report.phishing@utoronto.ca**.

Language

Is the language appropriate and professional? Phishing frauds carry a tone that tries to illicit panic, fear and urgency, in order to prompt an immediate action from the recipient. Check for typos and incoherent sentences. Phishing scammers prioritize volume and are prone to making a number of mistakes.

Click-bait

This may include elements like an extreme-sounding subject line, strong messaging and excessive links and buttons. The sender is including as many enticing options as possible to encourage you to open malicious software or program(s).

Do research

Search online for signatures, names, organizations and anything else to verify the message’s legitimacy. If nothing turns up, it’s likely they do not exist.

Visit our “Phish Bowl” at **securitymatters.utoronto.ca** to view reported phishing attempts at the University of Toronto (U of T).

SECURITY MATTERS

Five safe web surfing tips

Password manager

Use a password manager, such as **KeePass** or **Lastpass**, to store passwords for your multiple accounts (i.e., banking, school portal, webmail). This allows users to possess multiple unique accounts without having to memorize several passwords.

Separate browsers

Use two browsers on every device. One for general browsing and one for private and sensitive actions, such as banking and online shopping. Separating your browsers also increases security when saving login information because your general browsing may take you to unsecure sites.

Trusted browser plugins

Using browser plugins can add an extra layer of protection during Internet sessions. For example, **Privacy Badger** allows you to disable tracking and location features, **HTTPS Everywhere** allows you to create encrypted connections whenever possible and **World of Trust** gives websites trustworthiness ratings based on community feedback. Make sure the browser plugin is trusted by downloading it from the original source, and not a third-party.

Guard app permissions

Apps may prompt you for access to your microphone, camera, gallery and location in order to provide a service. In some cases, this information is used for data mining. Provide this information only if/when it is essential to the functionality of the app. Treat app permissions like browser plugins and only download official apps from trusted and verified parties.

Security Matters

Want to learn more about spotting phishing emails and/or how to protect yourself? Visit **securitymatters.utoronto.ca** to find out about recent University of Toronto (U of T) cyber attacks.

SECURITY MATTERS

Practicing cyber safety at work

Beware of urgent messages

Take your time if a suspicious message states that you must take an action immediately. Cyber criminals want you to react without thinking; an urgent call to action makes you more likely to cooperate.

Do not open unexpected attachments

This is the most common method of spreading malicious software. Report emails that contain suspicious links and attachments to **report.phishing@utoronto.ca**.

Spot impersonators

Confirm sender identities by hovering over email addresses and by checking display and domain names.

Cyber criminals often impersonate official businesses, banks, schools and other organizations so it's important to ensure the web address is from the legitimate organization.

If you're unsure whether an email is from someone at your organization, simply call or ask them as a confirmation before taking action.

Avoid suspicious links

Always verify the origin of links in suspicious emails. Simply hover your cursor over link(s) to reveal the URL.

Security Matters

Want to learn more about spotting phishing emails and/or how to protect yourself?

Visit **securitymatters.utoronto.ca** to find out about recent University of Toronto (U of T) cyber attacks.