READY Newsletter
Rochester Institute of Technology

This SPECIAL EDITION of the RIT Ready Newsletter focuses on how to recognize and respond to email phishing attacks.

Phishing is a type of social engineering used to obtain user information fraudulently either by clicking on a malicious link in an electronic communication or otherwise providing personal information. RIT receives many phishing emails every day and you must be able to recognize these sort of attacks to keep RIT and you safe.

How to recognize a phishing email

- **Spelling and grammar errors**. Companies proofread their messages to make sure there are no typos.
- **Personal Information requested**. RIT and other legitimate businesses will never ask for personal information or login credentials through email.
- **Unfamiliar source name and address**. Make sure to read the address of the sender. It should be a recognizable username and domain name.
- **Masked URLs.** Hover your cursor before clicking. Do not click on any links without examining where the URL leads.
- **Urgent and threatening tone**. Read the context of the email to see if the attacker is trying to get you to respond quickly.

If you happen to fall for a phishing attack

1. Report the incident to spam@rit.edu as explained below
2. Delete the email.
3. Change your password.
4. Scan your system for viruses and spyware.

To report a phishing attack to spam@rit.edu

- Report the phish by composing a new message to spam@rit.edu and inserting the suspected phishing email into the new message by dragging it into the new email window and then send it.
- Delete the phishing email after forwarding it.

The RIT Information Security Office web site provides best practices on protecting yourself from phishing and other cyber threats. Visit the page or contact us at infosec@rit.edu to learn more about the best practices to keep yourself safe.

R·I·T Alert

Make sure your mobile phone number is in the RIT Alert system.

- Faculty and Staff – go to myinfo.rit.edu and add in the *phone numbers emergency notification information* area.
- Students – go to SIS and enter in the Cell/Mobile phone field of the *Personal Information* area.