Security Tip of the Week

How to Spot a Phishing Email

It could be a phishing email if...

- There are misspelled words in the e-mail or it contains poor grammar.
- The sender name doesn't seen related to the sender email address.
- The message is making you an offer that is too good to be true.
- The message is asking for personally identifiable information, such as credit card numbers, account numbers, passwords, PINs or Social Security Numbers.
- There are "threats" or alarming statements that create a sense of urgency. For example: "Your account will be locked until we hear from you" or "We have noticed activity on your account from a foreign IP address."
- The domain name in the message isn't the one you're used to seeing. It's usually close to the real domain name but not exact.

For more information on this week's tip visit www.rochester.edu/it/security/securitytipofweek.

Need Help?

Online: www.rochester.edu/it • Email: UnivITHelp@rochester.edu • Phone: 275-2000 (5-2000)