Click Wisely

Phishing Attacks!

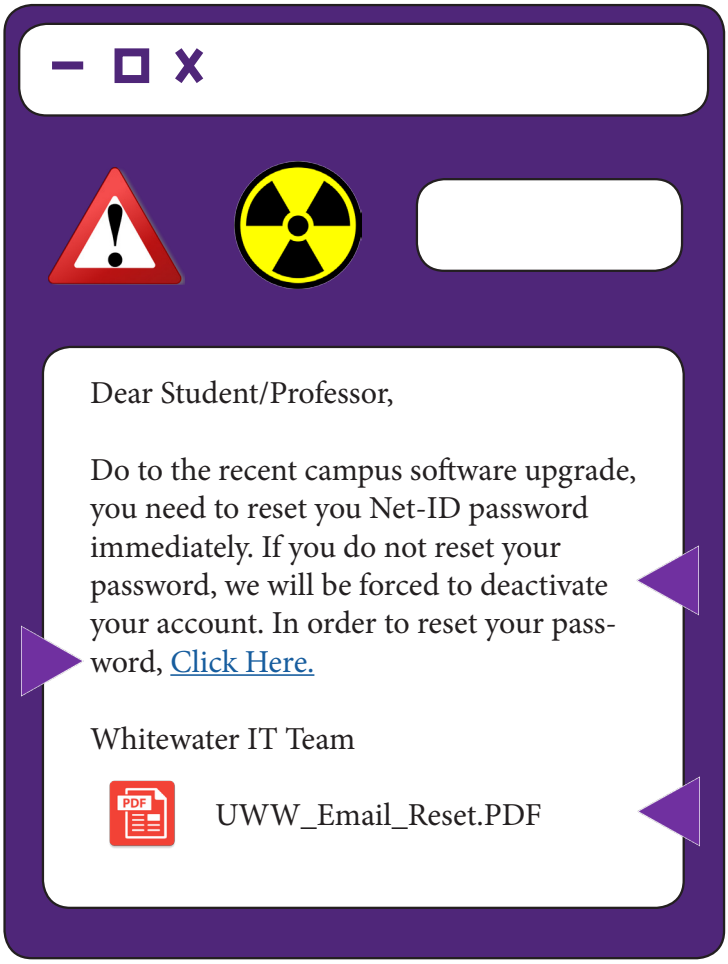
A Phish is an email sent by a cyber criminal to trick you into clicking an unsafe link or file. Always be on the lookout for phishing attacks.

#1 Links

The purpose of a phising email is to trick you into clicking a link. Usually these links look a little "off." Watch out for these tricks.

- Alternate spellings such as Whitwater or Whitewatr.
- Unofficial links such as uww.example.com or uww.tech.net.
- Links hidden behind a URL shortener such as wisc.com/yh83459gr

If the link is just words like **"Click Here,"** hover your cursor over them to show the actual link. On a mobile device you can press and hold.



#2 Content

People are more likely to click if they feel scared. Be suspicious of emails with this sort of content.

- Threats to suspend accounts, remove access or lose items.
- Signs of a phishing message include grammar/spelling issues, unfamiliar email address, messages asking to verify a user's credentials, or offers that seem too good to be true.
- If the content makes you feel like you should act fast, slow down and take time to think.

#3 Attachments

A Phish may also include a file attachement. **DO NOT** open it! It could contain malware. The attachment could also take you to a dangerous phising site. Be safe, be smart and be vigilant.

What should I do if I spot a Phish?

Forward all suspicious emails to suspiciousemail@uww.edu.

Or contact the TSC HelpDesk at 262-472-4357, helpdesk@uww.edu

For more info on IT Security please visit:
uww.edu/icit/services/it-security

UNIVERSITY OF WISCONSIN WHITEWATER
Instructional, Communication & Information Technology