Beware of spear phishing attempts

You could receive an e-mail at work because you are part of a specific group targeted by cybercriminals engaging in spear phishing attacks. Criminals know that one successful ‘bite’ from someone in a well placed position could yield them great profit.

This is how spear phishing works

While Providence has strong firewalls and anti-virus protection, spear phishing can overcome these protections, by gaining the cooperation of internal people. Cybercriminals build a webpage or e-mail that mimics a department inside the organization, or a trusted source used by the targeted users. E-mails from the information services or human resource departments are a common delivery method. Responding to requests to verify passwords enables hackers to penetrate the network and highjack e-mail accounts.

Take these steps to foil phishing attacks

1. Suspicious? Don’t automatically trust the sender information in an e-mail address. Spear phishing attempts appear legitimate because cybercriminals successfully replicate the identity information in e-mails. As always, if you do not know the sender, delete the message.

2. Be aware that phishing is a social engineering technique and hackers rely on your desire to cooperate or help fix a situation. If you are hesitant about a request do not click on any embedded links or provide any information. Close the e-mail and delete it. There is no need to report the suspected attack.

3. Remember a Providence staff member from human resources or information services will never ask you to divulge your password, particularly in e-mail.

If you believe that you inadvertently provided your access credentials to a non-authorized party, report it immediately. A compromised e-mail account can be used to broadcast SPAM or additional phishing e-mails to thousands of computers, including everyone in your e-mail contacts list. Learn more about phishing attacks and protect access to your e-mail account.