Phishing

What is Phishing?

Phishing is typically an email scam which tries to trick people into thinking a legitimate organization is requesting private information. These scams typically ask you to respond quickly, warning you of a sudden change to your account and requesting to supply and verify information that you still the service. These attempts often looks identical to the service the email is mimicking common targets such as the University, your bank, ADP, EBay, and PayPal.

What does a Phishing email look like?

Phishing emails are typically unsolicited and have

- a generic greeting
- warning of some sudden change in an account
- and requires you to verify personal or private information that you still use the service.

These emails either include directions to reply with private information, or provide a link to a malicious web site to verify your account. Emails claiming very sudden changes or those that use poor spelling and grammar are clear warning signs of a fraudulent phishing email.

What should I do if I receive a Phishing email attempt?

Just delete the message. Do not respond in anyway. Always be skeptical when someone is requesting information, and never email your password, bank account numbers, social security, or credit card numbers to anyone. If it seems phishy it probably is.

Will Suffolk send legitimate emails that look like phishing scams?

There will be times when legitimate messages must be sent to inform our email users of necessary changes to their accounts. These may include password expiration notices.

It is very important to remember that Suffolk will never ask for your password in an email. Any password changes will always direct you to the University official website Suffolk.edu.

If you are ever in doubt about the legitimacy of a potential phishing email, please call the University ITS Help Desk at (617)557-2000.

Why can't Suffolk University stop these emails?

Suffolk University stops over a half million phishing attempts, spam emails, and virus infected messages every day, but the methods scammers use change quickly to try to stay ahead of blocking techniques. Additionally, due to the wide range of Suffolk University users we must also be careful not to block legitimate email.

How can I avoid phishing scams?

- Never send passwords, bank account numbers, social security numbers or other private information in an email.
- Avoid clicking links in emails, especially any that are requesting private information.
- Be wary of any unexpected email attachments or links, even from people you know.
- Never enter private or personal information into a popup window.
- Pay attention to the URL (the web site address in your browsers address bar). Look for 'https://' and a lock icon in your browser address bar and confirm the web site address before entering any private information on a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling

What should I do if I have been scammed by phishing?

Contact the organization that was the target of the scam. Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future. For Suffolk University accounts contact the Help Desk (617)557-2000. If you suspect a bank or credit card account may have been compromised, contact that institution to check your account immediately and request a credit report.