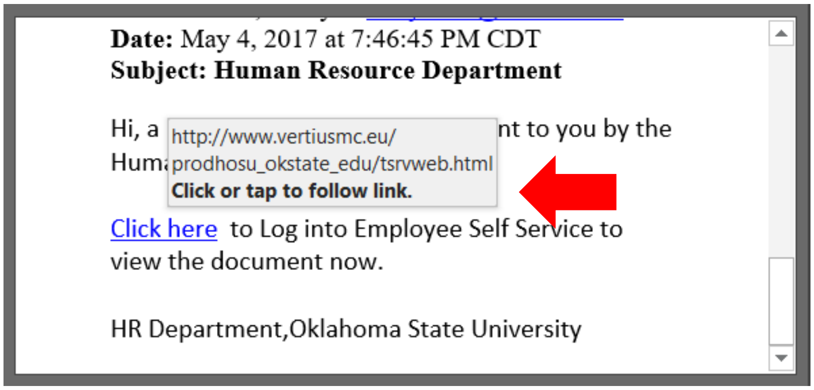
In the past few weeks, we have had a rash of new phishing emails. You have probably noticed one or more of these emails pretending to be from Human Resources or from the IT helpdesk. These emails are getting shorter in length, which can make them a little harder to detect when they are fake. However, they are still very dangerous and should be taken very seriously. Opening links, from phishing emails, can give the creator information about you. Specifically that your email account is active, your name, and could possibly allow them to spoof your email (essentially send emails from your email account.) If you open any attachments, included with these emails, malicious program can be installed on your computer, possibly leading to your information being stolen or worse all your files being encrypted with no way to recover them.

OSU's Central IT email administrators, along with help from information security technicians at Microsoft, work very hard trying to block or remove phishing email before they are delivered However, there is no way for them to remove 100% of all attacks. This means we must be vigilant when checking email to ensure that we are not exploited. How can we do this? By following several very simple rules when looking at emails.

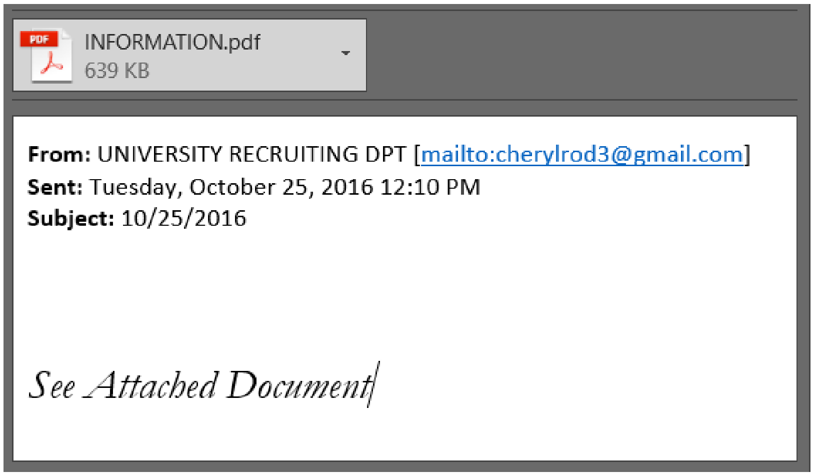
1. Do not assume that all emails from @okstate.edu email address are safe. Email addresses can be easily faked.
2. If the email states it is from someone in HR, does the sender indeed work for HR?
3. Check for misspellings in emails. Phishing emails are notorious for having many spelling or grammar errors.
4. Check link addresses by placing your cursor over the link (do not click the link.) If the address is not an okstate.edu website, do not click on it.
5. Do not open attachments unless you know the sender is real and you expect them to send you something. You can always check with the sender to verify the email.


Date: May 4, 2017 at 7:46:45 PM CDT
Subject: Human Resource Department

Hi, a http://www.vertiusmc.eu/ nt to you by the
Hum prodhosu_okstate_edu/tsrvweb.html
Click or tap to follow link.

Click here to Log into Employee Self Service to view the document now.

HR Department,Oklahoma State University



From: UNIVERSITY RECRUITING DPT [mailto:cherylrod3@gmail.com]
Sent: Tuesday, October 25, 2016 12:10 PM
Subject: 10/25/2016

See Attached Document

When dealing with phishing email, it is always important to question first and act second. It is much easier and it takes much less time to verify an email than it does to remove malware from your computer and deal with the consequences of careless actions. If you receive emails that are spam, please forward them to abuse@okstate.edu. Also, if you have any questions, please contact your Support Specialist.