OCTOBER 2018

OUCH!

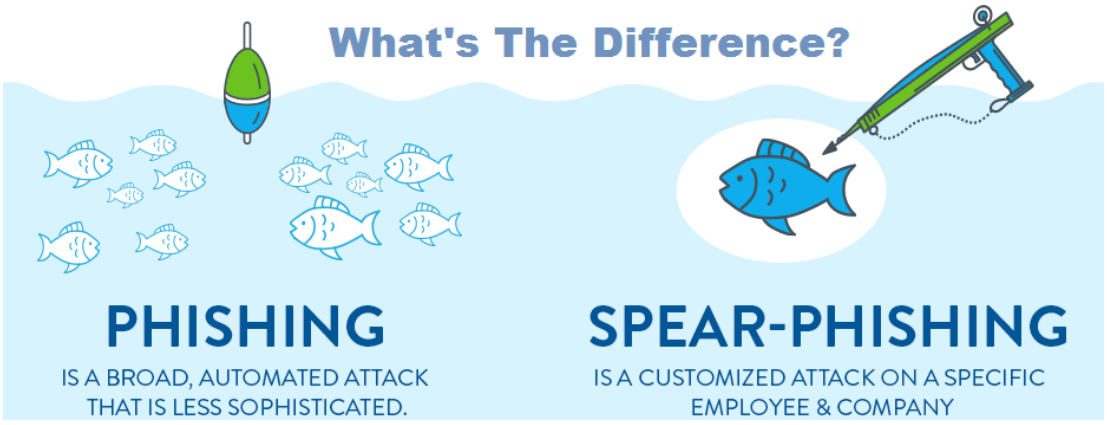
Don't Get Hooked

These days it's hard to tell if an email is a phishing email or not. Thankfully, as phishing relies on human error to succeed, vigilance and common sense form a key part of a strong defense. There are many different types of phishing scams floating around, so it pays to know what steps you need to take when reading your email to tell if it is a legitimate email or a phish.

Types of Phishing

Phishing

The most basic and commonly seen type of attack, of course, is the phishing email. Phishing emails are sent to a group of users who are unique enough to be used as bait but broad enough to ensnare a large number of people. The point is to cast as large a net as possible. In contrast, other forms of attack are much more targeted.



Spear Phishing

Spear phishing, as might be gathered from its title, usually targets a specific person or organization. Since these types of attacks are so pointed, phishers scour the Internet for available information about their target in order to craft a believable email to extort information (if not money) from victims.

Whaling

Whaling is a form of spear phishing directed at executives or other high-profile targets within a business, government, or other organization, such as a CEO or someone who has access to financial assets.

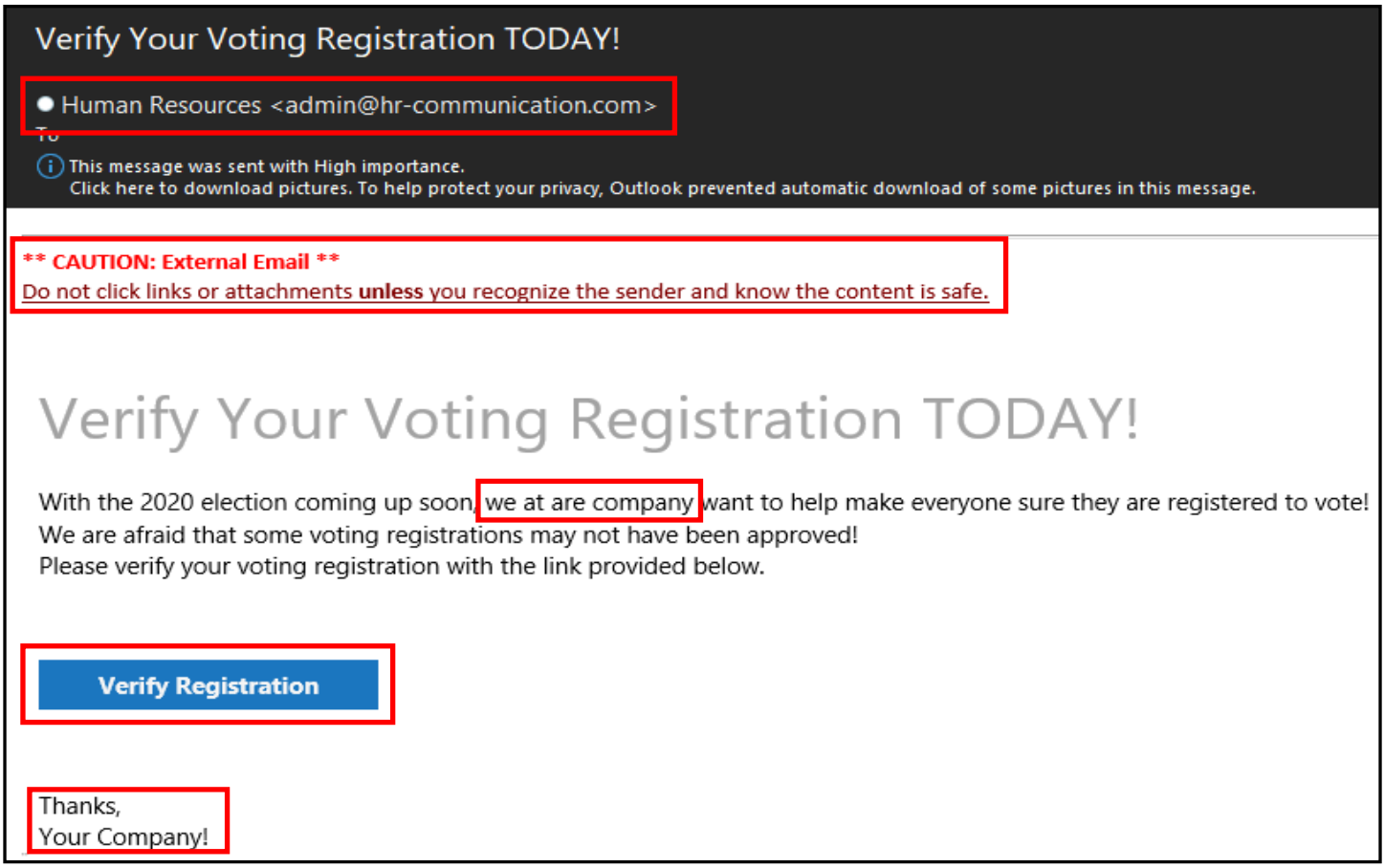
New Hanover Regional Medical Center

OUCH!

OCTOBER 2018

Don't Get Hooked

Recently a phishing simulation was sent out house wide. Were you able to spot the phishing email or did you get caught?



1. Notice the displayed name is "Human Resources" but the email address isn't nhrmc.org. If you hover over the name in Outlook you can see the actual email address.
2. Hover over links and be sure they are going somewhere you recognize. In the simulation the link was definitely not an NHRMC link. This link led to a fake website designed to look like a NHRMC login page. Had this been real and you logged into this page, it would steal your username and password giving the attackers access to our network.
3. Other things to pay attention for are misspelled or misused words. In this simulation email there are a couple of misused words and some bad grammar in general.

All employees are a critical link in identifying and reporting suspicious emails. It is important that if you see a suspicious email in your Inbox that you report it..

Please do not report spam emails that are sent from a mailing list you have subscribed to or emails that have been automatically placed in your Junk Email.

New Hanover Regional Medical Center

OCTOBER 2018

OUCH!

Analyze Your Email

1. QUESTION **Every email you receive.**

- Does the sender name match the email address?
- Is there a **"CAUTION: External Email header"** on the email but it says it's from your manager?
- Do you have your bank statements, Paypal or other accounts setup to use to this address?

2. CHECK **The Links before you click.**

- Inspect all links and addresses carefully to see if they match the real address
- Be wary of shortened URL's such at bit.ly since you can't see the real web address.
- **Hover to Discover** - To see the real address of a link hover your mouse over the link without clicking.

3. REFUSE **To provide usernames, passwords via**

- Legitimate banks and companies will never ask for credentials via email.
- Beware of subject lines that claim your **"account has been suspended"** or your account had an **"unauthorized login attempt."**
- Beware of Urgent or Threatening Language in the Subject Line or the body of the email invoking a sense of urgency or fear.

Refuse to click on a link to go to a website but instead go to the known website and login in

4. REPORT **Suspicious emails to IS Security.**

- If you are using Outlook, click the Report Phishing button to report an email. When you click the email will automatically be sent to IS Security.
- Additionally, you can forward the email as an attachment to phishing@nhrmc.org if you are unable to submit via the Report Phishing button.

New Hanover Regional Medical Center