Phishing 101

Phishing 101

Types of Phishing

- **Phishing is the act of casting a wide “net” to scam or infect as many users as possible. This type of phishing does not discriminate between users or organizations.**
- **Spear Phishing is targeting a specific user/group of users to get specific information. They will typically use familiar wording to get you to give up confidential information.**

Phishing 101

- The goal of any phishing email you receive is to get information from you!
- They will usually try to get you to click a link to a fraudulent website or download a malicious attachment!

Phishing 101

How effective is phishing training?

- 95% of all attacks on enterprise networks are the result of successful spear phishing. – SANS Institute
- Regular training helps reduce the risk of successful phishing attacks by 10-20%.

Phishing Pop Quiz

What type of email had the most phishing success?

- Fear-based emails (Complaint filed, Expense declined)
- Social-based emails (Holiday eCards, Funny pics)
- Reward-based emails (Employee raffle, free lunch)
- Job Function-based emails (New fax, Sign in online)

Phishing Pop Quiz

- Social-based emails – 16% success rate
- Reward-based emails – 13.8% success rate
- Job Function-based emails – 11.8% success rate
- Fear-based emails – 10.4% success rate

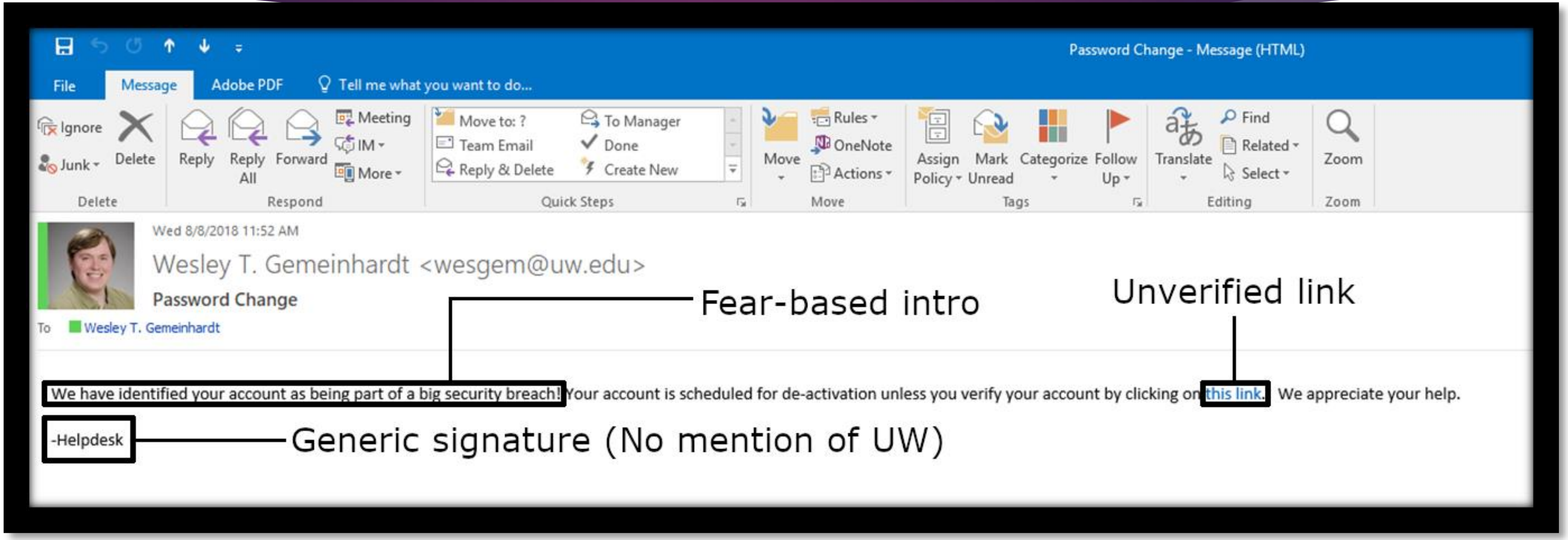
-Statistics from Enterprise Phishing Resiliency and Defense Report 2017

Identifying Phishing Emails At the UW

Identifying Phishing Emails At the UW

- Phishing emails to the UW are primarily Fear and Urgency based emails
- “Your password is about to expire!”
- “Your account is in violation and will be shut down!”
- “Click here to activate your membership!”

Identifying Phishing Emails at the UW



Wed 8/8/2018 11:52 AM

Wesley T. Gemeinhardt <wesgem@uw.edu>

Password Change

To Wesley T. Gemeinhardt

We have identified your account as being part of a big security breach! Your account is scheduled for de-activation unless you verify your account by clicking on this link. We appreciate your help.

-Helpdesk

Fear-based intro

Unverified link

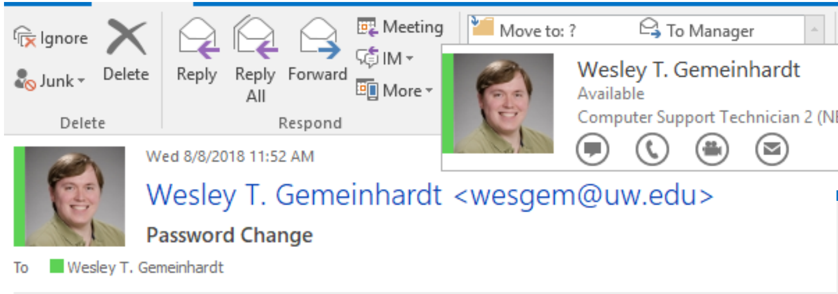
Generic signature (No mention of UW)

Identifying Phishing Emails at the UW

Hover and Verify

- **Hover over the Sender and link (DO NOT CLICK)**
- **Is the sender claiming to be from your organization, but is using a email address outside of the company?**
- **Does the link lead outside the company? Is it a bit.ly link?**

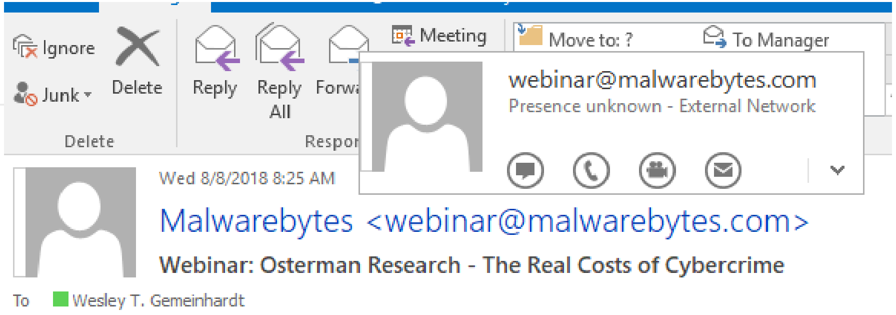
Identifying Phishing Emails at the UW



Wesley T. Gemeinhardt
Available
Computer Support Technician 2 (NE S S...

Wed 8/8/2018 11:52 AM
Wesley T. Gemeinhardt <wesgem@uw.edu>
Password Change
To 🟩 Wesley T. Gemeinhardt

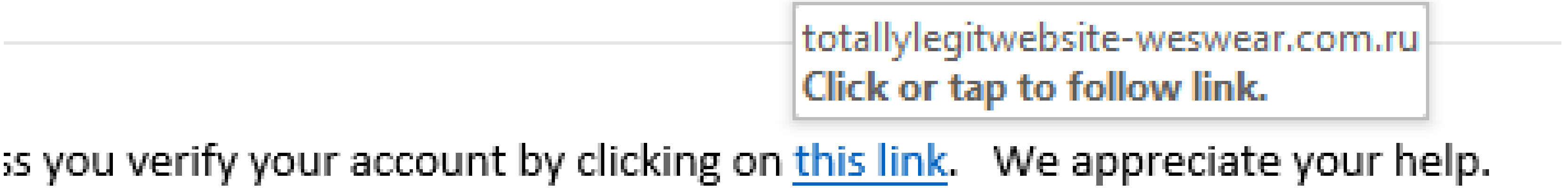
∨ External Email Address



webinar@malwarebytes.com
Presence unknown - External Network

Wed 8/8/2018 8:25 AM
Malwarebytes <webinar@malwarebytes.com>
Webinar: Osterman Research - The Real Costs of Cybercrime
To 🟩 Wesley T. Gemeinhardt

Identifying Phishing Emails at the UW



totallylegitwebsite-weswear.com.ru
Click or tap to follow link.

ss you verify your account by clicking on this link.   We appreciate your help.

Identifying Phishing Emails at the UW

Other Warning Signs of a Phishing Email

- **Are there spelling/grammatical errors?**
- **Is it CC’d to multiple people? Are the email addresses in alphabetical order?**
- **Were you expecting the email from the sender?**
- **Is the signature extremely generic?**

I’ve Identified the Phishing Email, Now What?

I’ve Identified the Phishing Email, Now What?

“If you receive an email you suspect is phishing, in which someone is trying to get you to download an attachment or enter your ID and password onto a fake web page, inform the department about it.”

I’ve Identified the Phishing Email, Now What?

Other Steps to Take

- **If the sender is another company's address, create a new message and notify them that you suspect their account is sending phishing emails**