An Information Security publication for the WPI community

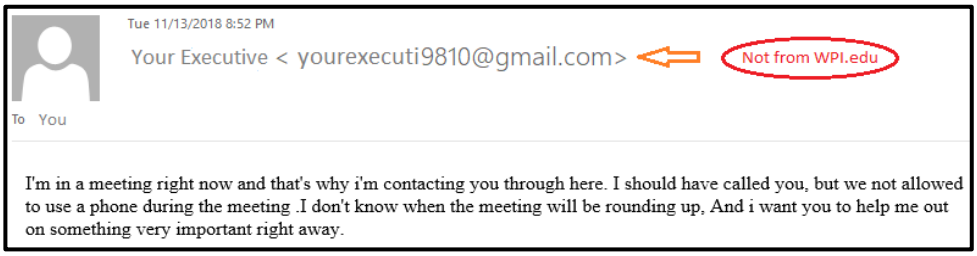
# SECURE IT

2019 November

## Holiday Phishing Expedition

Please be extra vigilant of phishing attacks during the upcoming holidays. Scammers try to take advantage of your holiday spirit, and the hustle and bustle of increased online activity. We have seen an uptick of Business Email Compromise (also known as CEO Fraud), where cybercriminals try to impersonate a colleague. They attempt to get you to execute an unauthorized wire transfer, send out confidential information, or purchase gift cards.

These phishing attacks use social engineering to prey on your good nature. Because they are targeted individual attacks rather than mass-email to the WPI community, they are not stopped by spam filters. They require recipients to be actively aware. This example shows the first stage of the attack where the attacker attempts to begin a conversation:




*CEO Fraud Example 1*

You can protect against CEO Fraud that appears in your inbox by:

1. Checking the **From:** address of the email. If it is not @wpi.edu then it is spoofed.
2. Investigating unusual email requests. If the email seems out of character for your executive or colleague, then contact them by another means using the contact information in your official department directory. If you don't know their contact information, reach out to someone who does.
3. Reporting CEO Fraud emails to IT and discuss with your colleagues. CEO Fraud targets specific groups of people, so discussing raises awareness for everyone.

Report CEO Fraud

## Multi-Factor Authentication

Currently, Multi-Factor Authentication (MFA) is required for login to Workday and Salesforce, whether connecting from the WPI network or remotely. A pilot is underway to enable MFA for all applications that use Single Sign-On functionality when accessed remotely for select staff members that have access to sensitive data. This will better safeguard WPI data by facilitating an additional layer of security when off-campus. Information Technology (IT) and select Student Affairs staff began the expanded usage on November 14.

### Cybersecurity Feedback

IT recognized National Cyber Security Awareness Month during October by offering tips to protect yourself and bolster #herdimmunity for WPI. Let us know what cybersecurity means to you, what you learned, or what you would like to know more about using our feedback form.

Cybersecurity Feedback Form

### Tip: Online Shopping

'Tis the season for e-commerce! Protect your identity, accounts, and important data with these tips:

- Do not use your WPI account or email for online shopping.
- Create different passwords for personal accounts; do not use the same password used for WPI.
- Beware of e-skimming where cyber criminals capture credit card and identity data from payment processing web sites. The National Initiative for Cybersecurity Careers and Studies (NICCS) details the scheme.

E-Skimming Article (PDF)