Deep Dive into Email Security

Michael Platt
Systems Security Analyst

CompTIA Security+
Microsoft Security Operations Analyst

Harrisburg University Graduate, 2010

- BS, Computer and Information Sciences
- Certificates: CompTIA Security+, Microsoft Security Operations Analyst

13 years of IT experience

- Capital Blue Cross (Intern with Help Desk) – Healthcare
- Susquehanna River Basin Commission (Desktop Support) - Environmental
- Quandel Enterprises (Network Administrator) - Construction
- Harrisburg University (Security Analyst) – Education

Current Role: Proactively enforce data integrity, security policies and remediate threats. Provide network and software support via the IT Helpdesk.

CYBER GUARD DUTY: "DON'T CLICK THAT EMAIL KAREN!"

When I was a kid, I thought "hacking" was all about writing Matrix-like code, when in reality it's just sending emails that say, "give me your passwords" and they do.

Source: Someone on Twitter

What is email security?

- The practice of protecting email accounts and communications from unauthorized access, loss, or compromise.

Why is email security important?

- More than 333 billion emails are sent and received daily worldwide.
- Most cyberattacks—**94 percent**—begin with a malicious email.
- Cybercrime cost more than $4.1 billion in 2020 according to the FBI's Internet Crime Complaint Center (IC3).

Two important types of email threats

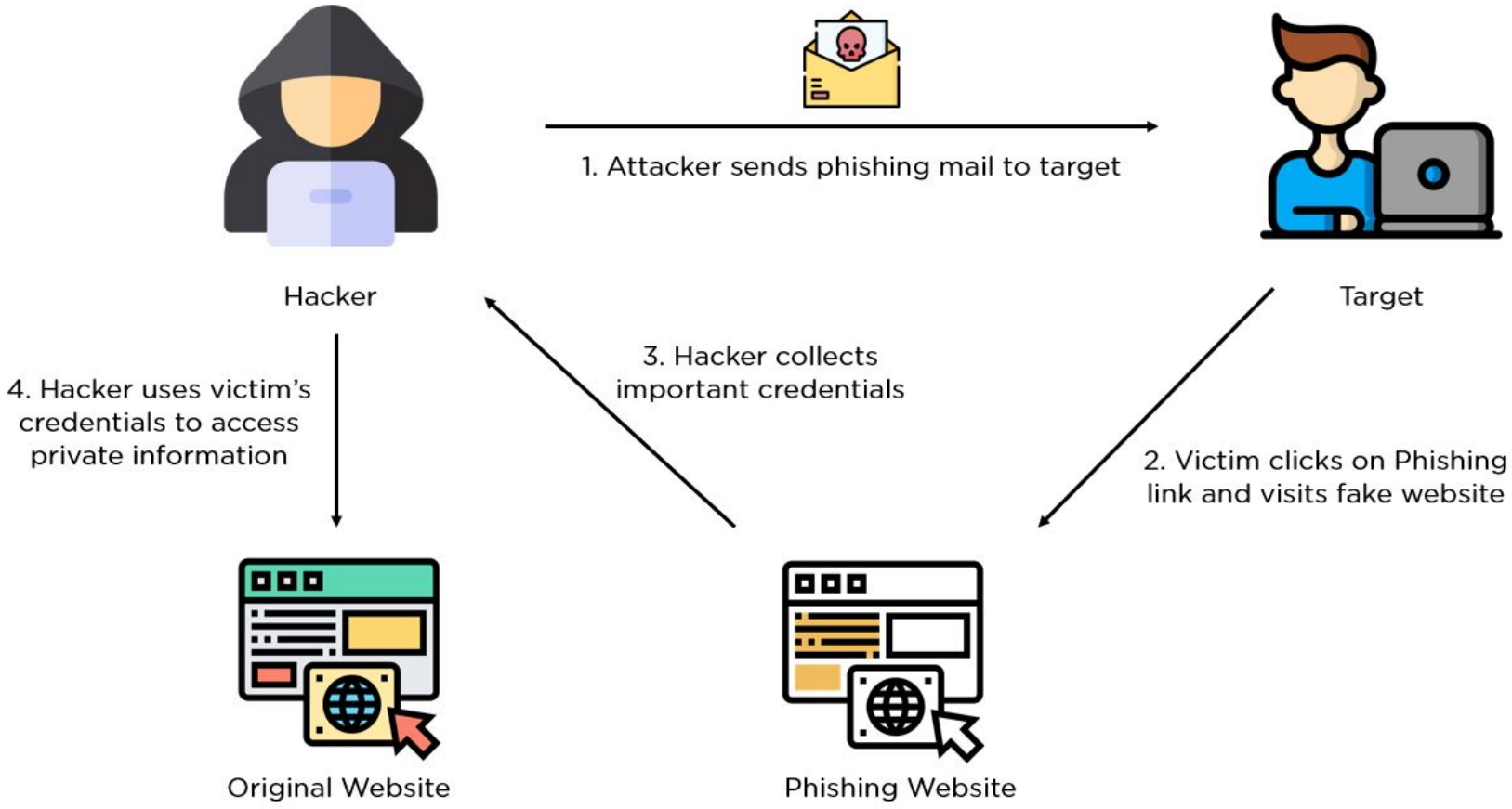
Phishing - Pretending to be a trusted person or organization to trick victims into disclosing valuable information such login credentials and other types of sensitive data.

Impersonation - Pretending to be a trusted person or organization to secure money or data via email. Business email compromise is one example in which a scammer impersonates an employee to steal from the company or its customers and partners. 1.8 billion in lost revenue according to FBI (IC3).

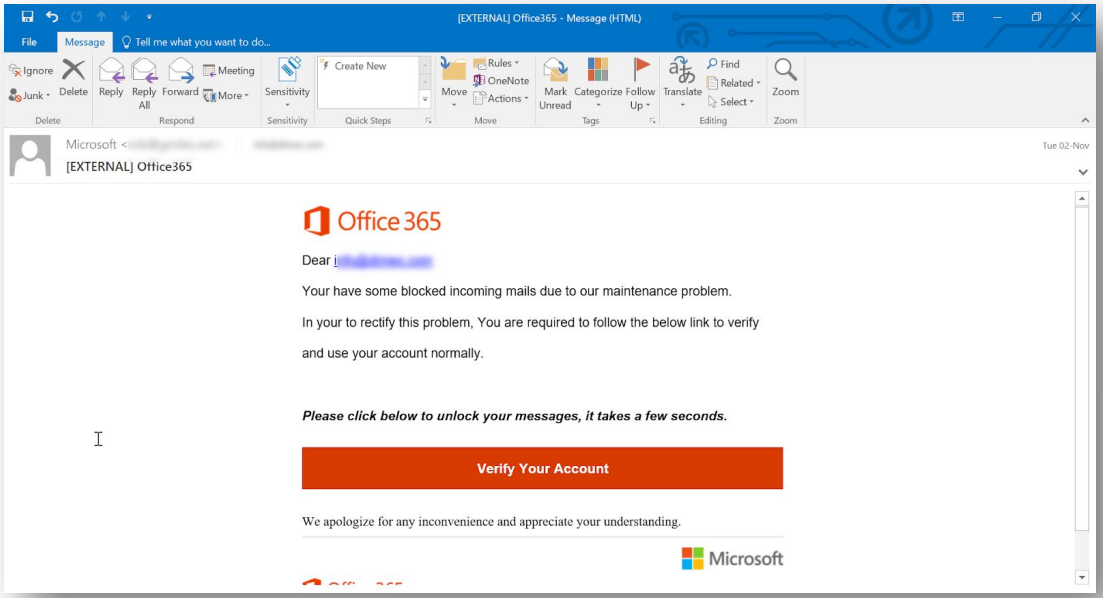
Credential Harvest

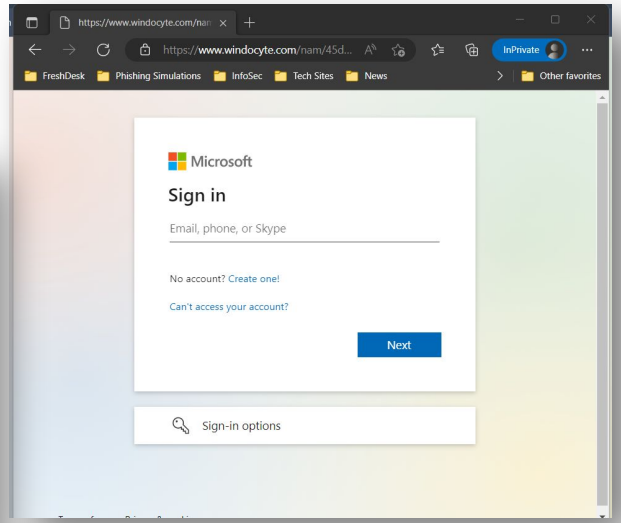
In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a website luring the target to submit their username and password. Typically, the page attempting to lure the target will be themed to represent a well-known website to build trust in the target.

Credential Harvest



Credential Harvest





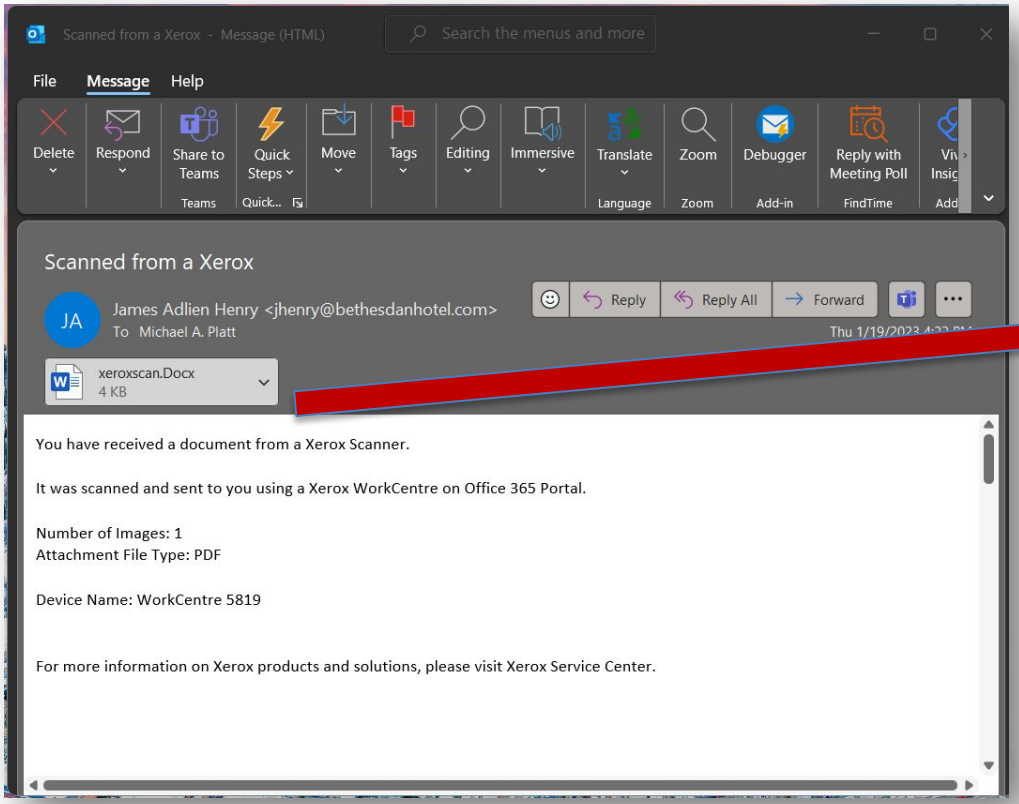
Hacker

HARRISBURG UNIVERSITY OF SCIENCE AND TECHNOLOGY

Malware Attachment

In this type of technique, a malicious actor creates a message, with an attachment added to the message. When the target opens the attachment, typically some arbitrary code such as a macro will execute in order to help the attacker install additional code on a target's device, or further entrench themselves.

Malware Attachment

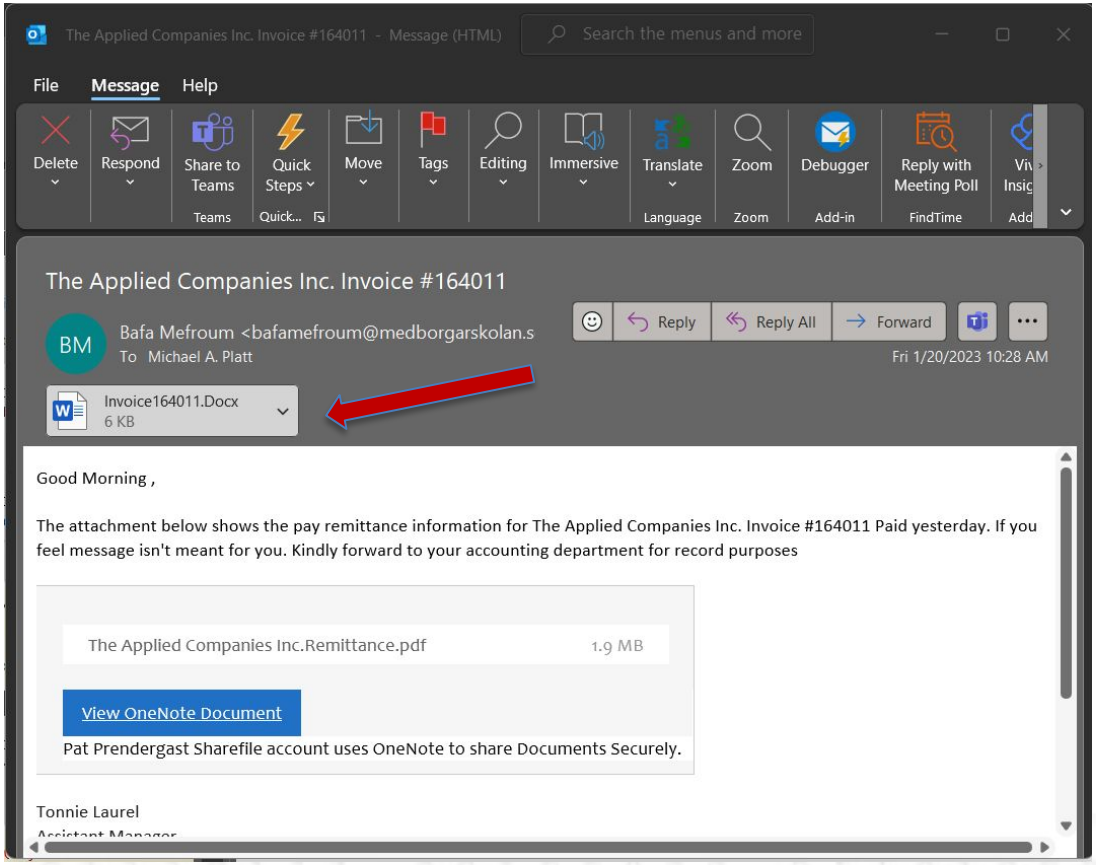


HARRISBURG UNIVERSITY OF SCIENCE AND TECHNOLOGY

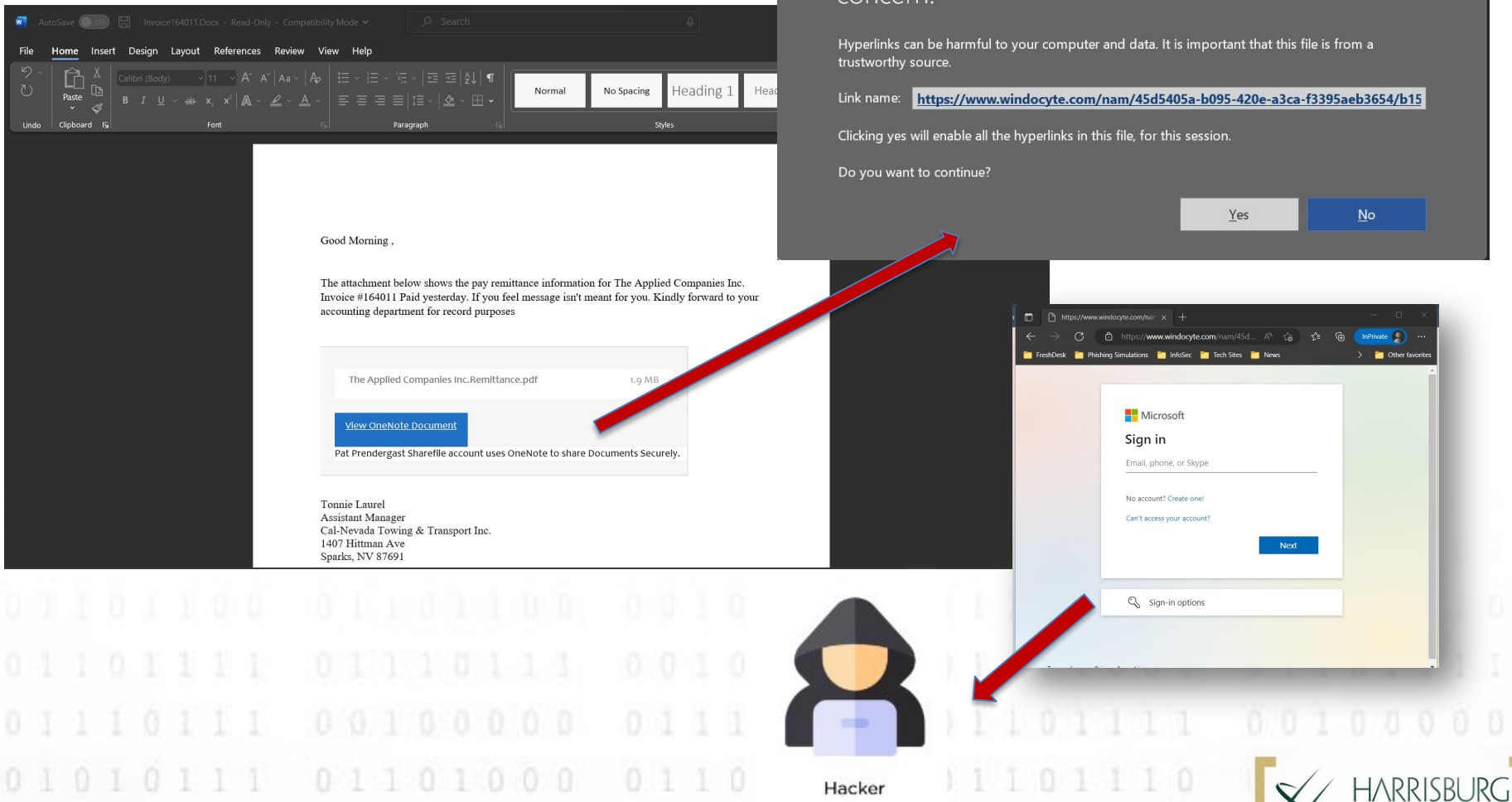
Link in Attachment

When the target opens the attachment, they are represented with a URL in the actual attachment, if the target then clicks on that URL they are taken to a web site, luring the target to submit their username and password. Typically, the page attempting to lure the target will be themed to represent a well-known web page to build trust in the target.

Link in Attachment



Link in Attachment

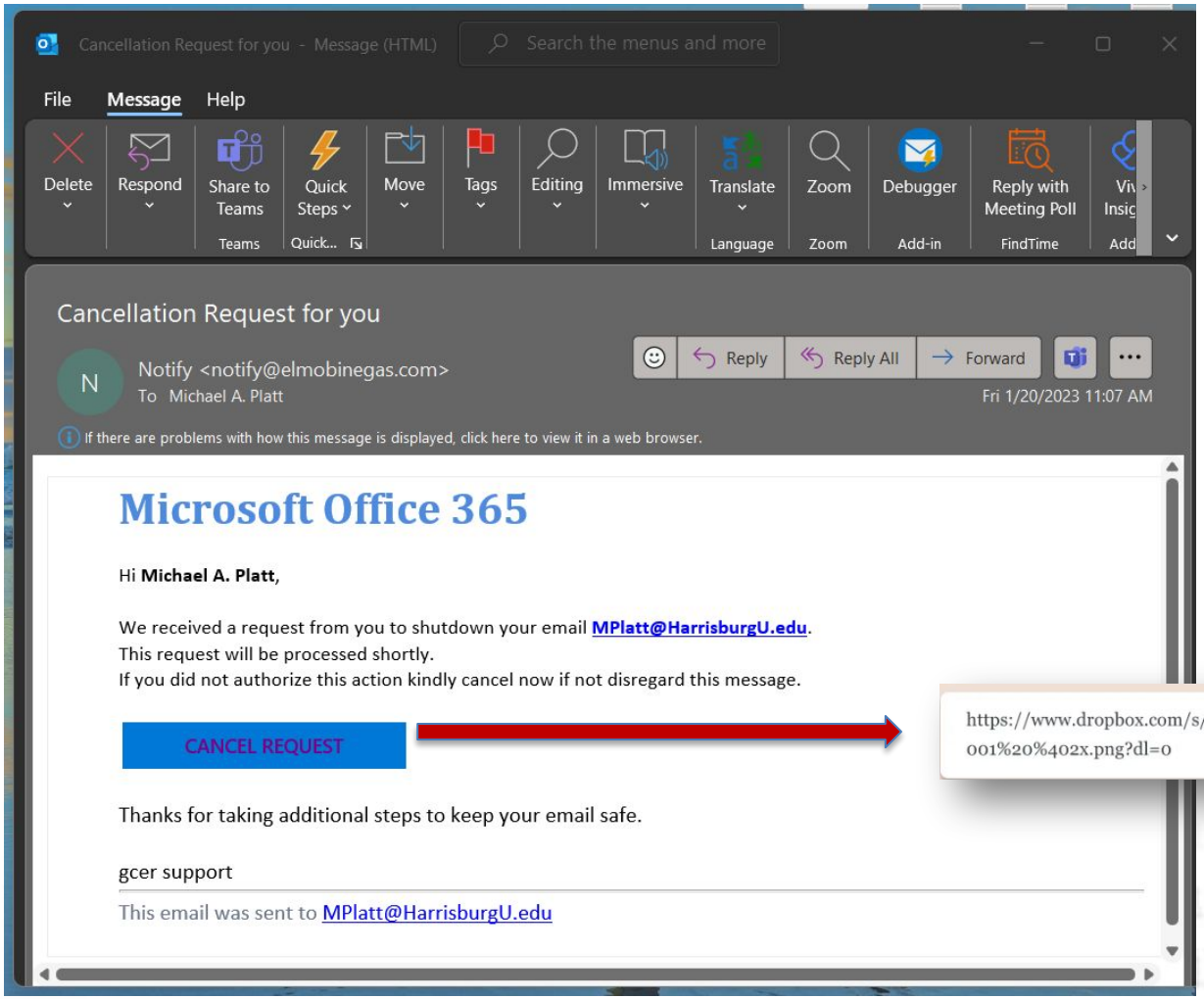


Link to Malware

In this type of technique, a malicious actor creates a message, with an attachment added to the message. However instead of directly inserting the attachment into the message, the malicious actor will host the attachment on a well-known file sharing site, (such as SharePoint, or Dropbox).

When the target clicks on the URL it will open the attachment, typically some arbitrary code such as a macro will execute in order to help the attacker install additional code on a target's device, or further entrench themselves.

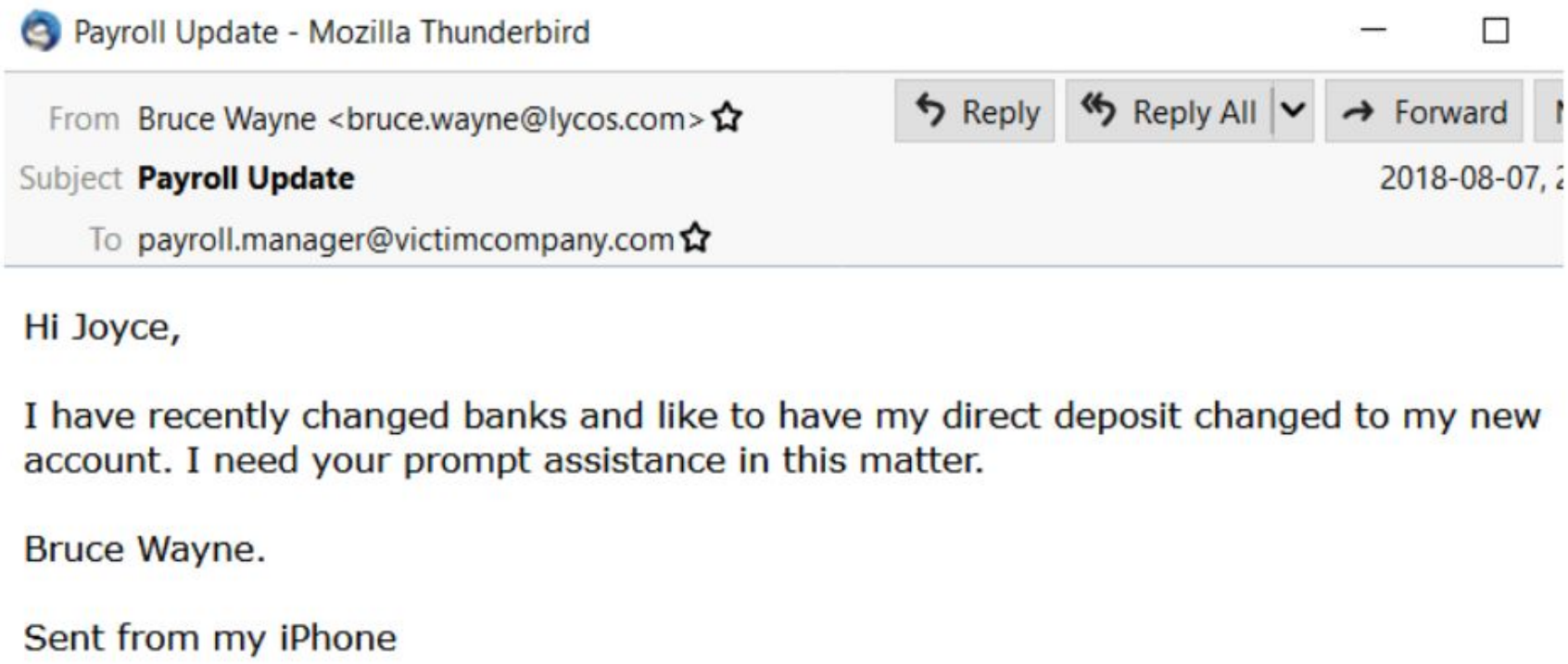
Link to Malware



https://www.dropbox.com/s/f9n3pyncyzaunby/Direct%20Download%20Link%2001%20%402x.png?dl=0

HARRISBURG UNIVERSITY OF SCIENCE AND TECHNOLOGY

Business Email Compromise (BEC)



Tips to Help You Defend

Urgent call to action or threats - Be suspicious of emails that claim you must click, call, or open an attachment immediately.

Spelling and bad grammar – Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have an editorial staff to ensure customers get high-quality, professional content. If an email message has obvious spelling or grammatical errors, it might be a scam.

From: *(A familiar name, often a supervisor)*@gmail.com>
Sent: Wednesday, February 27, 2019 12:36 PM
To: *(Email may be sent to a list of people, including people you know)*

Subject: URGENT REQUEST

Hi,Got a moment?Give me your personal cell number.I need you to complete a task for me

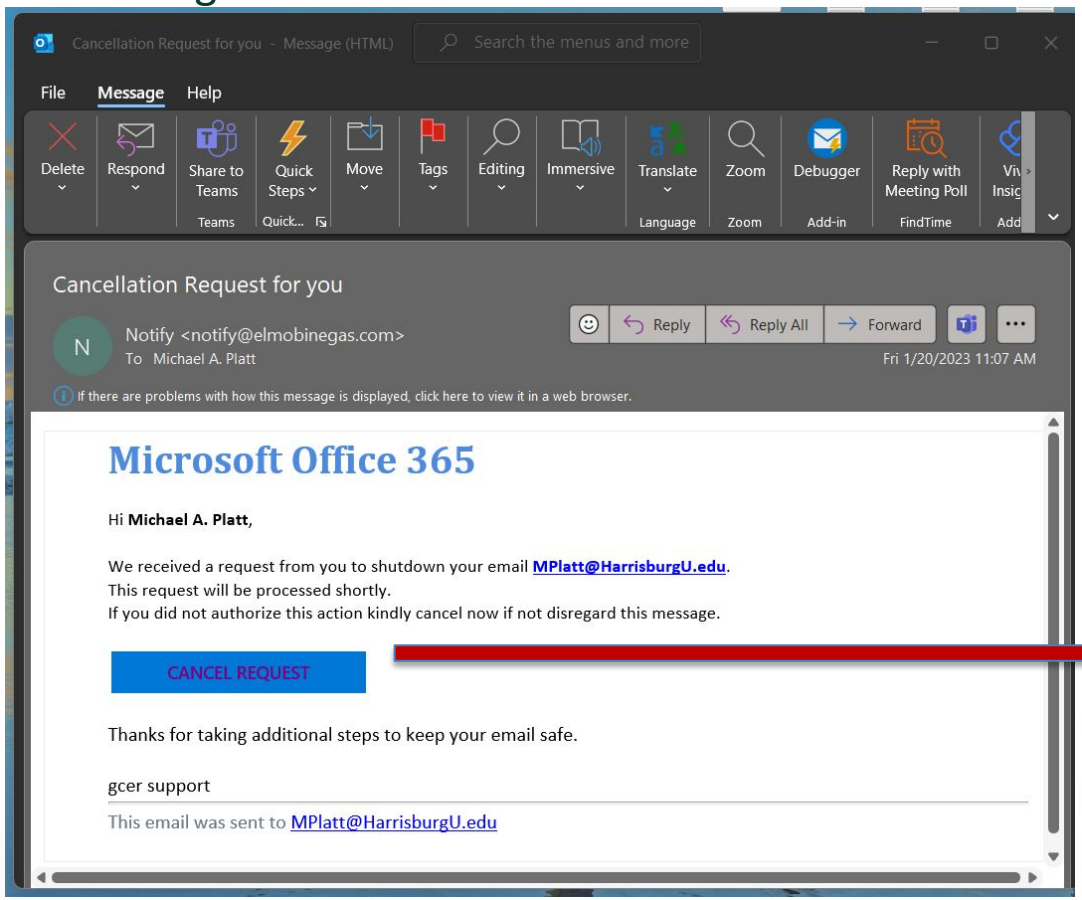
Thanks

(A familiar name, often a supervisor often a person in a leadership position)
Professor of Accounting

Sent from my iPhone

Tips to Help You Defend

Suspicious links - If you suspect that an email message is a scam, do not open any links that you see. Instead, hover your mouse over, but don't click. Does the link look legit?

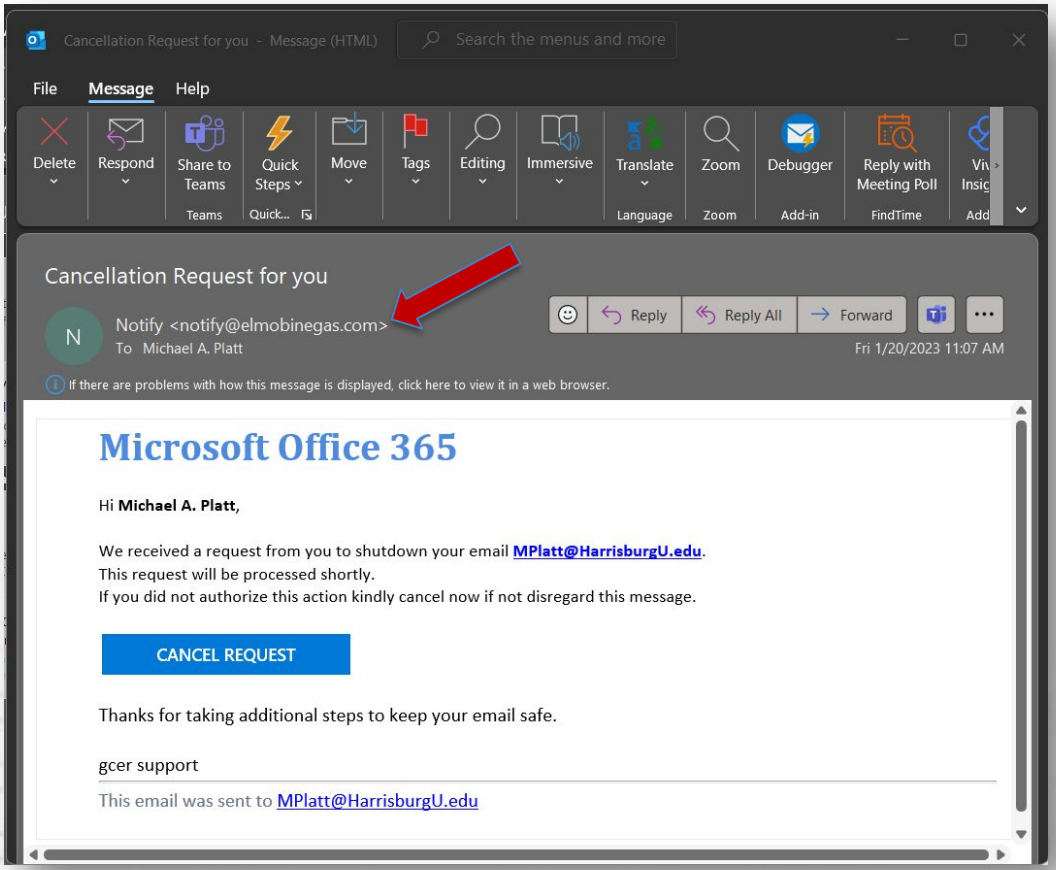


https://www.dropbox.com/s/f9n3pyncyzaunby/Direct%20Download%20Link%2001%20%402x.png?dl=0

HARRISBURG UNIVERSITY OF SCIENCE AND TECHNOLOGY

Tips to Help You Defend

Mismatched or spoofed email domains - If the email claims to be from a reputable company, like Microsoft, but the email is being sent from another email domain like Yahoo.com, Gmail.com it's probably a scam.



HARRISBURG UNIVERSITY OF SCIENCE AND TECHNOLOGY

What is one simple action you can take to prevent 99.9 percent of attacks on your accounts?


99.9%
of attacks can be blocked with multi-factor authentication[7]
[7] 2018 Microsoft annoucing MFA, aka.ms/MFA99
Read more at
aka.ms/gopasswordless

Questions?

https://www.linkedin.com/in/michaelaplatt/