Deep Dive into Email Security

Michael Platt 0 1 Systems Security Analyst 0 CompTIA Security+ Microsoft Security Operations Analyst 0 0



Harrisburg University Graduate, 2010

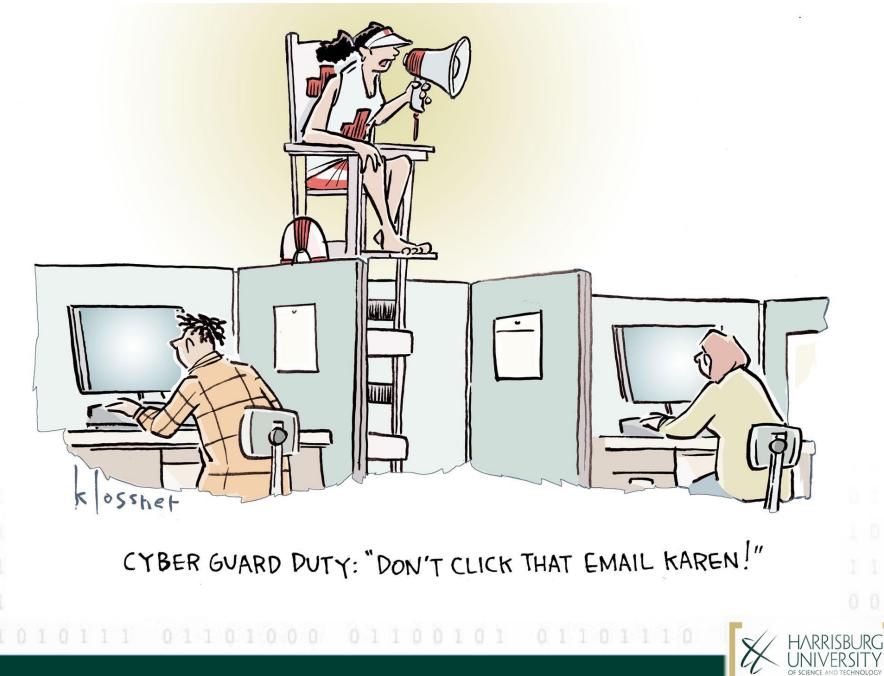
- BS, Computer and Information Sciences
- Certificates: CompTIA Security+, Microsoft Security Operations Analyst

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

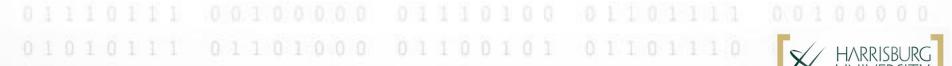
Current Role: Proactively enforce data integrity, security policies and remediate threats. Provide network and software support via the IT Helpdesk.

HARRISBURG UNIVERSITY OF SCIENCE AND TECHNOLOGY





"WELL, THEY BANNED PASSWORD RE-USE. WHAT DO YOU EXPECT ME TO DO?"



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—<u>94 percent</u>—begin with a malicious email.
- Cybercrime cost more than \$4.1 billion in 2020 according to the FBI's Internet Crime Complaint Center (IC3).

01110111 0010000 01110100 011011



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).

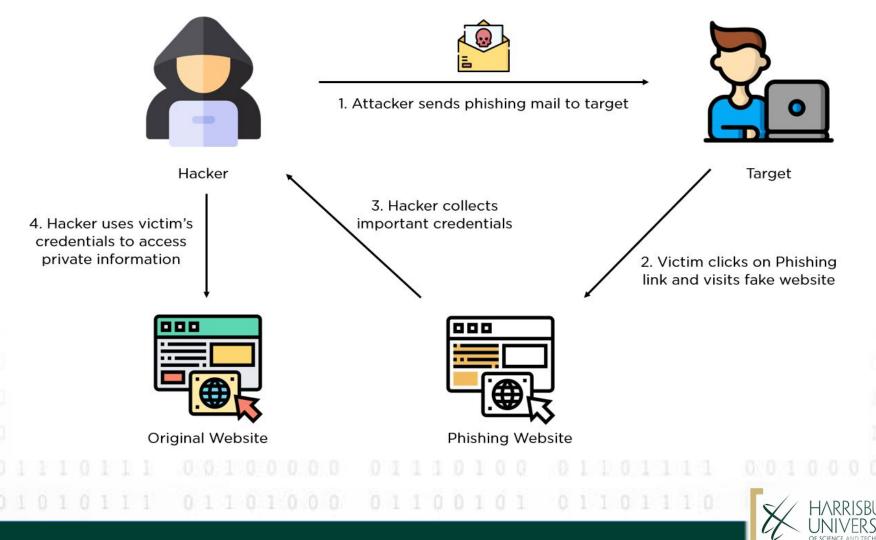


Credential Harvest

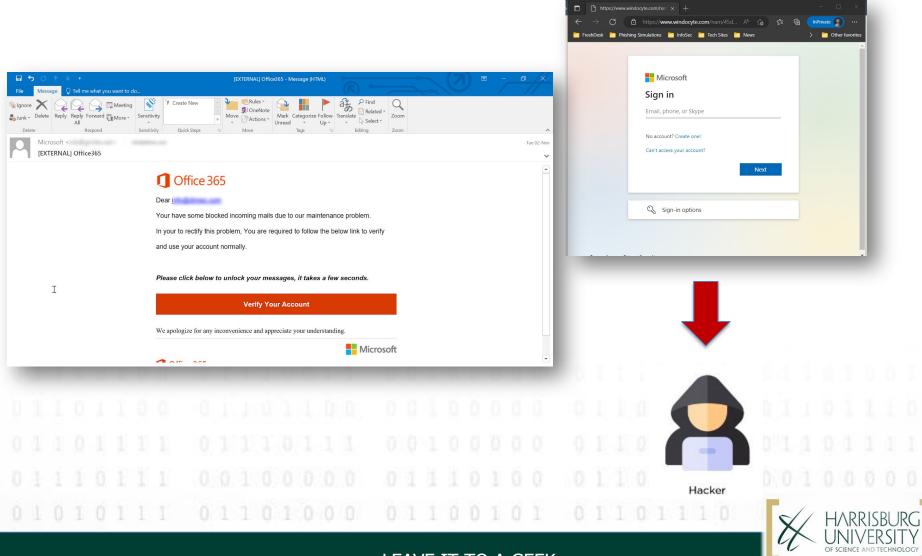
In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a website luring the target to submit their username and password. Typically, the page attempting to lure the target will be themed to represent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



Credential Harvest



Credential Harvest

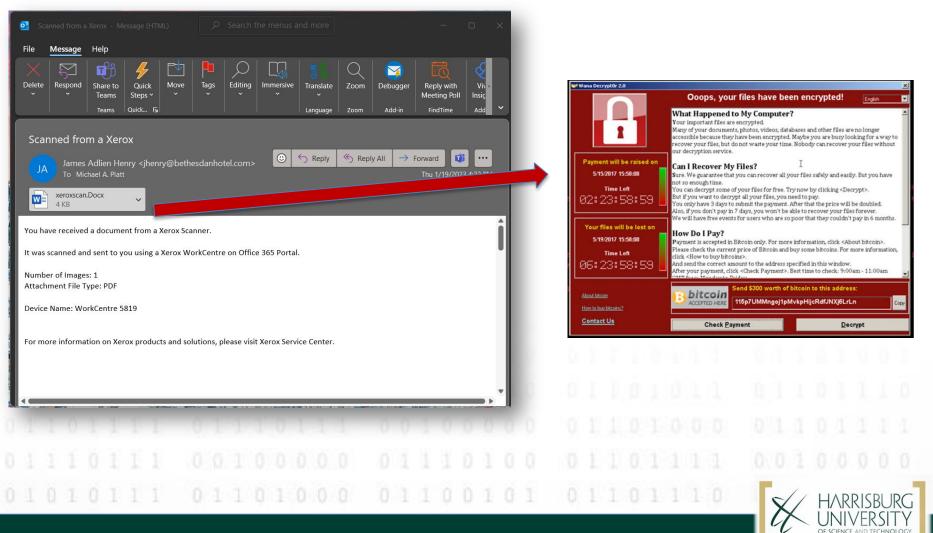


Malware Attachment

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



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

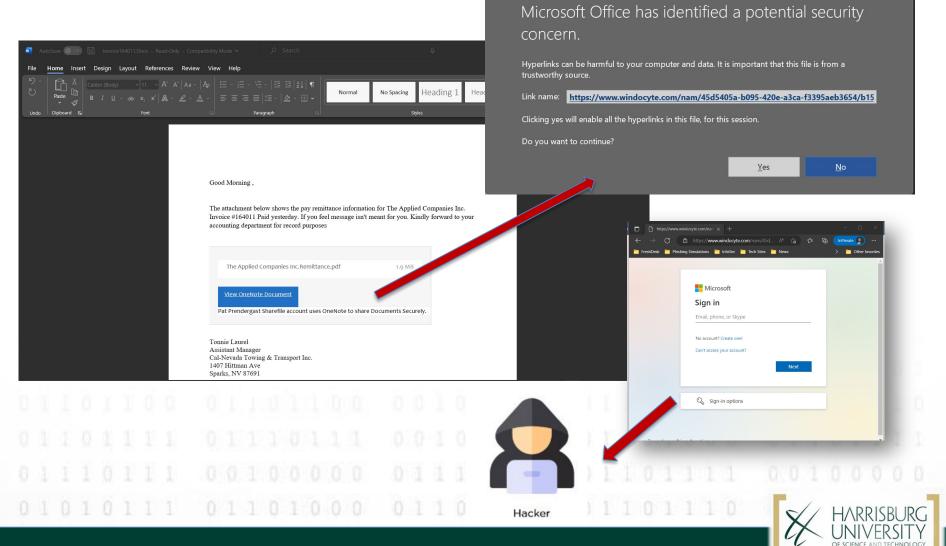
File	Message	Help	o															
Delete	Respond	Į	e to ims S	Quick Guick Steps ~	Move	Tags	Editi) ng Im	mersive	e Transla Langua			bugge Add-in		Reply w Reeting FindTin	vith Poll	Vi Insig	⊆
Tho	Applie	d Cor	nnani	oc Inc		co #16	1011											
The						nedborg		n c	:	← Rep	у (5	Reply All		Forv	vard	0] .]
BN		lichael A		lament	oumen	neuborg	arskola	1.5						Fr	i 1/20/.	2023	10:28 /	AM
	Invoice' 6 KB	164011.C	юсх	~	4													
Good	Morning .																	
	Morning ,		shows t	he nav i	remittan	ice inform	nation f	or The	Annlie	d Compai	ies Inc. I	nvoice #	6401	1 Paic	l veste	erdav	lf vo	
The at	Morning , tachment essage isr	below											16401	1 Paic	l yeste	erday	r. If yo	u
The at	tachment	below											16401	1 Paic	l yeste	erday	r. If yo	u
The at feel m	tachment	below 't mear	nt for yo	u. Kind	ly forwa	rd to you			epartm				16401	1 Paic	l yeste	erday	r. If yo	u
The at feel m	tachment essage isr	below I't mear	nt for yo	u. Kind	ly forwa	rd to you			epartm	nent for r			16401	1 Paic	l yeste	erday	r. If yo	u
The at feel m	tachment essage isr The Appl	below n't mean lied Cor <u>Note D</u>	nt for yo npanies ocumer	u. Kind Inc.Rei	ly forwar	rd to you e.pdf	r accou	nting de	1.9	MB			16401	1 Paic	l yeste	erday	r. If yo	u
The at feel m Pa Tonnie	tachment essage isr The Appl View One t Prender e Laurel	below n't mean lied Cor <u>Note D</u> gast Sh	nt for yo npanies ocumer	u. Kind Inc.Rei	ly forwar	rd to you e.pdf	r accou	nting de	1.9	MB			16401	1 Paic	l yeste	erday	r. If yo	u
The at feel m Pa Tonnie	tachment essage isr The Appl <u>View One</u> t Prender	below n't mean lied Cor <u>Note D</u> gast Sh	nt for yo npanies ocumer	u. Kind Inc.Rei	ly forwar	rd to you e.pdf	r accou	nting de	1.9	MB			16401	1 Paic	l yeste	erday	r. If yo	u
The at feel m Pa Tonnie	tachment essage isr The Appl View One t Prender e Laurel	below n't mean lied Cor <u>Note D</u> gast Sh	nt for yo npanies ocumer	u. Kind Inc.Rei	ly forwar	rd to you e.pdf	r accou	nting de	1.9	MB				1 Paic	l yeste	erday	r. If yo	u
The at feel m Pa Tonnie	tachment essage isr The Appl View One t Prender e Laurel	below n't mean lied Cor <u>Note D</u> gast Sh	nt for yo npanies ocumer	u. Kind Inc.Rei	ly forwar	rd to you e.pdf	r accou	nting de	1.9	MB			16401	1 Paic	l yeste	erday	r. If yo	u

LEAVE IT TO A GEEK

HARRISBURG

ND TECHNOLOGY

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.



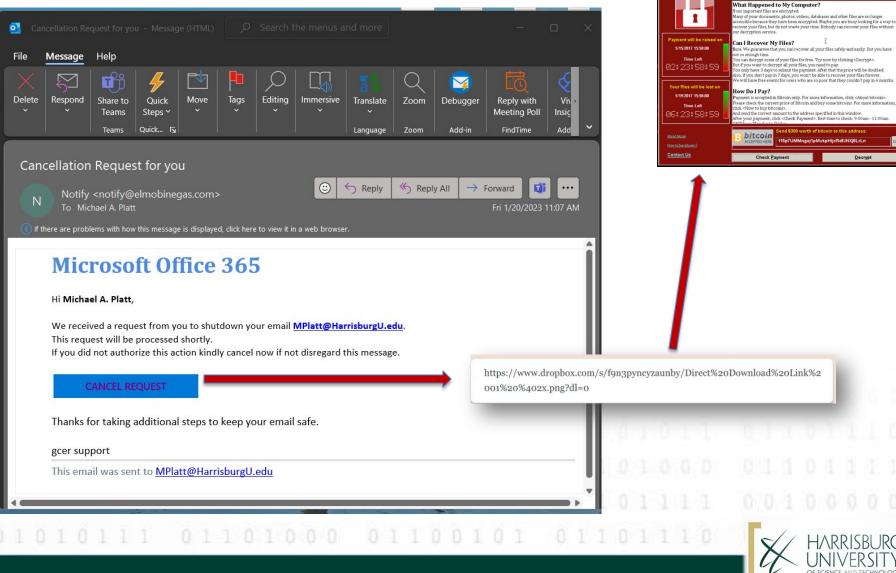
Link to Malware

Ooops, your files have been encrypted!

Check Payment

vkpHiicRdfJNXi6LrL

Decryp



Business Email Compromise (BEC)



Hi Joyce,

I have recently changed banks and like to have my direct deposit changed to my new account. I need your prompt assistance in this matter.

Bruce Wayne.

Sent from my iPhone



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

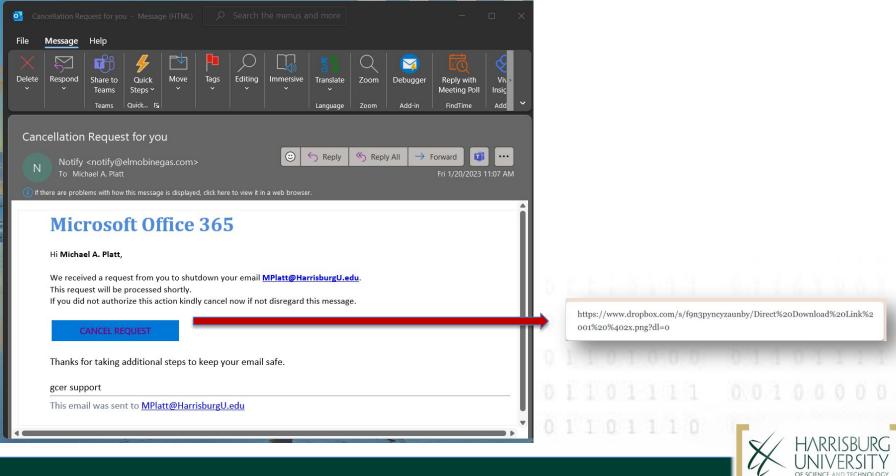
(A familiar name, often a supervisor often a person in a leadership position) Professor of Accounting

Sent from my iPhone



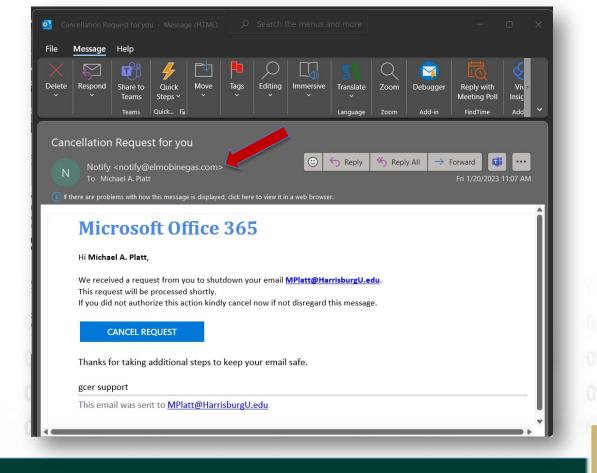
Tips to Help You Defend

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?



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.



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

 01110100
 011001100
 00100000
 0110101
 01

 01101111
 01110111
 00100000
 01101000
 01

 01101111
 01100000
 01110100
 01101111
 00

 010101111
 01100000
 01100101
 01101111
 00



99.9%

of attacks can be blocked with multi-factor authentication⁷

7 2018 Microsoft annoucing MFA, aka.ms/MFA99

Read more at aka.ms/gopasswordless

 01101111
 01110111
 00100000
 01101000
 011010101

 011010111
 00100000
 01110100
 01101111

 01010111
 01101000
 01100101
 01101110



		ł																																						
		1		1		1	1	1		1	1		1			Qı			>t	ic	r		5	1		1	ĩ		1	1	1				1					
		1	1	1	0	1	0	0	0	1	1		1		0			70		0	0	13	0	1	0	0	1	0			0		0	1	1	1	0	1	0	1
()	1	1	0	1	1	1	0	0	1	1	1	0	0	0	0	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	0	1	0	0
- 0)	1	1	0	h	t	tp	S:	/仏	N	W	Ń	Ø	ir	h	e	ji	n	.0	C	n	n/	ñ	n/I	mi	С	h	a	e	B	ap	bla	tt/	1	1	0	0	Ö	1	0
()	1	1	0	1	1	0	0	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	1	1	0	0	0	1	1	0	1	1	0	1	1	1	1
()	1	1	0	1	1	0	1	0	1	1	0	0	1	0	1	0	1	1	1	0	0	1	1	0	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0
()	1	1	0	1	1	1	1	0	1	1	1	0	1	0	1	0	1	1	1	0	0	1	0	0	0	1	0	0	0	0	0	0	1	1	1	0	0	1	1
()	1	1	1	0	1	0	0	0	1	1	1	0	1	0	1	0	1	1	0	0	1	0	0	0	1	1	0	0	1	0	1	0	1	1	0	1	1	1	0
()	1	1	1	0	1	0	0	0	1	1	1	0	0	1	1	0	0	1	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	0	1	0	0	1
()	1	1	0	1	1	0	0	0	1	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	1	1	0	1	1	0	1	1	1	0
()	1	1	0	1	1	1	1	0	1	1	1	0	1	1	1	0	0	1	0	0	0	0	0	0	1	1	0	1	0	0	0	0	1	1	0	1	1	1	1

