COMMON EMAIL SECURITY THREATS

End to End™ NETWORKS

THREAT	WHAT IT IS	WHAT IT CAN DO
MALWARE One of the more common ways to infiltrate or damage computers 	Software that infects computers with viruses, worms, Trojan horses, spyware and adware	• *Watch a user through their webcam without their knowledge* • Intimidate a user with scareware, usually a pop-up message that indicates the computer has a security problem or other false information • Reformat the hard drive causing loss of all information • Alter or delete files • *Steal sensitive information/log a user's keystrokes* • Send emails on the user's behalf • *Take control of a computer and all software running on it*
PHARMING Common type of online fraud 	A way to point users to a malicious and illegitimate website by redirecting the legitimate URL. Even if the URL is entered correctly, it can still be redirected to a fake website	• *Convince a user the site is real and legitimate by spoofing or looking almost identical to the actual site.* Personal information may be given unknowingly to someone with malicious intent.
PHISHING *Used most often by Cyber criminals, easy to execute and produces results with little effort* 	Fake emails, text messages and websites created to look like they are from authentic companies. Sent by criminals to steal personal and financial information, also known as 'spoofing'	• *Trick a user into giving information by asking them to update, validate or confirm their account.* Often presented in a manner that seems official and intimidating. • *Provide cyber criminals with usernames and passwords so they can access accounts (online banking, shopping etc.) and steal credit card information*
RANSOMWARE Latest in cyber scams on the Web 	*Type of malware that restricts access to a user's computer or files and displays a message that demands payment in order for the restriction to be removed.* Two most common means of infection appear to be phishing emails that contain malicious attachments and website pop-up advertisements.	• Lockscreen: display an image that prevents a user from accessing the computer • Encryption: encrypt files on the system's hard drive and sometimes on shared network, USB, external and cloud storage drives preventing a user from opening them Will display a notification stating the computer or data has been locked and demanding a payment for the user to regain access. Sometimes the notification states that authorities have detected illegal activity and the payment is a fine to avoid prosecution.

EMAIL SECURITY GUIDE
- WHAT TO LOOK FOR -

From:

Is the sender unfamiliar to you?

When you hover over the email address, is it different than what appears in the header?

Is the email out of character?

Is the email from someone outside of you organization and asking you to something outside of your typical role?

Is the sender a stranger?

Does the email include a link or attachment?

To:

- ✓ Is the email being sent to multiple people that you don't know?
- ✓ Was the email sent to multiple people within your organization who typically would not be cc'd on the same messages?
- ✓ Is your name spelled wrong?

Subject:

- ✓ Does the subject line differ from the contents of the email?
- ✓ Does the email subject line have language quirks that seem out of place?
- ✓ Does the subject line say something that makes you panic or feel like something has gone wrong?
- ✓ Does it imply you must take action immediately?

***From:** CEO*
***Sent:** 4:07 PM*
***Subject:** Fw: Attached Wiring Instruction*
***To:** CFO*
***CC:** Admin, Customer Service*

Paul,

Process the wiring instruction attached. Code this to Professional Services as a Prepaid expense, and email me the confirmation when completed. I'll forward support later on. I am currently busy and I'll appreciate swift email correspondence.

clickthisandbebreached.com

Date:

- ✓ Was the email sent at an odd hour compared to when you received it?

End to End™ NETWORKS

www.endtoend.com

1-877-363-2363

Hyperlinks:

- ✓ Is there a hyperlink in the email?
- ✓ When you hover over (but don't click) on the link, does it go to a different website?
- ✓ Does the hyperlink look similar to a legitimate website but differ slightly?

Attachments:

- ✓ Is there an attachment?
- ✓ Does the attachment end in anything other than .txt?
- ✓ Was the attachment unexpected?

IF YOU ARE ABLE TO ANSWER YES TO ANY OF THE QUESTIONS ABOVE…..PROCEED WITH CAUTION!