INFILTRATED

The Threat You Never Saw Coming

Sponsored by:

Westchester Community College
Cyberseccurity Club

WiCyS
Women in Cybersecurity

SGA

Our Mission: Make students understand that cybersecurity awareness IS a career skill — no matter their major, industry, or job path.

Cybersecurity isn't just an IT skill — it's a professional skill.
Every employer expects employees to recognize suspicious emails, protect company data, and avoid falling for employment scams. Phishing awareness is part of being career-ready.

Learning Objectives

Understand what phishing is and recognize its common forms (email, SMS, social & voice phishing).

Learn how social engineering exploits human trust to breach even the most secure systems.

Explore real-world case studies.

Develop practical skills to analyze and identify phishing attempts through interactive simulations.

Learn how to report phishing attempts and implement preventive measures like MFA and secure password practices.

Increase overall awareness.

Terminology – Lets Discuss

- Social Engineering
- Phishing
- Malware
- Anti-virus
- Multi-Factory Authorization (MFA)


POV: I get a phishing email saying the CEO wants to give me $100k
189K
IT department
Me
326

Why Social Engineering Works

- Social engineering and phishing work effectively because they exploit fundamental aspects of human psychology and behavior. Attackers use psychological manipulation to take advantage of people's natural tendencies like trust, helpfulness, curiosity, and fear. For example, phishing attacks often create a sense of urgency or fear—like a fake security alert—to prompt individuals to act quickly without thinking critically. They may also impersonate trusted authorities or contacts, leveraging people's inclination to help others or comply with authority figures.
- This manipulation taps into kindness and social norms, where most people want to be cooperative and avoid conflict, which makes them vulnerable to deception. Unlike traditional hacking that exploits software flaws, social engineering exploits human vulnerabilities, which are often easier to manipulate. Because attackers craft believable scenarios tailored to the victim's context or emotions, people often let their guard down, enabling attackers to gain access to sensitive information or systems.

Most Common Types of Phishing

Email Phishing: The most common type, where attackers send mass emails pretending to be real organizations to trick people into clicking bad links or downloading malware.

Spear Phishing: A targeted attack using personalized info about the victim to increase trust and success, often aimed at specific employees.

Whaling: Spear phishing aimed at high-value targets like executives or senior management, leveraging their authority to manipulate others.

Smishing: Phishing via SMS/text messages with malicious links or prompts.

Vishing:

Common Indicators of Phishing Emails

Red Flags: Phishing emails often have telltale signs, including:

- **Suspicious Sender Addresses:** Email addresses that are similar to, but not exactly the same as, a legitimate one.
- **Unexpected Attachments:** Attachments that you weren't expecting, especially if they're in executable formats.
- **Grammatical Errors:** Poor grammar, spelling mistakes, and awkward phrasing are common in phishing emails.
- **Urgent Language:** Messages that create a sense of urgency or fear, pressuring the recipient to act quickly.

Evaldas Rimasauskas

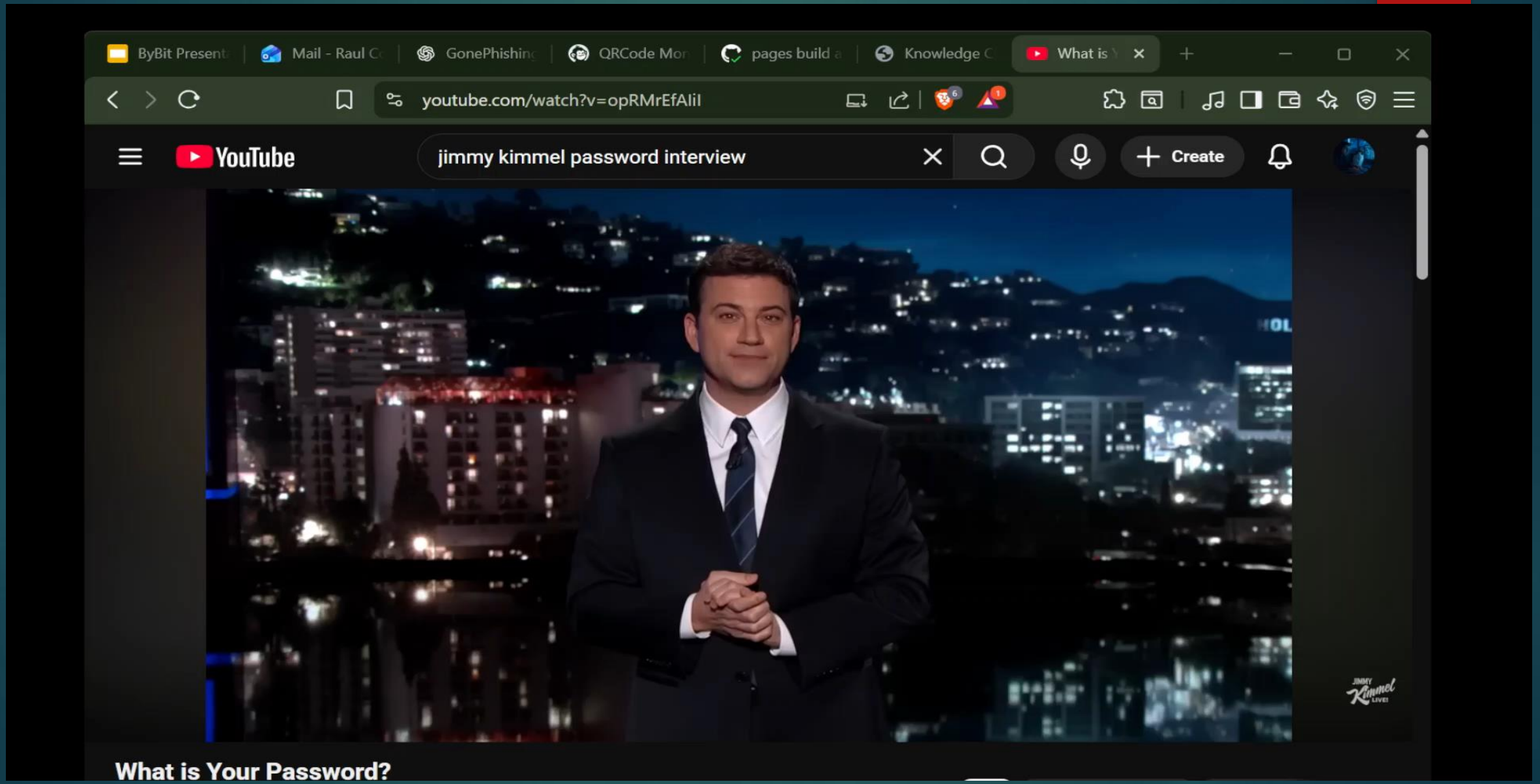
a Lithuanian national, is one of the most audacious examples of **CEO fraud and phishing impersonation** targeting major tech companies—**Google and Facebook**—between 2013 and 2015.

Case Study —$122 Millions stolen from Facebook and Google

Rimasauskas orchestrated a **Business Email Compromise (BEC)** scheme by:

- **Impersonating Quanta Computer**, a legitimate Taiwan-based hardware supplier that had real business relationships with Google and Facebook.
- **Registering a fake company** in Latvia with the same name—Quanta Computer—and opening bank accounts in Latvia and Cyprus under this name.
- **Sending phishing emails** to employees at Google and Facebook, pretending to be Quanta representatives. These emails included:
  - **Fake invoices**
  - **Forged contracts and letters**
  - **Documents with counterfeit corporate seals**
- The emails were convincing enough that employees at both companies **wired payments** to the fake Quanta accounts, believing they were settling legitimate debts.

What's your password?



RANSOMWARE

- Email attachments can be malicious in nature.
- That innocent-looking link, silently installs malicious software. Little by little, they steal your data. The hacker later reveals themselves asking for money or they will sell your data.
- On some occasion, they will encrypt your data as well. Locking you out, unless you pay.


Wanna Decryptor 1.0
Ooops, your files have been encrypted!
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files for free. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
How Do I Pay?
Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28
Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
QR Code
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1
Copy
Check Payment
Decrypt

Patient Dies During Cyber Attack – Waiting for Blood Results

- A long wait for a blood test result, due to the cyber-attack impacted pathology services at the time.
- Without this pathology service the NHS Trusts in the area were unable to do work involving transfusions or blood matching. Instead, they had to use O-type blood for everyone – the universal blood type.
- More than 1,000 cancer treatments were delayed, 2,000 outpatient appointments were canceled and more than 1,000 operations postponed.

A.I and Phishing

- (In previous trainings, misspelled words, grammar, etc. is what was taught to look out for but today's phishing attacks are different. With artificial intelligence, cybercriminals can craft flawless messages:
- Perfect spelling and grammar
- Context-aware language
- Personalized to you
- **Key Point:**
  AI-powered phishing emails can look just like real communication from your colleagues, bank, or favorite service—so old "red flags" are no longer enough.

Gabriela [redacted]

I know that calling +1 914-[redacted] or visiting 8[redacted] Place would be a convenient way to reach you in case you don't cooperate. Don't even try to hide from this. You've no idea what I'm capable of in Norwalk.

I suggest you read this message carefully. Take a minute to relax, breathe, and really dig into it. 'Cause we're about to discuss a deal between you and me, and I ain't playing games. You don't know anything about me whereas I know you very well and you must be wondering how, right?

Well, you've been a bit careless lately, clicking through those girlie videos and clicking on links, stumbling upon some not-so-safe sites. I actually placed a Malware on a porn website and you visited it to watch(if you know what I mean). When you were busy watching those videos, your device started working as a RDP (Remote Control) which provided me total accessibility to your smartphone. I can peep at everything on your screen, flick on your cam and mic, and you wouldn't even notice. Oh, and I have got access to all your emails, contacts, and social media accounts too.

Been keeping tabs on your pathetic life for a while now. It is simply your bad luck that I got to know about your blunder. I put in more days than I probably should've digging into your data. Extracted quite a bit of juicy info from your system. and I've seen it all. Yeah, Yeah, I've got footage of you doing filthy things in your house (nice setup, by the way). I then developed videos and screenshots where on one side of the screen, there's the videos you were playing, and on the other half, it is your vacant face. With just a single click, I can send this video to every single of your contacts.

I see you are getting anxious, but let's get real. Wholeheartedly, I am willing to wipe the slate clean, and let you move on with your daily life and wipe your slate clean. I am going to provide you two alternatives.
Option 1 is to disregard this e-mail. Let's see what is going to happen if you select this path. I will send your video to your contacts. The video was straight fire, and I can't even fathom the embarrasement you'll face when your colleagues, friends, and fam watch it. But hey, that's life, ain't it? Don't be playing the victim here.

Wiser second option is to pay me, and be confidential about it. We will call this my â€œprivacy chargesâ€. Lets discuss what happens if you select this choice. Your filthy secret remains private. I'll wipe everything clean once you send payment. You will make the payment by Bitcoin only. I want you to know I'm aiming for a win-win here. I stand by my promises.

Amount to be sent: USD 1950
My BTC Address: bc1qflsag8fmg48wy6zvqhja6eadf9005tkmxkjhw8

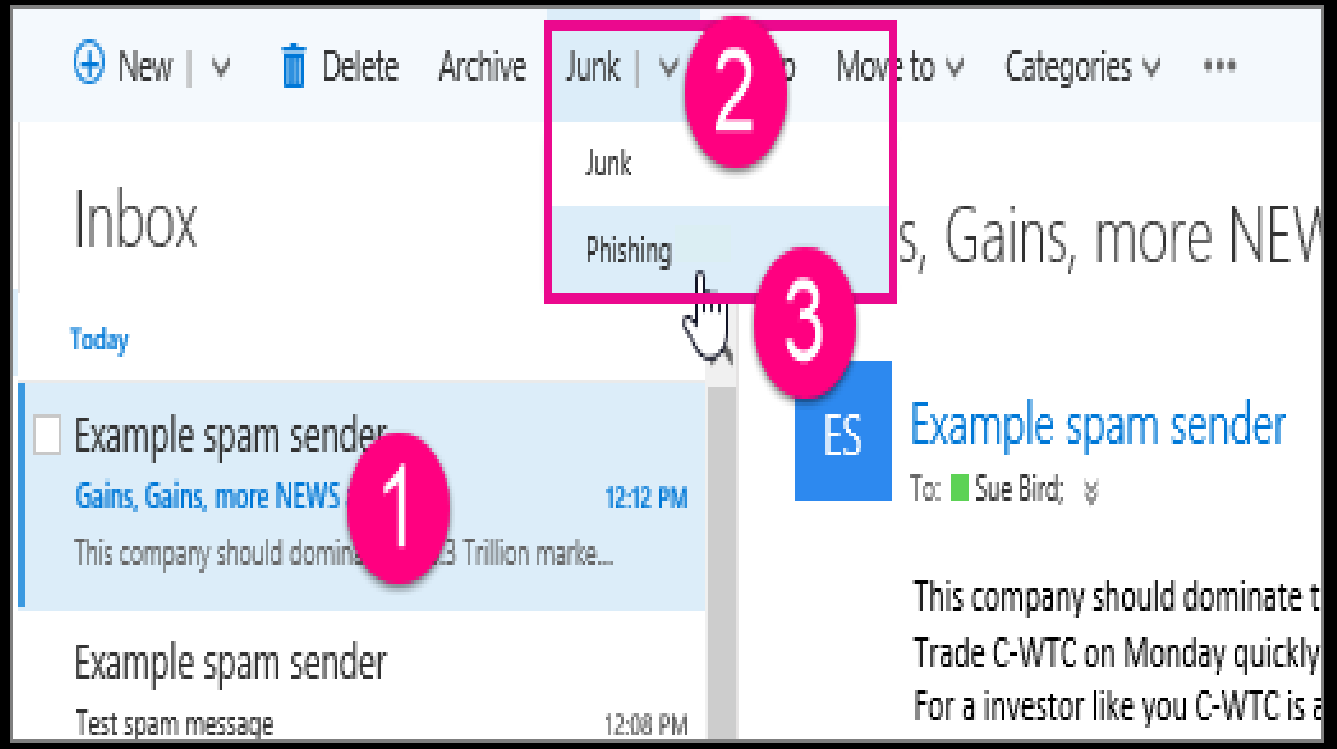
Let me tell ya, it's peanuts for your peace.

Pay Attention: You got one day to sort this out and I will only accept Bitcoin. I've a specific pixel in this e-mail, and right now I've been notified that you have read through this message. This email and Bitcoin address are custom-made for you, untraceable. If you are unfamiliar with Bitcoin, google it. You can buy it online or through a Bitcoin ATM in your neighborhood. There's no point in replying to this email or negotiating, it's pointless my price is fixed. As soon as you send the complete payment, my system will inform me and I will wipe out all the dirt I got on you. Remember if I catch that you've shared or discussed this email with anyone else, the video will instantly start getting sent to your contacts and I will post a physical tape to all of your neighborhood next week. And don't even think about turning off your phone or resetting it to factory settings, I already have all your data. I don't make mistakes, Gabriela.

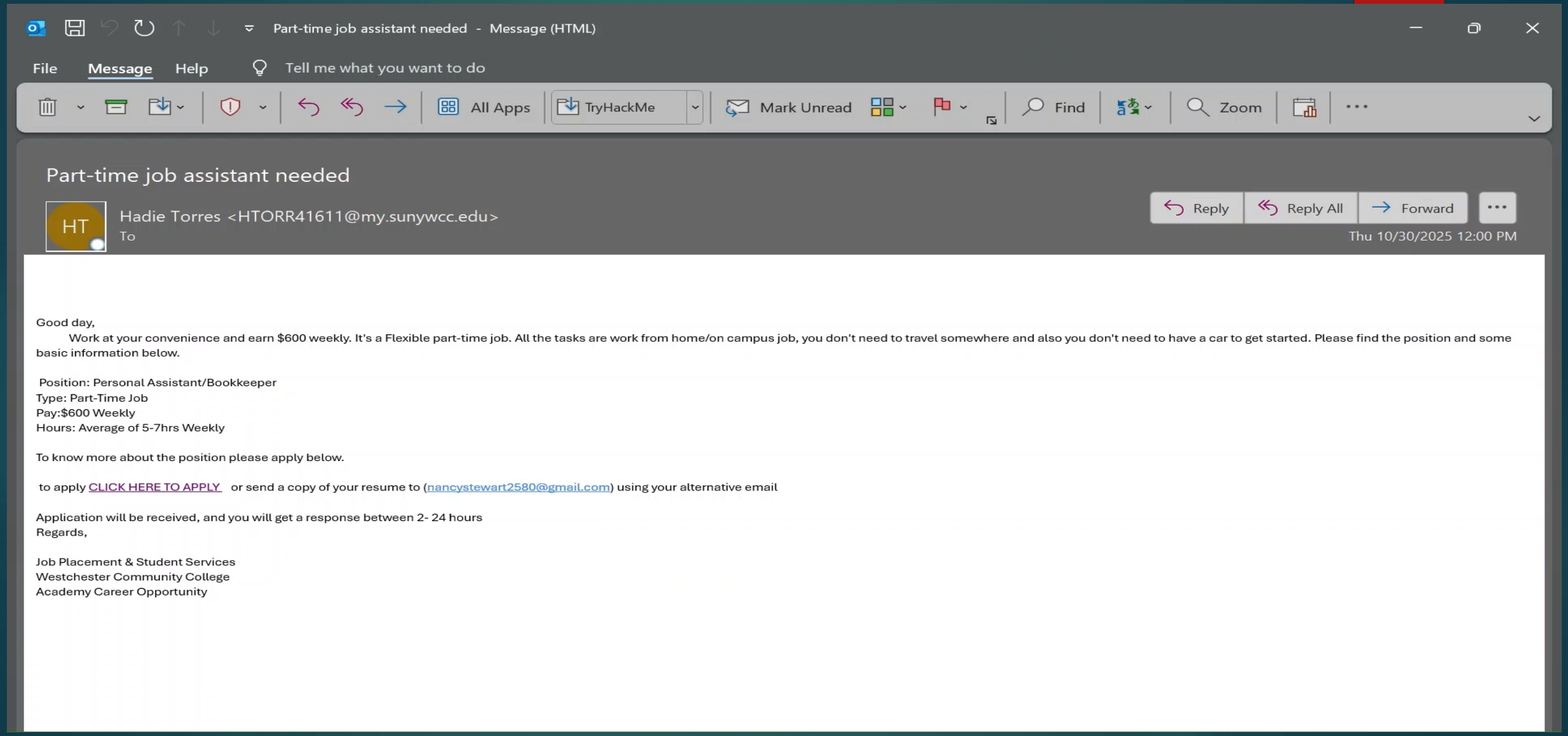
Honestly, those online tips about covering your camera aren't as useless as they seem. Now, I am waiting for my payment..

What to do

- DO NOT CLICK ON ANY LINKS
- DO Not Open/Download any attachments
- Hover over Links to view redirect.
- Check who the email is from.
- Check links using UrlScan.io
- Contact the Student HelpDesk at **914-606-5600** / **Phishbowl@sunywcc.edu**
- ***Contact your local police if you have suffered financially due to the phishing incident.***



Check Links


Part-time job assistant needed - Message (HTML)
File
Message
Help
Tell me what you want to do
All Apps
TryHackMe
Mark Unread
Find
Zoom
Part-time job assistant needed
HT
Hadie Torres <HTORR41611@my.sunywcc.edu>
To
Reply
Reply All
Forward
Thu 10/30/2025 12:00 PM
Good day,
Work at your convenience and earn $600 weekly. It's a Flexible part-time job. All the tasks are work from home/on campus job, you don't need to travel somewhere and also you don't need to have a car to get started. Please find the position and some basic information below.
Position: Personal Assistant/Bookkeeper
Type: Part-Time Job
Pay:$600 Weekly
Hours: Average of 5-7hrs Weekly
To know more about the position please apply below.
to apply CLICK HERE TO APPLY or send a copy of your resume to (nancystewart2580@gmail.com) using your alternative email
Application will be received, and you will get a response between 2- 24 hours
Regards,
Job Placement & Student Services
Westchester Community College
Academy Career Opportunity

GonePhishing

KNOWLEDGE CHECK


Questions?