

# TECH ACADEMY: STRONG PASSWORDS AND EMAIL SECURITY

Jason Walker | Neil Machowski | Jennifer Todd

# PREVENTION: WHAT A STRONG PASSWORD WILL DO FOR YOU

- Hard for hackers and bots to guess/decipher
- First line of defense
- Piece of mind
- Keeping your information safe (financial, medical, identity, etc.)

*PROVIDES ESSENTIAL PROTECTION.*

# PREVENTION: PASSWORDS AND PERMISSIONS

- Change Passwords every 90 days, do not use the same password within the last 5+ times. If your role relates to purchasing or high level administration, change more often (30 - 60 days)
- Never write down a password
- Limit Admin access. Most users can carry out their day-to-day tasks as a User or Super User
- Avoid generic logins and passwords if possible
- Never share your password

# WHAT ARE THE STANDARD PASSWORD REQUIREMENTS?

- Be at least 8 (eight) characters long
- One uppercase letter
- One lowercase letter
- One number
- One symbol

# PREVENTION: PASSWORDS AND PERMISSIONS

Avoid using personal information within passwords

- Social Engineering
- Avoid online self quizzes, surveys, and trends
  - *Generally, are answers to security questions*

# PREVENTION: PASSWORDS

- **Sentences** – First letter of each word
  - I Love Dis Stuff! 3-17-2022
  - iLds!3172022
- **Substitute symbols for letters**
  - MississippiLibraries
  - Mi\$\$iss99iLibr@ri3\$



Q&A

# A BASIC GUIDE TO EMAIL SECURITY







# OVERVIEW

- Why we have strong email security
- Types of email threats
- Q & A



# WHY WE HAVE STRONG EMAIL SECURITY

- Control of our device access
- Maintain communication confidentiality
- Stop ransomware attacks and other threats

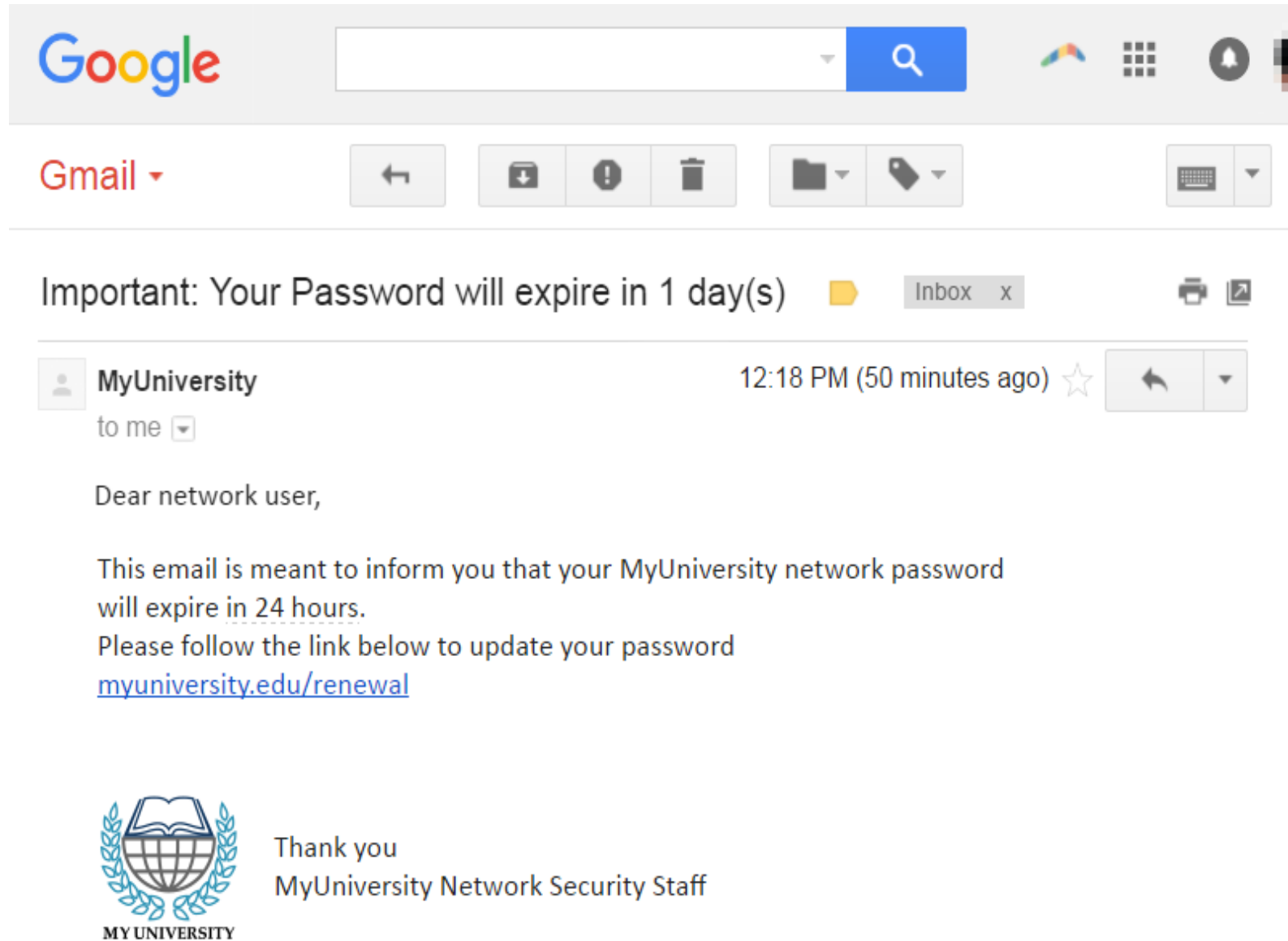


# COMMON EMAIL SECURITY THREATS

- Phishing and Whaling
- Business email compromise
- Malware
- Ransomware



# PHISHING EXAMPLE



The image shows a screenshot of a Gmail interface. At the top, the Google logo is on the left, followed by a search bar and navigation icons. Below this is the Gmail header with the 'Gmail' label and various icons for navigation. The main content area shows an email notification: 'Important: Your Password will expire in 1 day(s)'. The email is from 'MyUniversity' and is marked as 'Important'. The subject line is 'Important: Your Password will expire in 1 day(s)'. The sender is 'MyUniversity' and the recipient is 'to me'. The email was received at '12:18 PM (50 minutes ago)'. The body of the email reads: 'Dear network user, This email is meant to inform you that your MyUniversity network password will expire in 24 hours. Please follow the link below to update your password [myuniversity.edu/renewal](http://myuniversity.edu/renewal)'. At the bottom, there is a logo for 'MY UNIVERSITY' and the text 'Thank you MyUniversity Network Security Staff'.

Google

Gmail

Important: Your Password will expire in 1 day(s)

MyUniversity

12:18 PM (50 minutes ago)

to me

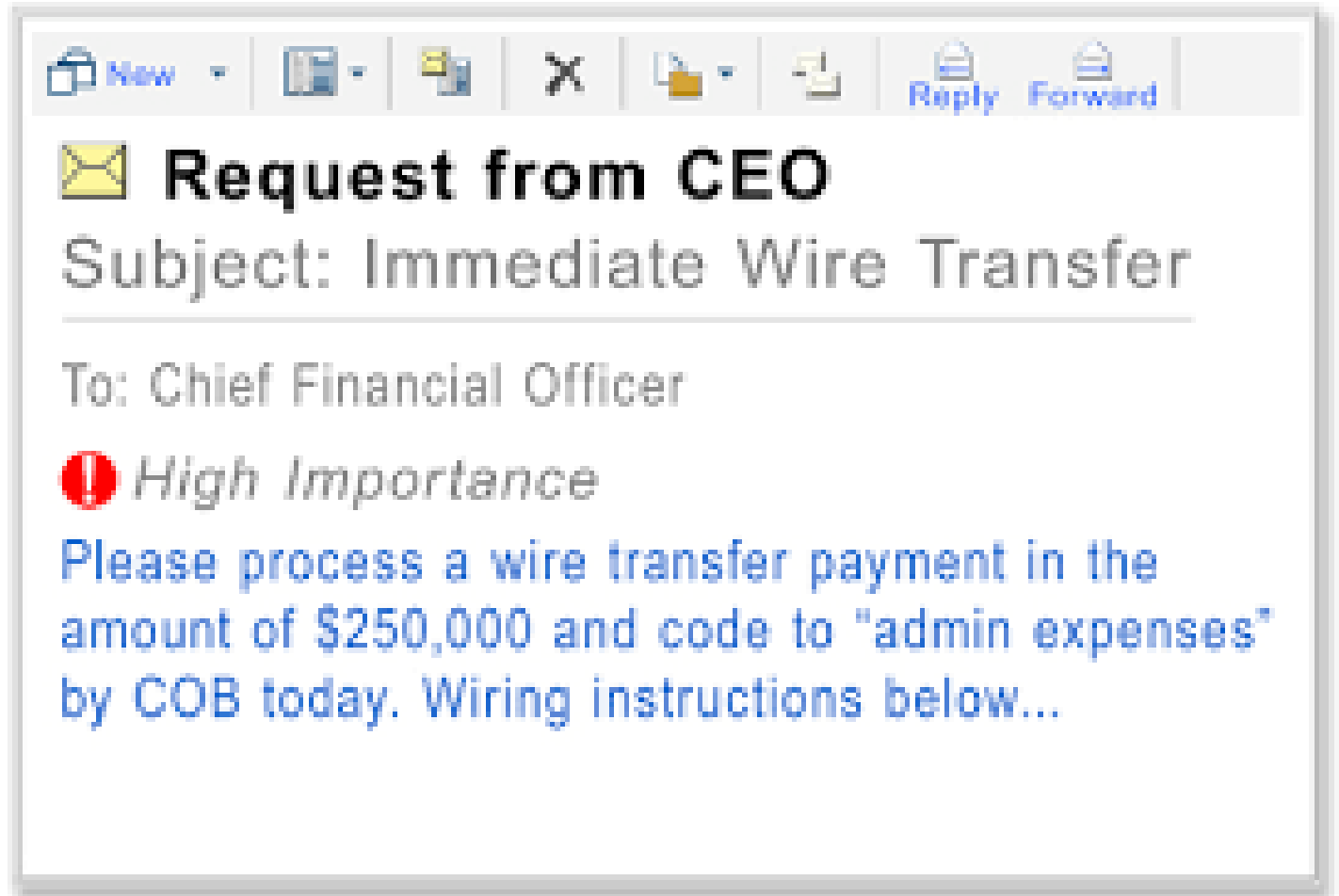
Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.  
Please follow the link below to update your password  
[myuniversity.edu/renewal](http://myuniversity.edu/renewal)

MY UNIVERSITY

Thank you  
MyUniversity Network Security Staff

**BUSINESS  
EMAIL  
COMPROMISE  
EXAMPLE**



# MALWARE EXAMPLE



**Dear brad**

To continue using your address confirm your ownership,

[Confirm ownership](#)

[admin@malware-traffic-analysis.net](mailto:admin@malware-traffic-analysis.net) setup team.

# RANSOMWARE EXAMPLE

NoCry Decryptor



## Oooooops All Your Files Are Encrypted ,NoCry

Can I Recover My Files ?

**Yes, You Can Recover All Your Files Easily And Quickly**

**But How ?**

**Send The Required Amount And  
I Will Send The Key To You For Decryption**

Your files will be lost on :

**71 : 58**

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

**Send \$100 worth of bitcoin to this address:**



1LHaSk425DzEoR6dT&t6gc4wkoKnQ4iVwK



# RED FLAGS

- X Are you the proper person?
  - Invoices
- X Sense of urgency
  - Reset password
- X Links
- X Grammar





# WHAT SHOULD YOU DO?

- If your email ends in **lib.ms.us**, report the email to MLC's helpdesk; otherwise, report to your tech staff
- **Do not** open attachments or links, or reply
- Delete the email
- If you *have* opened an attachment or link:
  - Disconnect device from network
  - Run an anti-malware scan immediately





# EMAIL SECURITY

- Spam Filters
  - Can't catch everything
  - Whitelist vs. Blacklist
- Multi-Factor Authentication
  - Online Banking



# QUESTIONS?



**HELP DESK PHONE**

(601) 432-4158



**HELP DESK EMAIL**

[helpdesk@mlc.lib.ms.us](mailto:helpdesk@mlc.lib.ms.us)