CHANGES

48th Annual Conference | Victoria Conference Centre

Securing the Business of Senior Care

BC Care Providers ASSOCIATION

#BCCPA2025

Title Sponsor

savaria

handicare | span

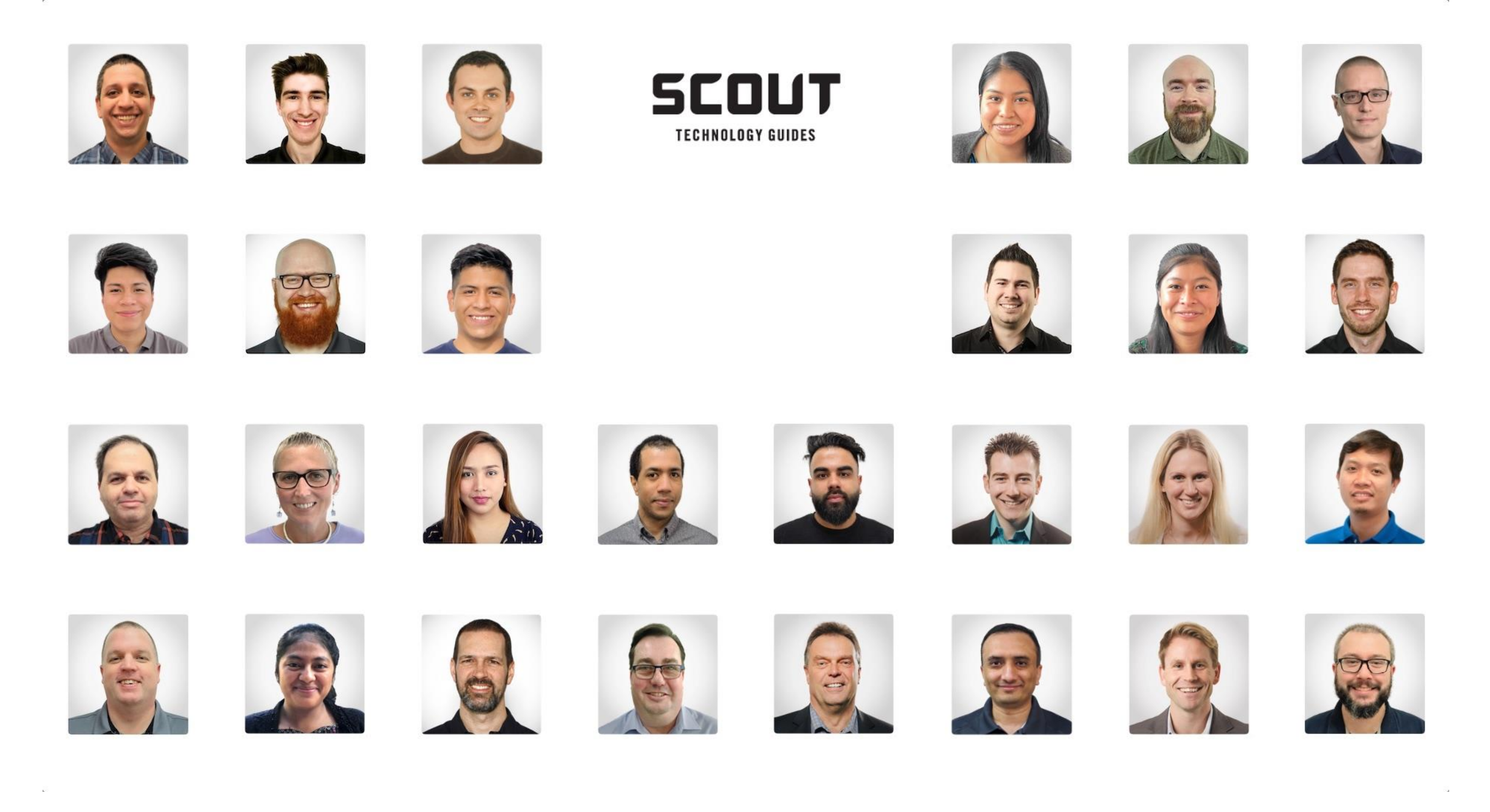
SCOUT

TECHNOLOGY GUIDES

Presented by Matt Dryfhout, Founder & CEO

Scout Technology Guides

Securing the Business of Senior Care

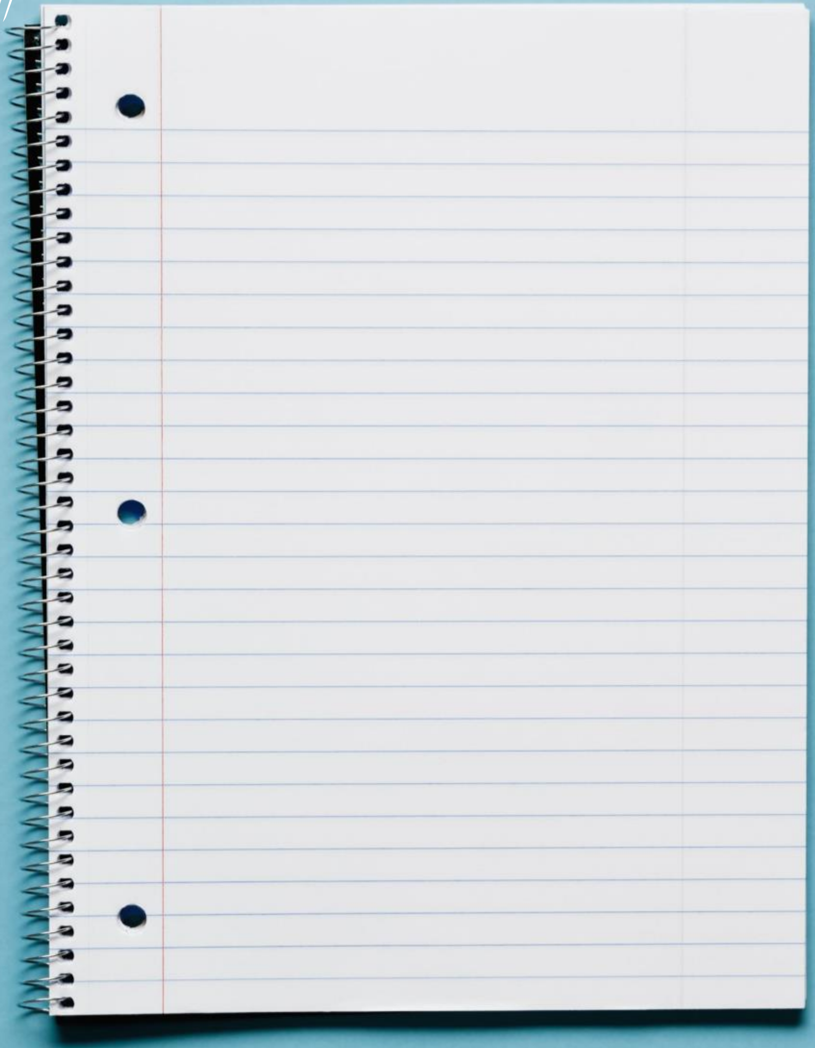


Introductions

- **Matt Dryfhout, Founder & CEO**
- **Scout was Founded in 2003** and now has 28 team members and ~55 core clients in the lower mainland that call on us for all their technology support (including Nursecall) and cyber security needs.
- **BCCPA Conference Silver sponsor for 8 years.**
- We're on a mission to **simplify** **cybersecurity!**

Workshop Agenda

- Understanding Password Evolution
- Identifying Phishing Threats
- Cyber Hygiene in Caregiving
- Reviewing Outbreak Examples paralleled with Health Care



SOME NICE FELLOW
HAS ENCRYPTED ALL MY DATA
memegenerator.net

Let’s start with the history of Passwords

- What was a good password?
  - **Complexity** – An upper case letter, lower case letter, number and / or symbol
  - **Length** – minimum of 8 characters, but we strive for at least 12
  - **Rotation** – change it once a year at least, quarterly was recommended
  - Can **not** contain a portion of your name

Where that got us:

A data composite of 2 million leaked passwords from 2016.

If you do not enforce a password policy effectively, this is what happens.

https://haveibeenpwned.com

1	**123456**
2	**password**
3	**12345678**
4	**qwerty**
5	**12345**
6	**123456789**
7	**football**
8	**1234**
9	**1234567**
10	**baseball**
11	**welcome**
12	**1234567890**
13	**abc123**
14	**111111**
15	**1qaz2wsx**
16	**dragon**
17	**master**
18	**monkey**
19	**letmein**
20	**login**
21	**princess**
22	**qwertyuiop**
23	**solo**
24	**passw0rd**
25	**starwars**

I save all my unique passwords in my browser, isn’t that good?

- Browser storage lacks robust encryption compared to dedicated tools.
- Common browsers are frequent targets for cyberattacks.
- Stored passwords can be easily accessed if the device is compromised.

Password Policy Standards in 2025

Focusing on your primary account (Microsoft 365 or Google)

According to Microsoft 365 Guidance (April 2, 2025):

Disable forced expiration
Set passwords to **never expire**—shift focus to more effective controls

Emphasize length over complexity
Enforce a minimum of **8 characters**, support up to **64** for passphrases

Mandate MFA
Use multi-factor authentication as the primary compensating control

Change only on compromise
Aligns with NIST SP 800-63B: no arbitrary rotation, reset only if there's evidence of a breach

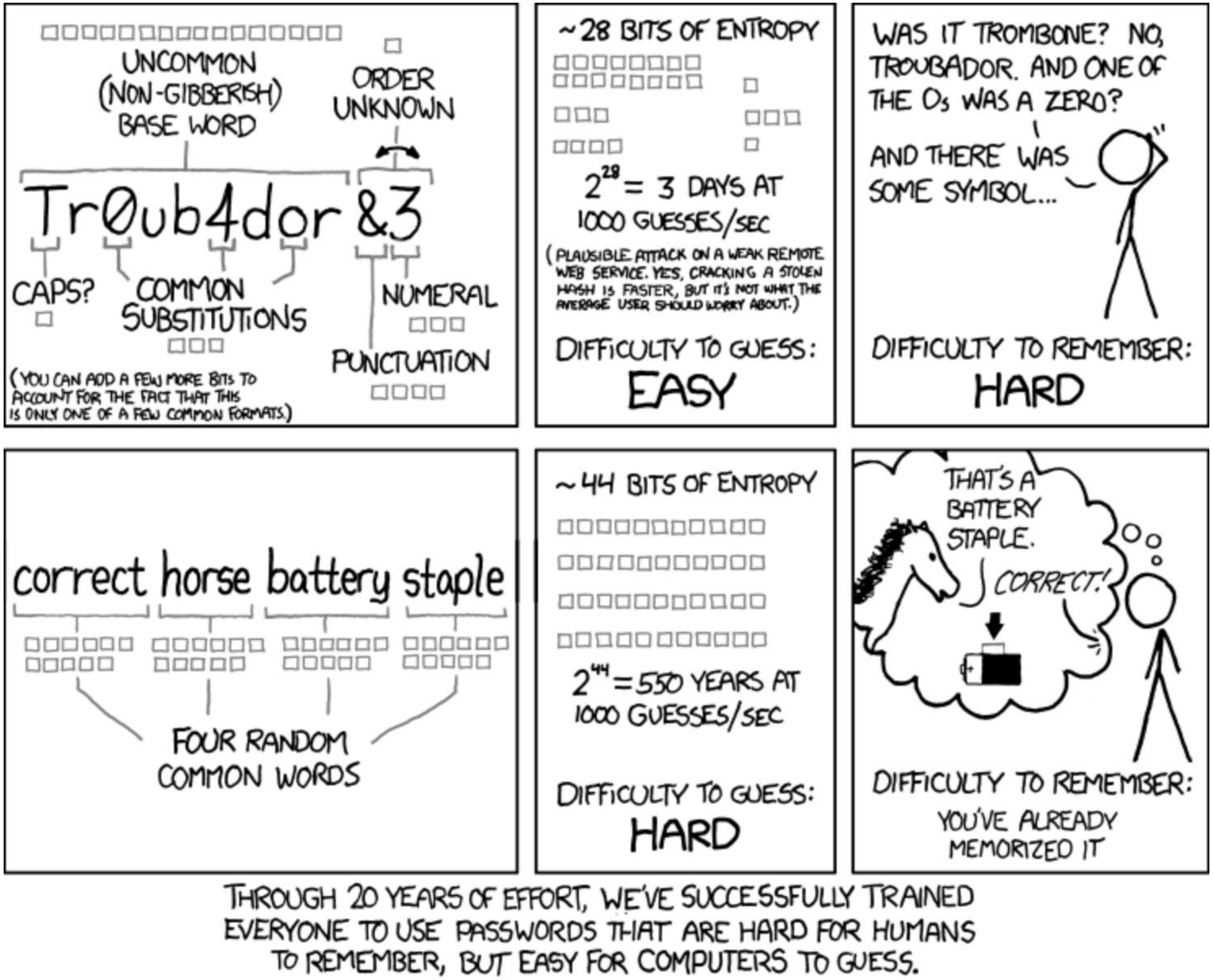
Source: Password policy recommendations - Microsoft 365 admin | Microsoft Learn

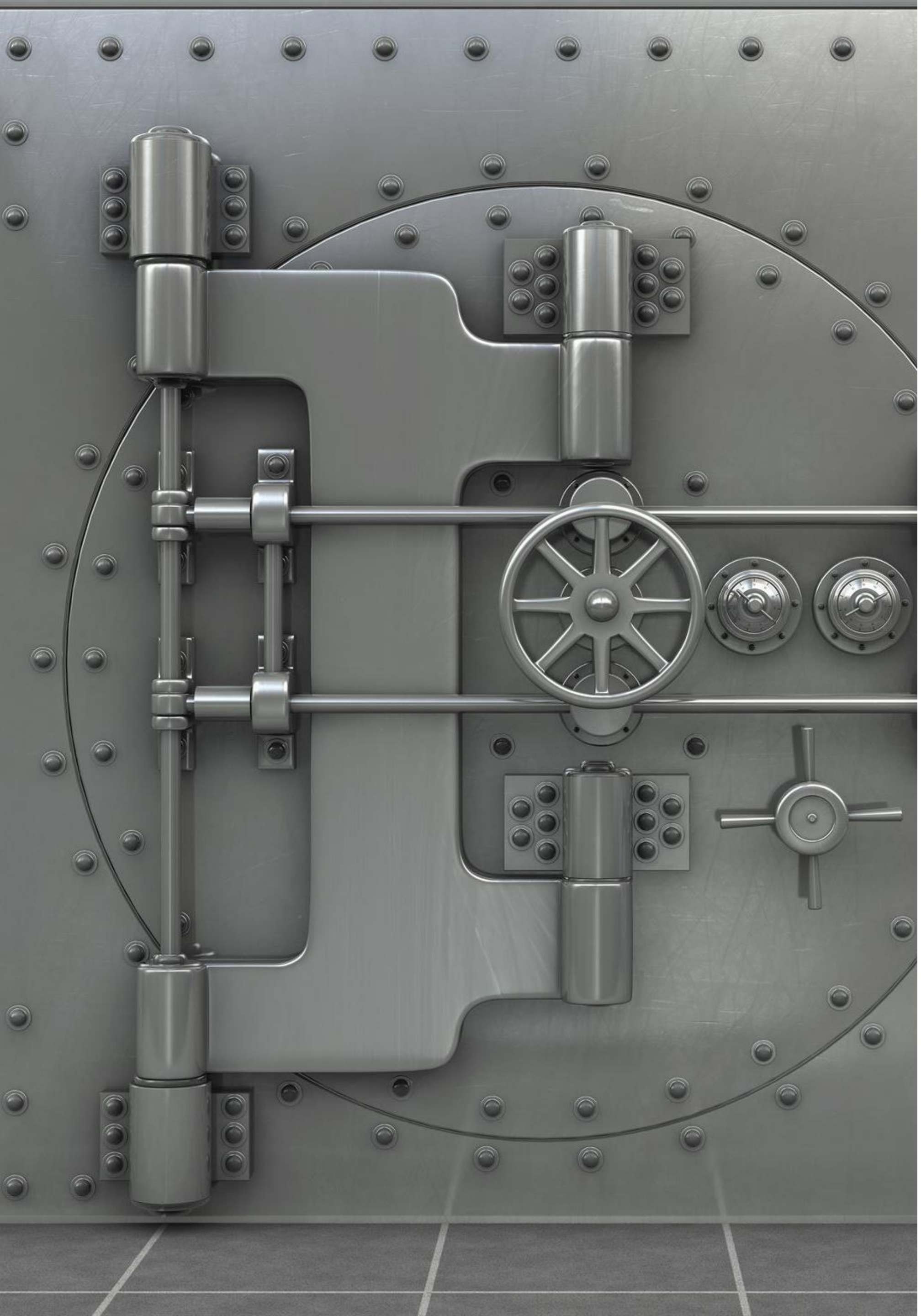
Introducing Passphrases

- Just because it's hard for you to remember does not mean it is more secure

- Never use the same password everywhere!

- https://xkcd.com/936/


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



Benefits of Using a Password Manager

- Generates strong, unique passwords for each account.
- Stores all passwords securely in one place which are synchronized across multiple devices
- Automatically fills in login forms to save time.
- Facilitates safe sharing of passwords with trusted users.
- Examples: Lastpass, 1password, bitwarden

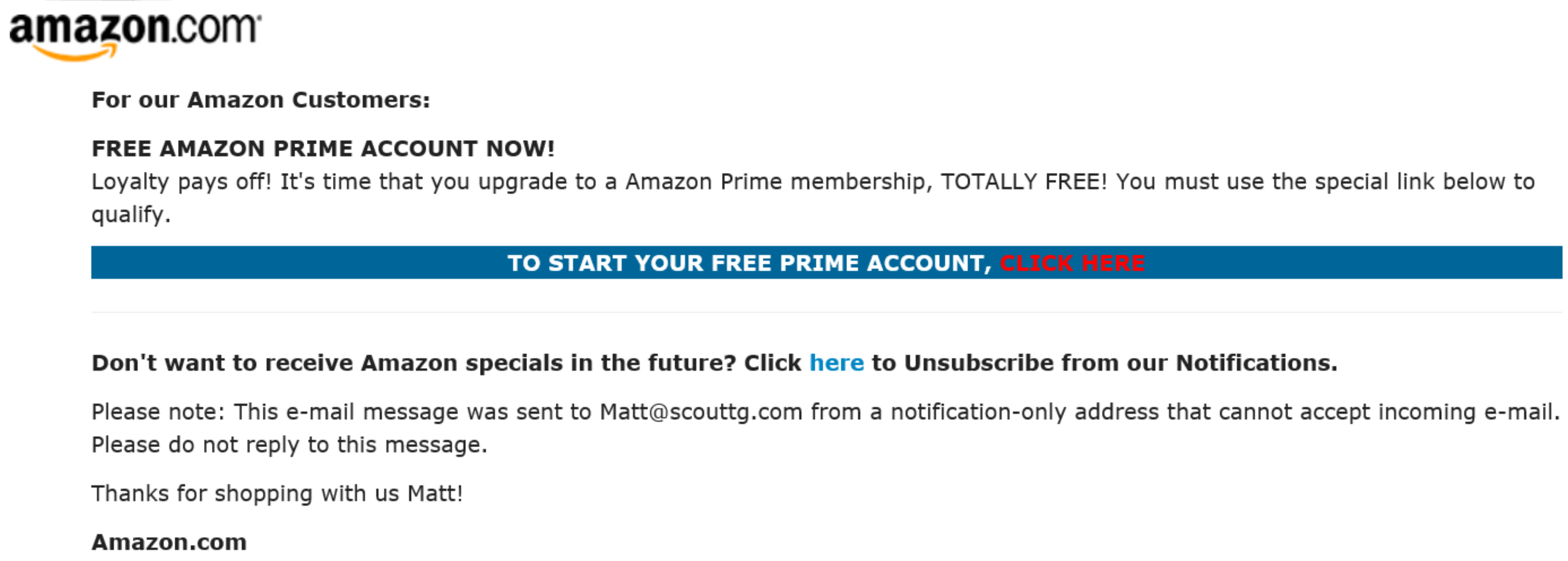
Understanding Multi-Factor Authentication (MFA)

- MFA adds an extra layer of security beyond passwords.
- In healthcare, think of MFA as wearing a mask for protection.
- Just as masks reduce infection, MFA prevents unauthorized access.
- Users must provide two or more verification factors.
- This method significantly reduces the risk of breaches.

Understanding Phishing Tactics

- Phishing is a major threat to cybersecurity today.
- Bad actors use various tactics to deceive victims.
- AI enhances malicious actors phishing techniques making it harder for human AND spam filter detection.

Phishing examples and quiz coming!



For our Amazon Customers:

FREE AMAZON PRIME ACCOUNT NOW!
Loyalty pays off! It's time that you upgrade to a Amazon Prime membership, TOTALLY FREE! You must use the special link below to qualify.

TO START YOUR FREE PRIME ACCOUNT, CLICK HERE

Don't want to receive Amazon specials in the future? Click here to Unsubscribe from our Notifications.

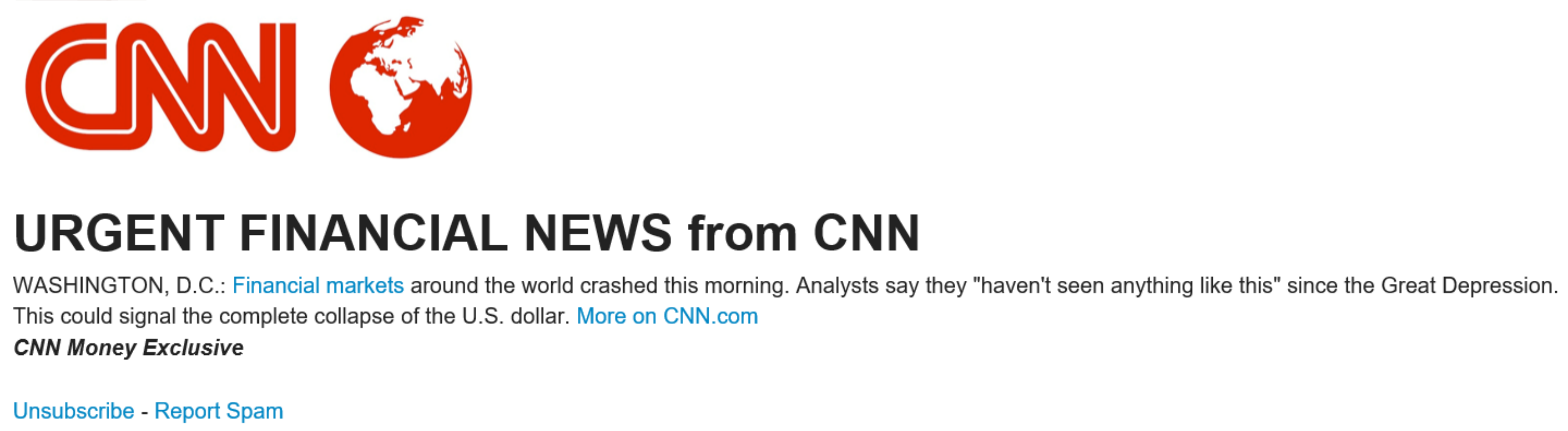
Please note: This e-mail message was sent to Matt@scouttg.com from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.

Thanks for shopping with us Matt!

Amazon.com

Example Phishing Emails:

Example Phishing Emails:



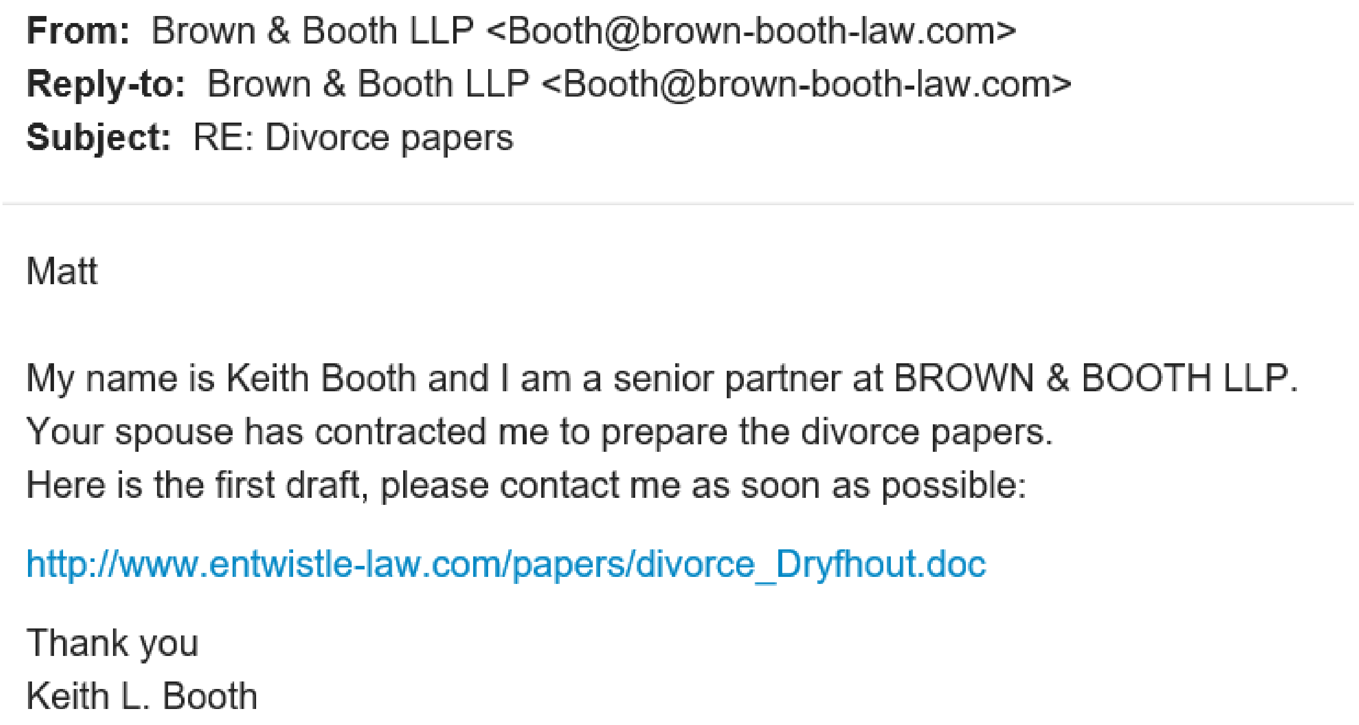
URGENT FINANCIAL NEWS from CNN

WASHINGTON, D.C.: Financial markets around the world crashed this morning. Analysts say they "haven't seen anything like this" since the Great Depression. This could signal the complete collapse of the U.S. dollar. More on CNN.com

CNN Money Exclusive

Unsubscribe - Report Spam

Example Phishing Emails:



From: Brown & Booth LLP <Booth@brown-booth-law.com>
Reply-to: Brown & Booth LLP <Booth@brown-booth-law.com>
Subject: RE: Divorce papers

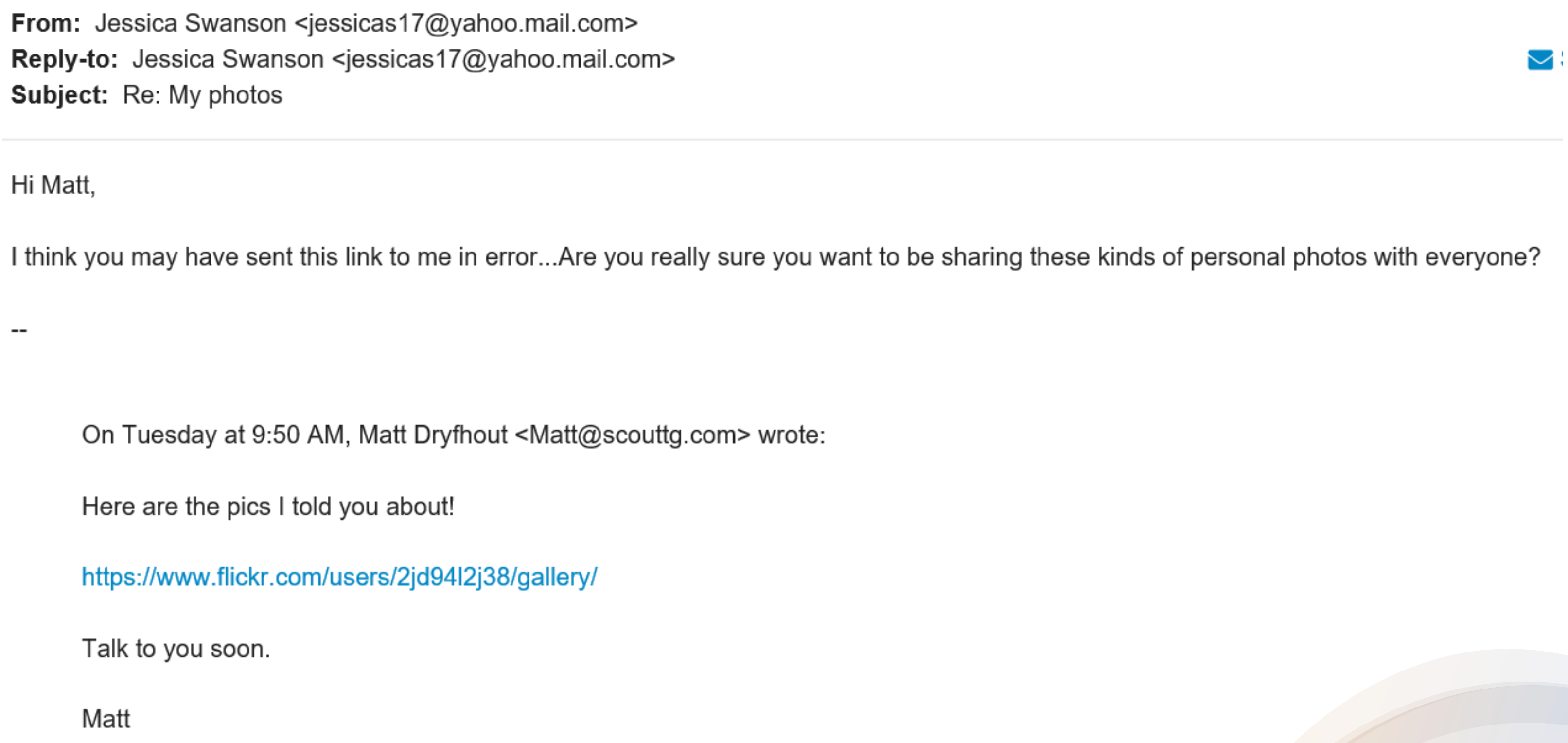
Matt

My name is Keith Booth and I am a senior partner at BROWN & BOOTH LLP.
Your spouse has contracted me to prepare the divorce papers.
Here is the first draft, please contact me as soon as possible:

http://www.entwistle-law.com/papers/divorce_Dryfhout.doc

Thank you
Keith L. Booth

Example Phishing Emails:



From: Jessica Swanson <jessicas17@yahoo.mail.com>
Reply-to: Jessica Swanson <jessicas17@yahoo.mail.com>
Subject: Re: My photos

Hi Matt,

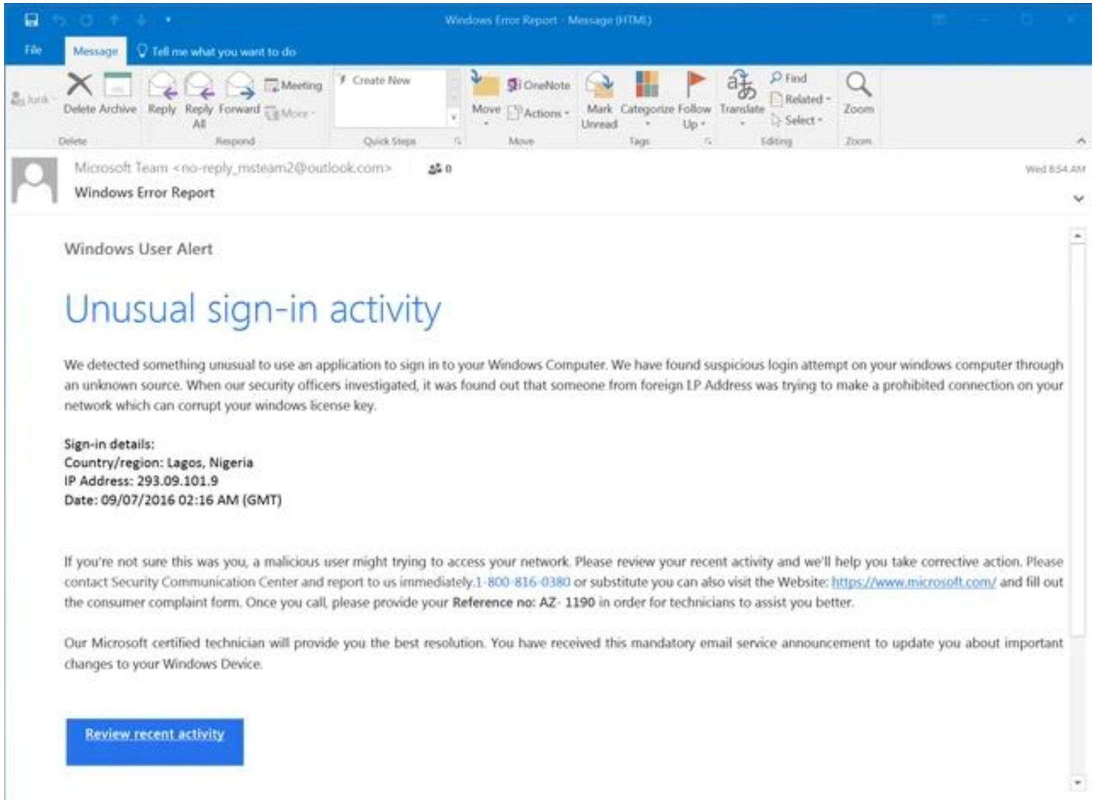
I think you may have sent this link to me in error...Are you really sure you want to be sharing these kinds of personal photos with everyone?

--

> On Tuesday at 9:50 AM, Matt Dryfhout <Matt@scouttg.com> wrote:
>
> Here are the pics I told you about!
>
> https://www.flickr.com/users/2jd94l2j38/gallery/
>
> Talk to you soon.
>
> Matt

Phishing Example: Microsoft Security Alert

- Subject: 'Microsoft Account Sign-in Attempt Blocked'
- Body instructs calling a 1-800 number to resolve issues.
- Red Flag: Requests phone call rather than secure portal update.



Microsoft Team <no-reply_msteam2@outlook.com>

Windows Error Report

Wed 8:54 AM

Windows User Alert

Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

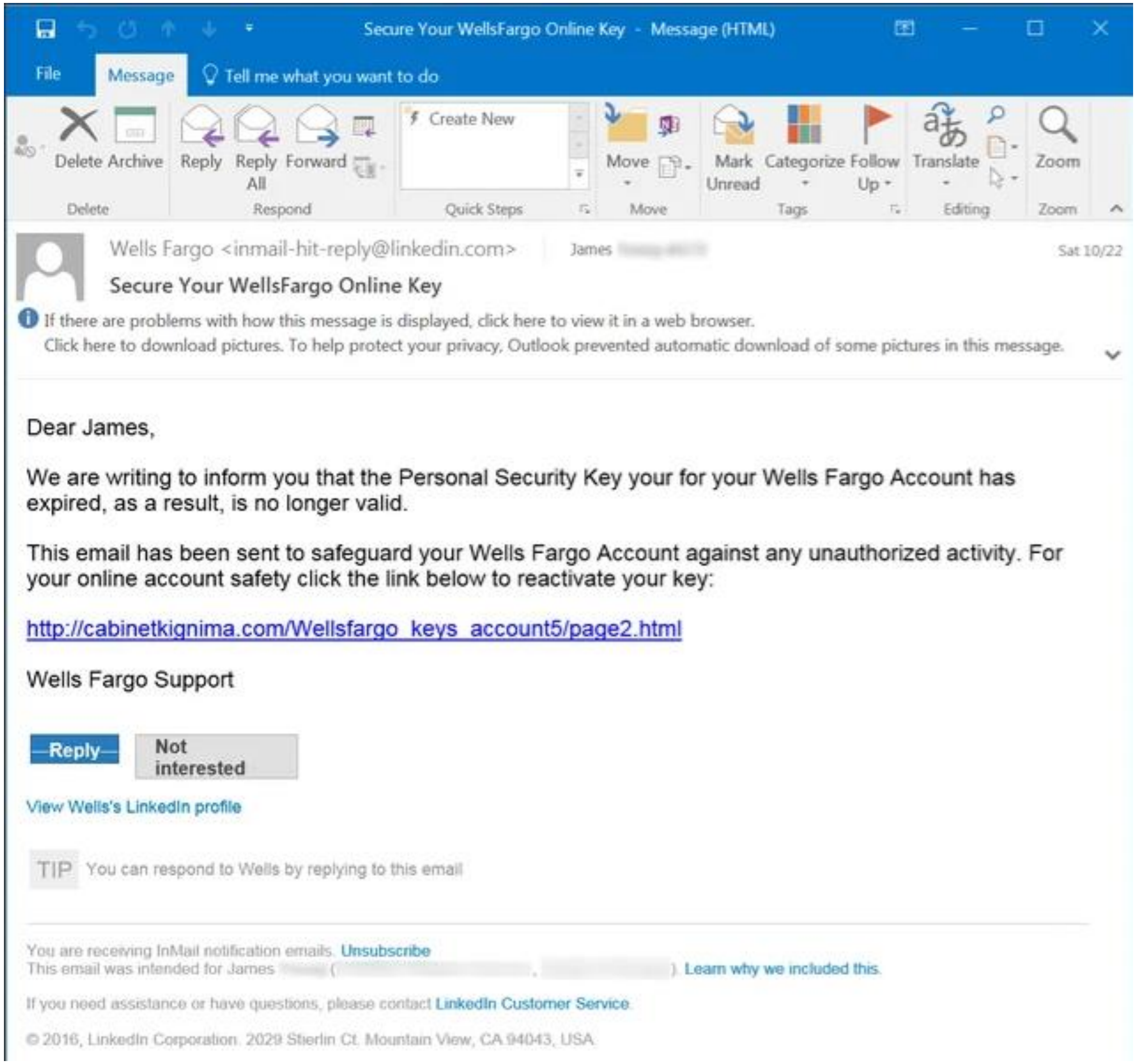
Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)

If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your **Reference no: AZ- 1190** in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

Phishing Example: Wells Fargo LinkedIn Scam - Part 1

- Use LinkedIn to deliver the message to inbox passing all filters
- Link leads to malicious domain hosting a login form.
- Red Flag: Hover URLs before clicking.



Wells Fargo <inmail-hit-reply@linkedin.com> James [redacted] Sat 10/22

Secure Your WellsFargo Online Key

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear James,

We are writing to inform you that the Personal Security Key your for your Wells Fargo Account has expired, as a result, is no longer valid.

This email has been sent to safeguard your Wells Fargo Account against any unauthorized activity. For your online account safety click the link below to reactivate your key:

http://cabinetkignima.com/Wellsfargo_keys_account5/page2.html

Wells Fargo Support

View Wells's LinkedIn profile

TIP You can respond to Wells by replying to this email

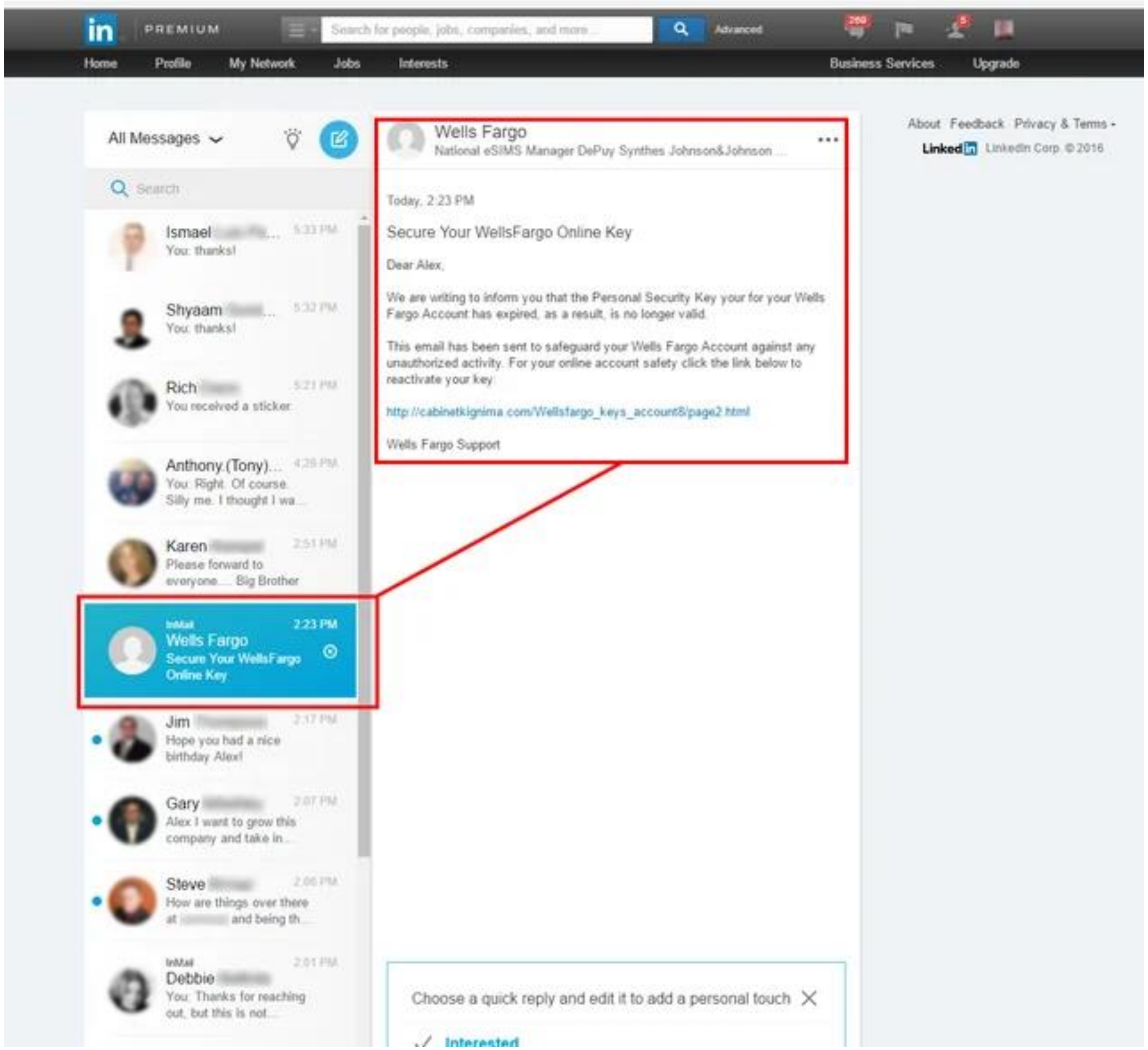
You are receiving InMail notification emails. Unsubscribe
This email was intended for James [redacted] ([redacted], [redacted]). Learn why we included this.

If you need assistance or have questions, please contact LinkedIn Customer Service.

© 2016, LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, USA

Phishing Example: Wells Fargo LinkedIn Scam – Part 2

- InMail from fake Wells Fargo profile with credentials link.
- Link leads to malicious domain hosting a login form.
- Red Flag: Bad actors can use fake accounts in any social networks to suggest credibility


in PREMIUM
Search for people, jobs, companies, and more...
Advanced
Home
Profile
My Network
Jobs
Interests
Business Services
Upgrade
All Messages
Search
About Feedback Privacy & Terms
Linked in LinkedIn Corp. © 2016

Ismael [redacted]... 5:33 PM
You: thanks!

Shyaam [redacted]... 5:32 PM
You: thanks!

Rich [redacted] 5:21 PM
You received a sticker

Anthony (Tony)... 4:28 PM
You: Right. Of course. Silly me. I thought I wa...

Karen [redacted] 2:51 PM
Please forward to everyone.... Big Brother

InMail 2:23 PM
Wells Fargo
Secure Your WellsFargo Online Key

Jim [redacted] 2:17 PM
Hope you had a nice birthday Alex!

Gary [redacted] 2:07 PM
Alex I want to grow this company and take in...

Steve [redacted] 2:06 PM
How are things over there at [redacted] and being th...

InMail 2:01 PM
Debbie [redacted]
You: Thanks for reaching out, but this is not...

Wells Fargo
National eSIMS Manager DePuy Synthes Johnson&Johnson ...

Today, 2:23 PM

Secure Your WellsFargo Online Key

Dear Alex,

We are writing to inform you that the Personal Security Key your for your Wells Fargo Account has expired, as a result, is no longer valid.

This email has been sent to safeguard your Wells Fargo Account against any unauthorized activity. For your online account safety click the link below to reactivate your key:

http://cabinetkignima.com/Wellsfargo_keys_account8/page2.html

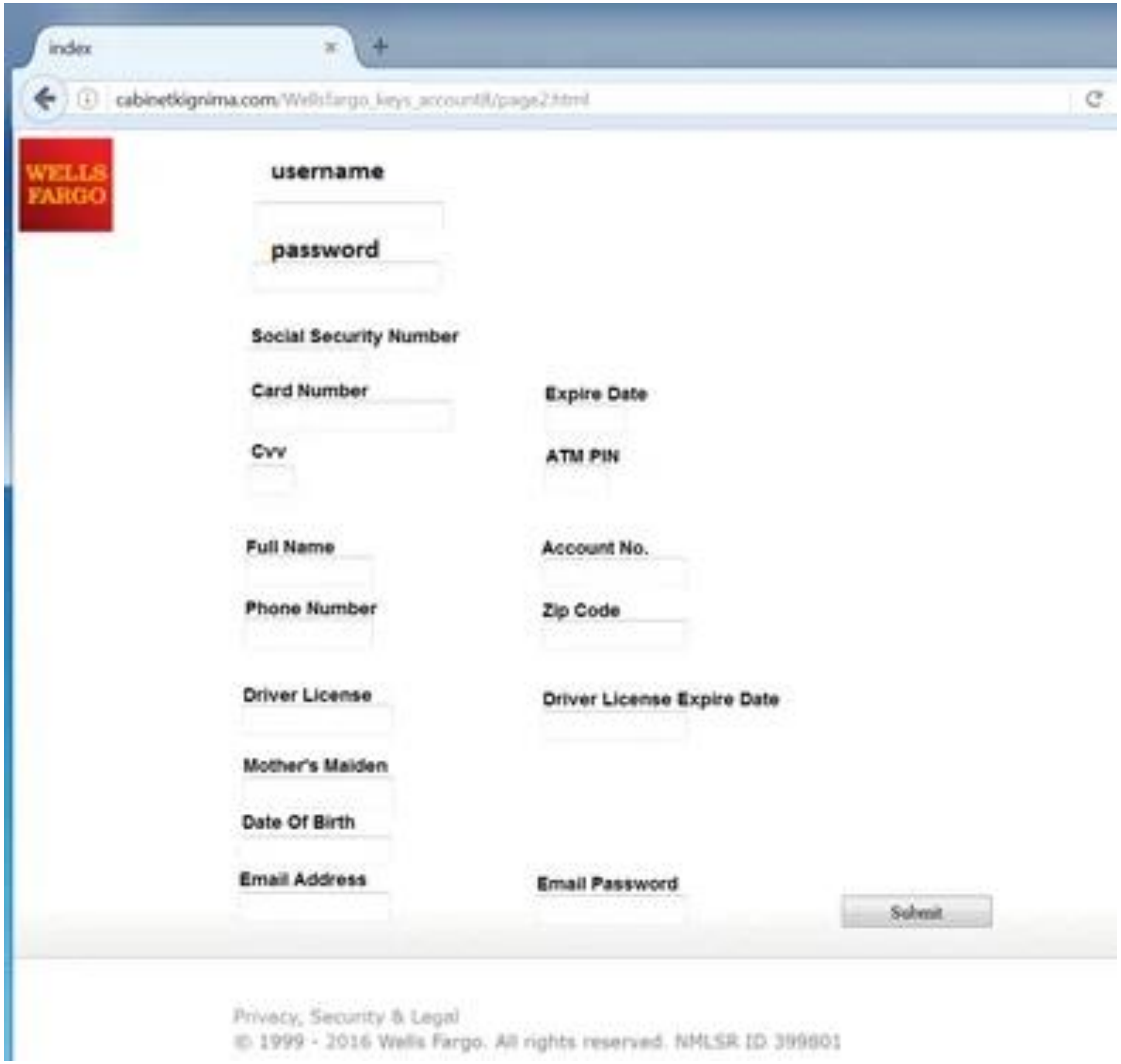
Wells Fargo Support

Choose a quick reply and edit it to add a personal touch

✓ Interested

Phishing Example: Wells Fargo LinkedIn Scam – Part 3

- This is the fake web form that sends results to the bad actor
- The elderly are most vulnerable to these
- Red Flag: URL is not Wellsfargo.com



cabinetkignima.com/Wellsfargo_keys_account8/page2.html

username

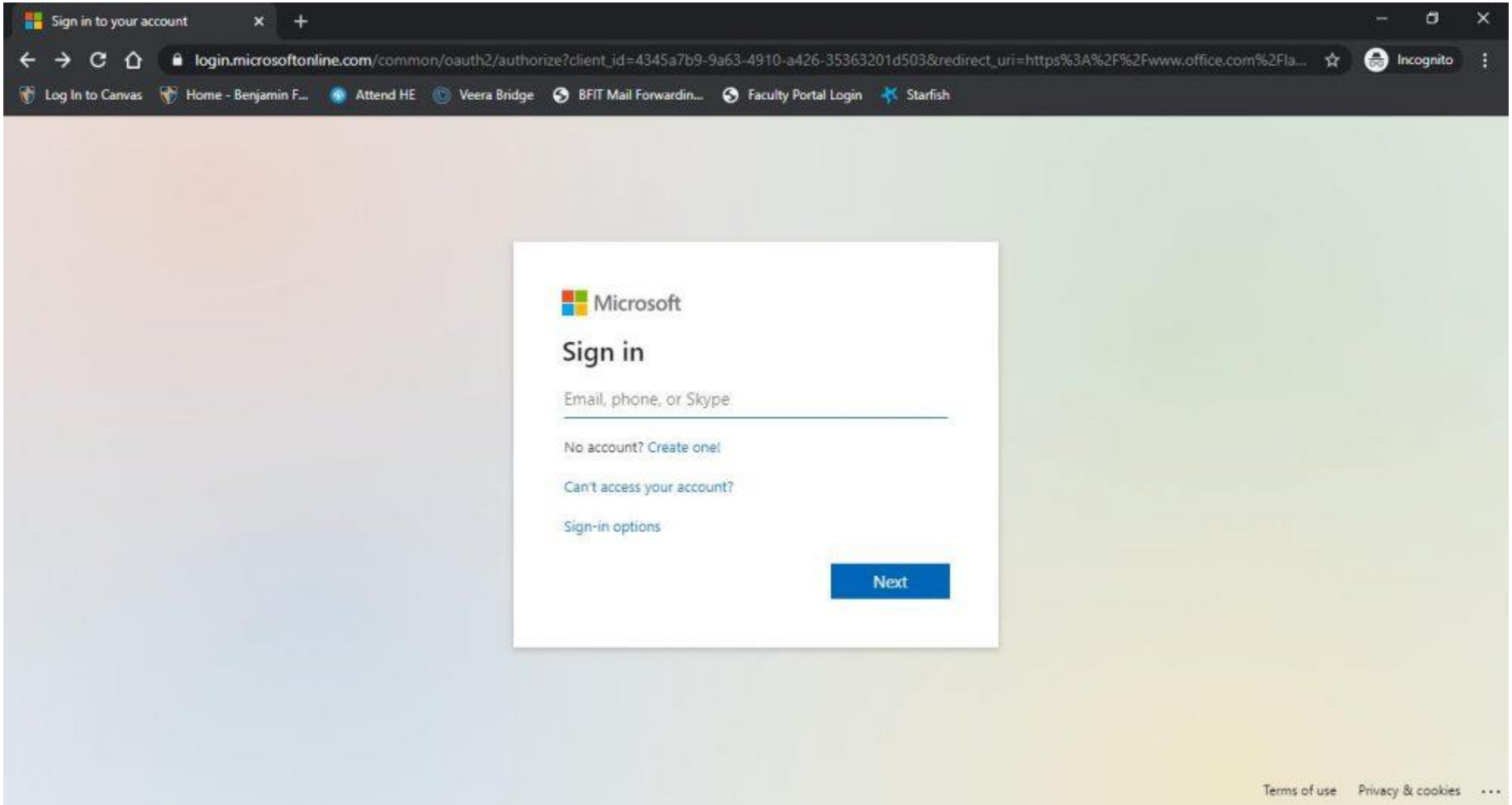
password

Social Security Number

Card Number	Expire Date
Cvv	ATM PIN
Full Name	Account No.
Phone Number	Zip Code
Driver License	Driver License Expire Date
Mother's Maiden	
Date Of Birth	
Email Address	Email Password

Privacy, Security & Legal
© 1999 - 2016 Wells Fargo. All rights reserved. NMLSR ID 399801

Recognize this?


Sign in to your account
login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201d503&redirect_uri=https%3A%2F%2Fwww.office.com%2Fla...
Incognito
Log In to Canvas
Home - Benjamin F...
Attend HE
Veera Bridge
BFIT Mail Forwardin...
Faculty Portal Login
Starfish

Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Sign-in options

MFA Cookie Theft in a Nutshell

- Fake login pages mimic real Microsoft login
- User logs in, attacker captures session cookie
- Cookie acts like a key—no password or MFA needed
- Attackers can enter anytime, undetected

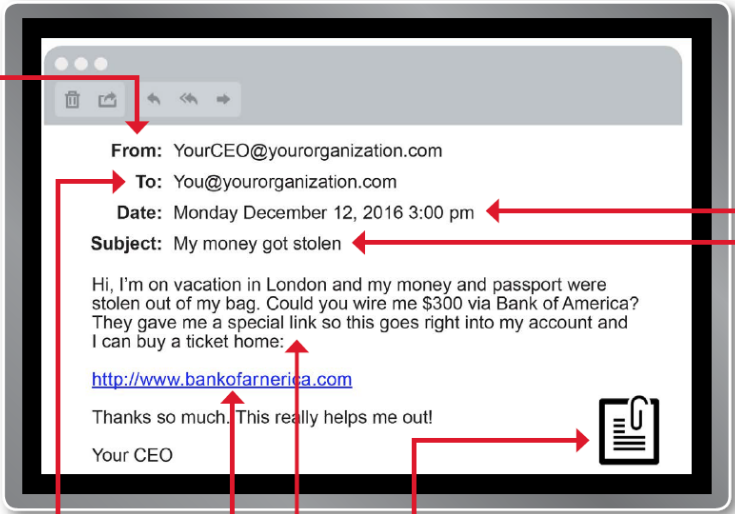
Why It’s Dangerous

- MFA appears to block access, but cookie theft bypasses it
- Phishing pages on trusted domains evade filters
- Tiny URL changes go unnoticed by most users
- Full mailbox access and data theft possible

Protection Steps

- Avoid public wifi (like airports) and use phone hotspot instead
- Type the URL yourself instead of clicking links
- Keep browser and OS updated and disable unapproved browser extensions
- Report odd login prompts immediately
- 24/7 Cloud Monitoring is the only defense today to catch this

How to spot the phishing emails Handout:



From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

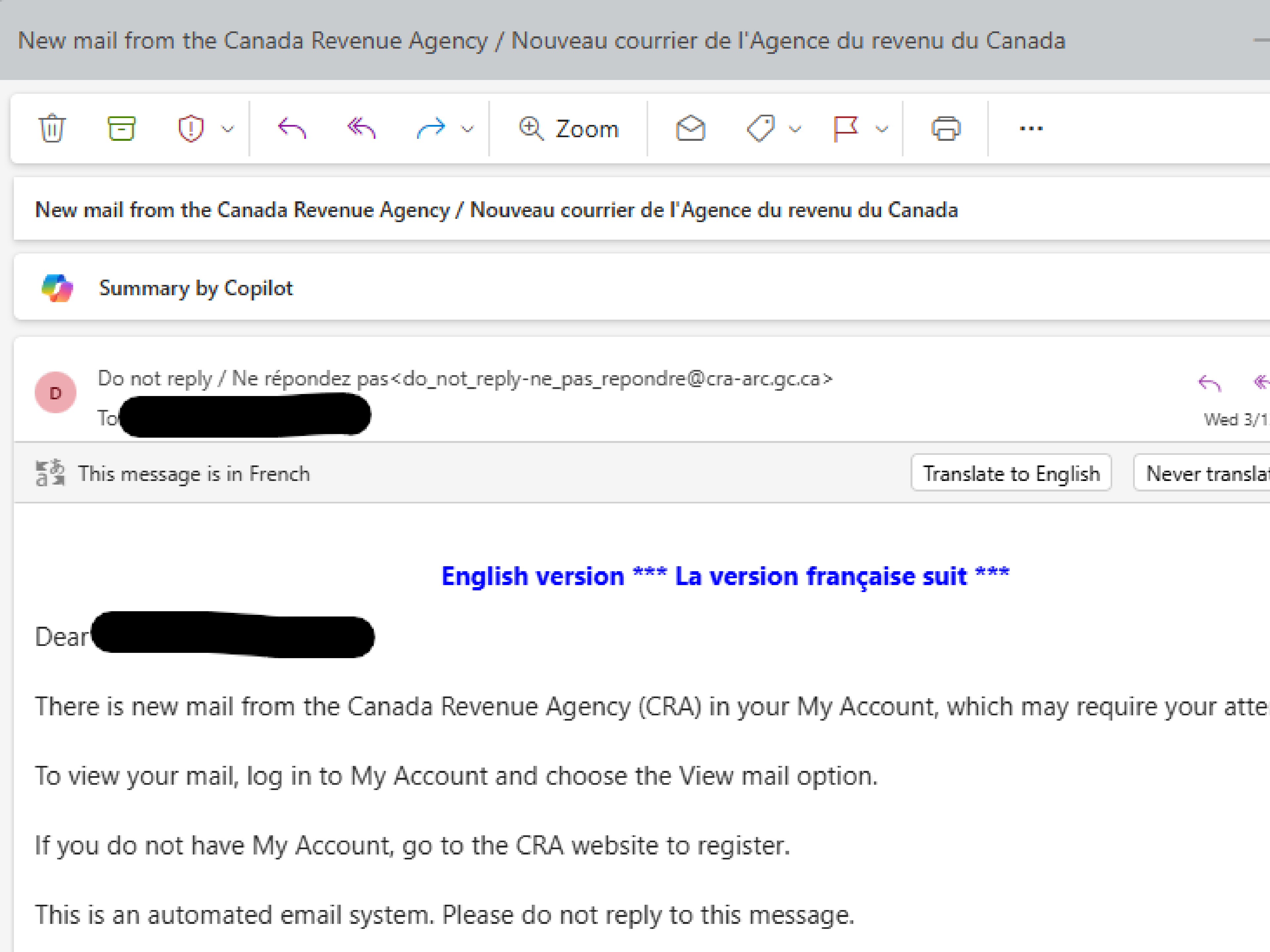
- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Quiz Time

Phishing or Not?



New mail from the Canada Revenue Agency / Nouveau courrier de l'Agence du revenu du Canada

New mail from the Canada Revenue Agency / Nouveau courrier de l'Agence du revenu du Canada

Do not reply / Ne répondez pas<do_not_reply-ne_pas_repondre@cra-arc.gc.ca>

To [redacted]

Wed 3/1

English version * La version française suit *****

Dear [redacted]

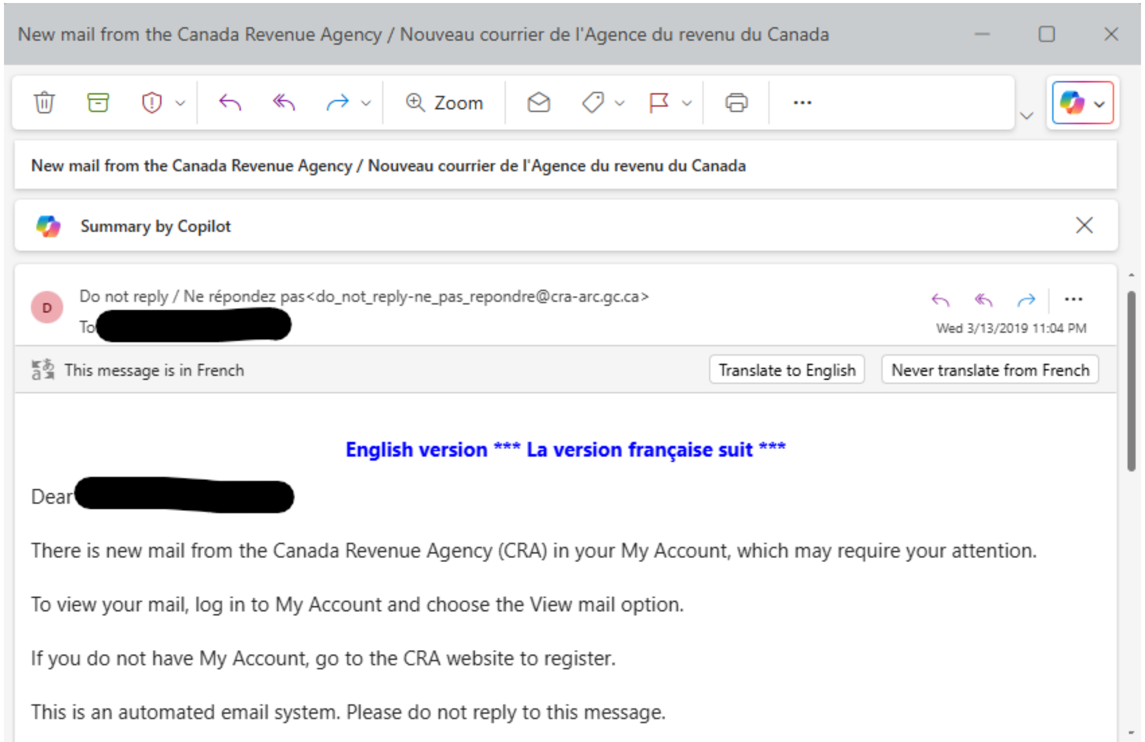
There is new mail from the Canada Revenue Agency (CRA) in your My Account, which may require your atte

To view your mail, log in to My Account and choose the View mail option.

If you do not have My Account, go to the CRA website to register.

This is an automated email system. Please do not reply to this message.

Not Phishing! (email directs user to go to their account without a link and the from is the valid government domain)



New mail from the Canada Revenue Agency / Nouveau courrier de l'Agence du revenu du Canada

New mail from the Canada Revenue Agency / Nouveau courrier de l'Agence du revenu du Canada

D Do not reply / Ne répondez pas<do_not_reply-ne_pas_repondre@cra-arc.gc.ca>

To [redacted]

Wed 3/13/2019 11:04 PM

This message is in French

English version * La version française suit *****

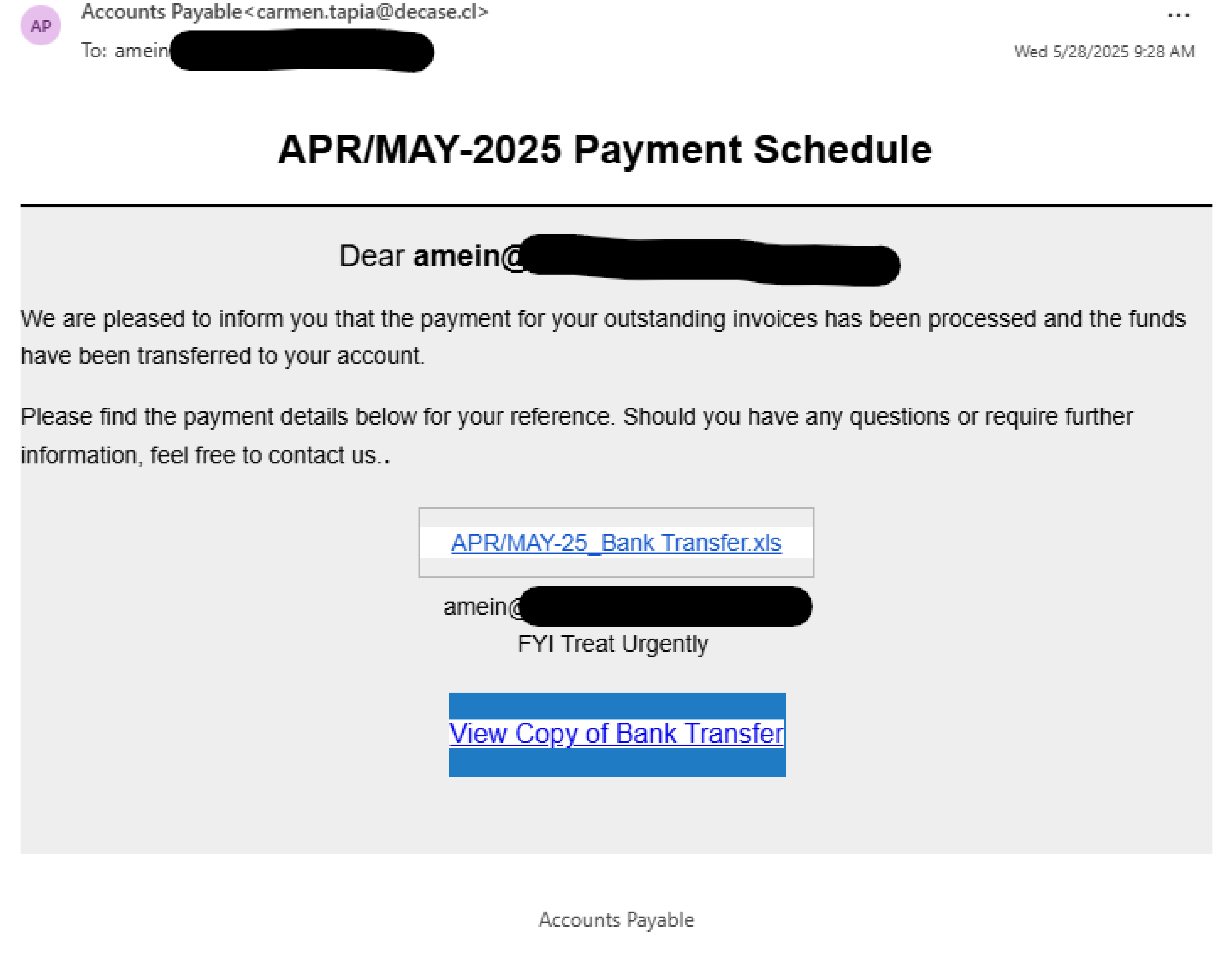
Dear [redacted]

There is new mail from the Canada Revenue Agency (CRA) in your My Account, which may require your attention.

To view your mail, log in to My Account and choose the View mail option.

If you do not have My Account, go to the CRA website to register.

This is an automated email system. Please do not reply to this message.



Accounts Payable<carmen.tapia@decase.cl>

To: amein[redacted]

Wed 5/28/2025 9:28 AM

APR/MAY-2025 Payment Schedule

Dear **amein[redacted]**

We are pleased to inform you that the payment for your outstanding invoices has been processed and the funds have been transferred to your account.

Please find the payment details below for your reference. Should you have any questions or require further information, feel free to contact us..

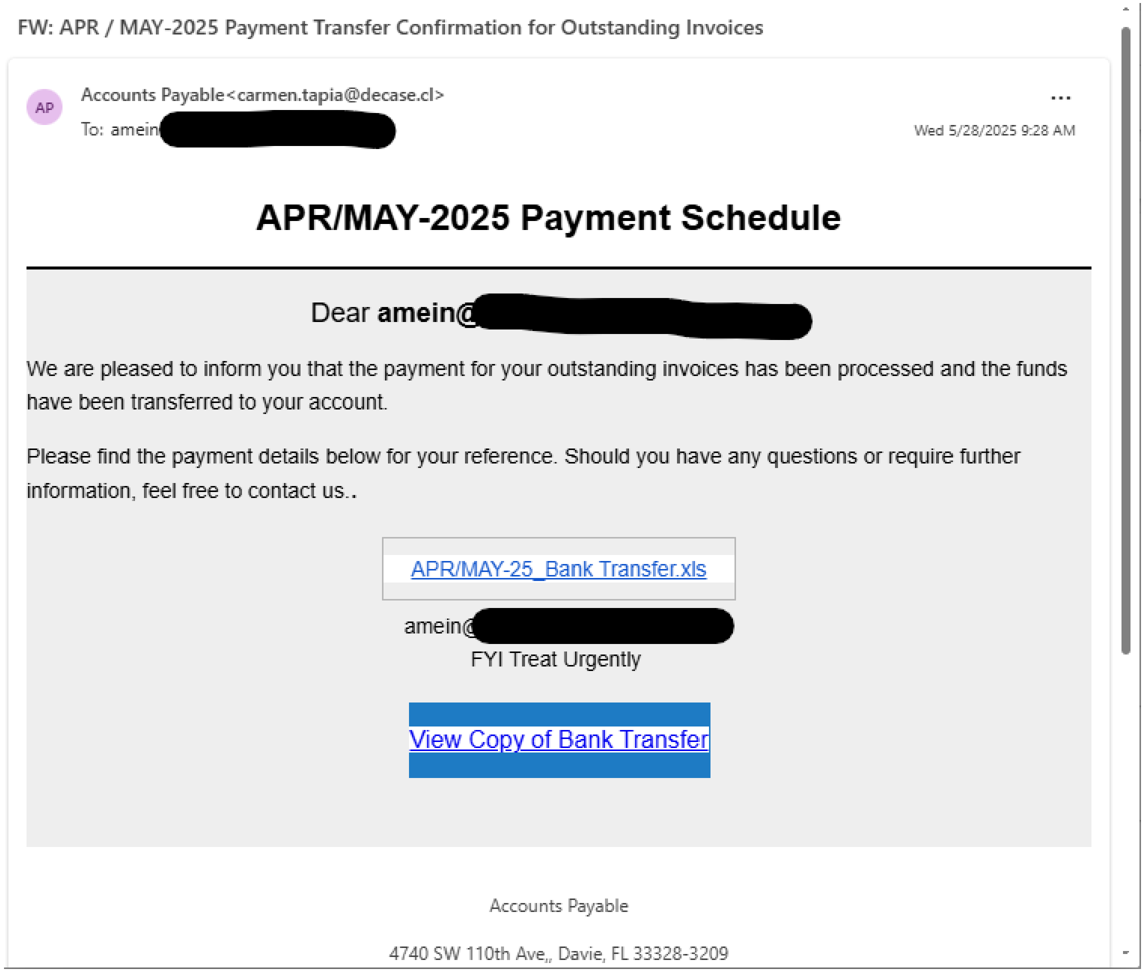
APR/MAY-25_Bank Transfer.xls

amein[redacted]

FYI Treat Urgently

Accounts Payable

Phishing! (From address is a random fake domain, the links are click bait)



FW: APR / MAY-2025 Payment Transfer Confirmation for Outstanding Invoices

Accounts Payable<carmen.tapia@decase.cl>

To: amein[redacted]

Wed 5/28/2025 9:28 AM

APR/MAY-2025 Payment Schedule

Dear **amein@**[redacted]

We are pleased to inform you that the payment for your outstanding invoices has been processed and the funds have been transferred to your account.

Please find the payment details below for your reference. Should you have any questions or require further information, feel free to contact us..

APR/MAY-25_Bank Transfer.xls

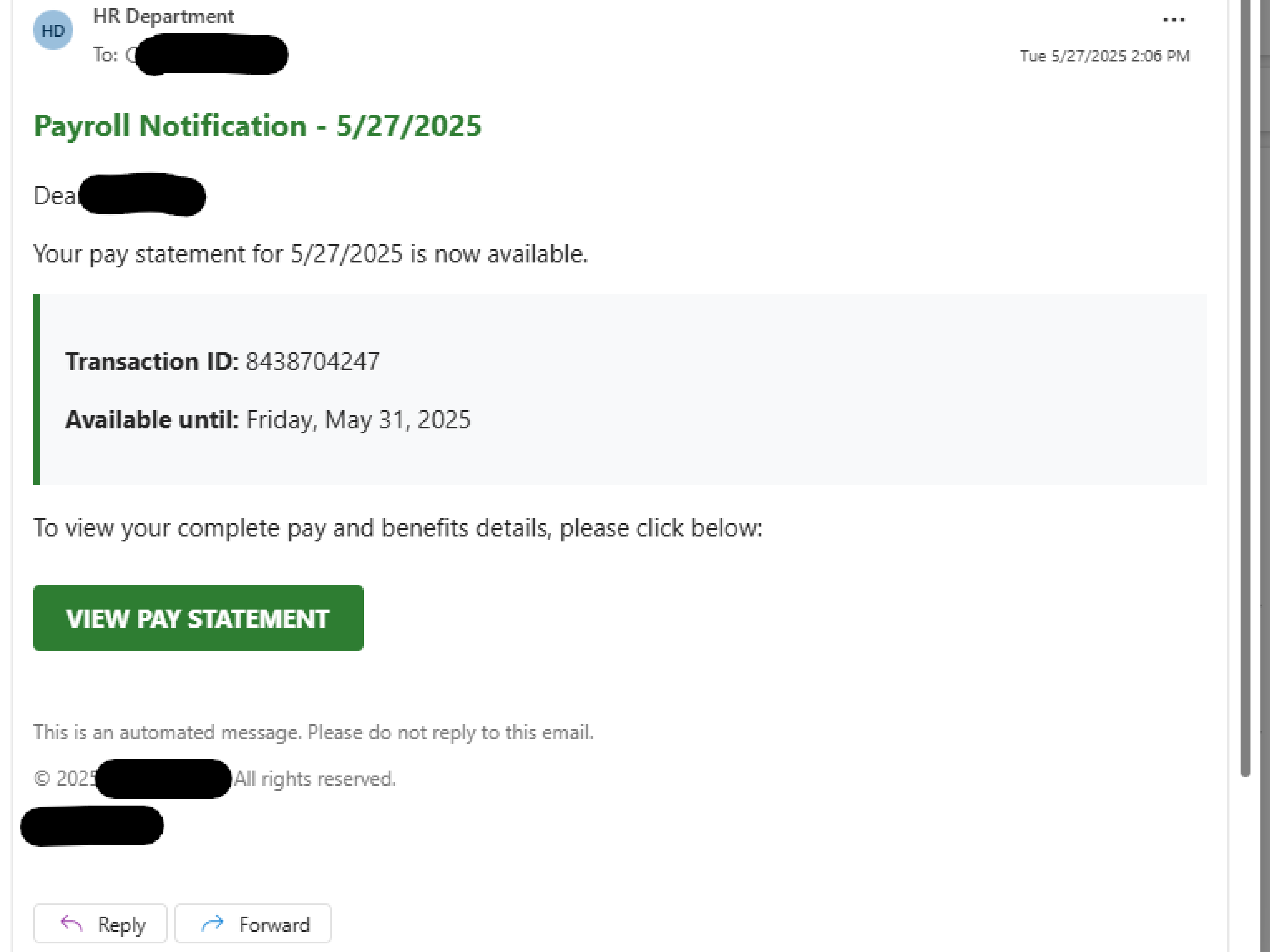
amein@[redacted]

FYI Treat Urgently

View Copy of Bank Transfer

Accounts Payable

4740 SW 110th Ave,, Davie, FL 33328-3209



HR Department

To: [redacted]

Tue 5/27/2025 2:06 PM

Payroll Notification - 5/27/2025

Dea[redacted]

Your pay statement for 5/27/2025 is now available.

> **Transaction ID:** 8438704247
>
> **Available until:** Friday, May 31, 2025

To view your complete pay and benefits details, please click below:

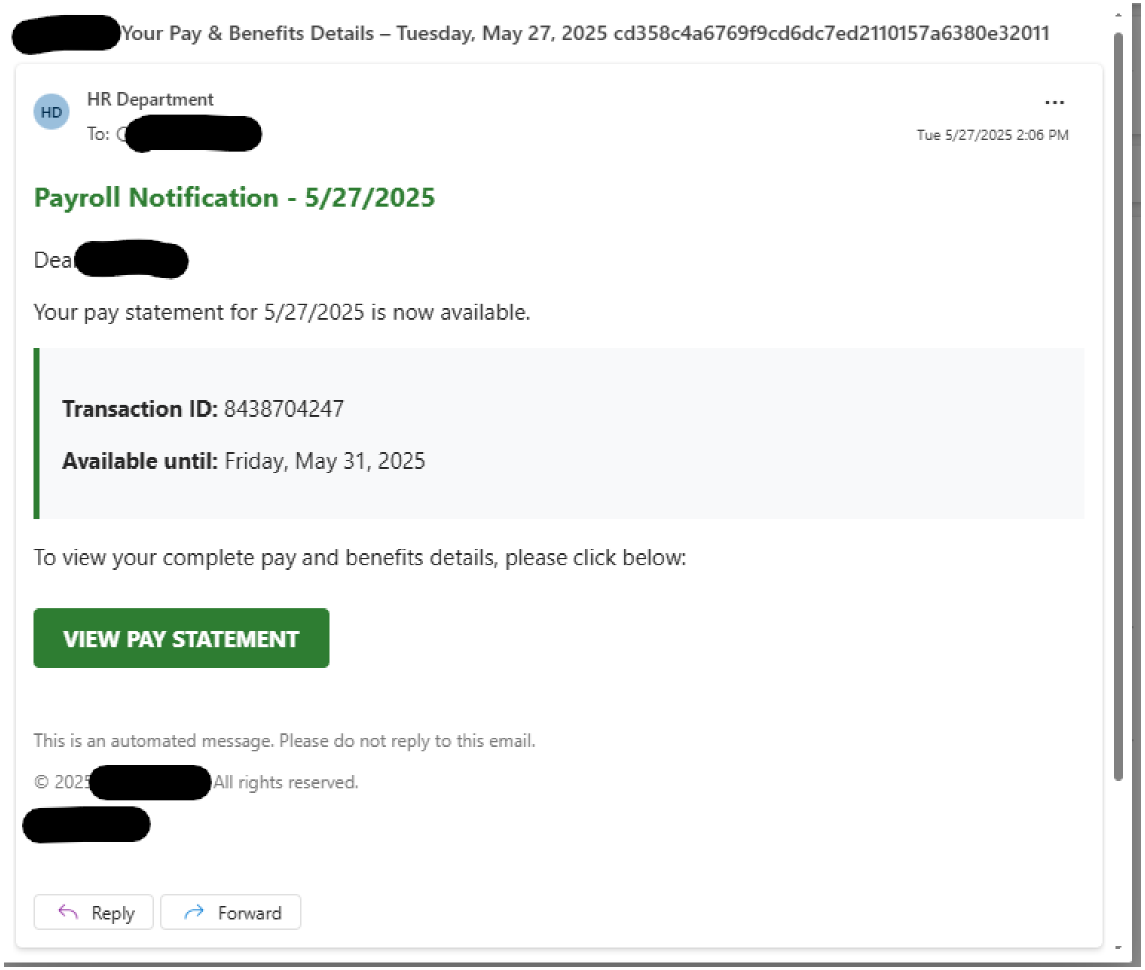
This is an automated message. Please do not reply to this email.

© 202[redacted]All rights reserved.

[redacted]

Phishing!

(This is not the way this company would normally receive these types of updates, always confirm with management)



[redacted] Your Pay & Benefits Details – Tuesday, May 27, 2025 cd358c4a6769f9cd6dc7ed2110157a6380e32011

HR Department
To: [redacted]

Tue 5/27/2025 2:06 PM

Payroll Notification - 5/27/2025

Dea[redacted]

Your pay statement for 5/27/2025 is now available.

Transaction ID: 8438704247

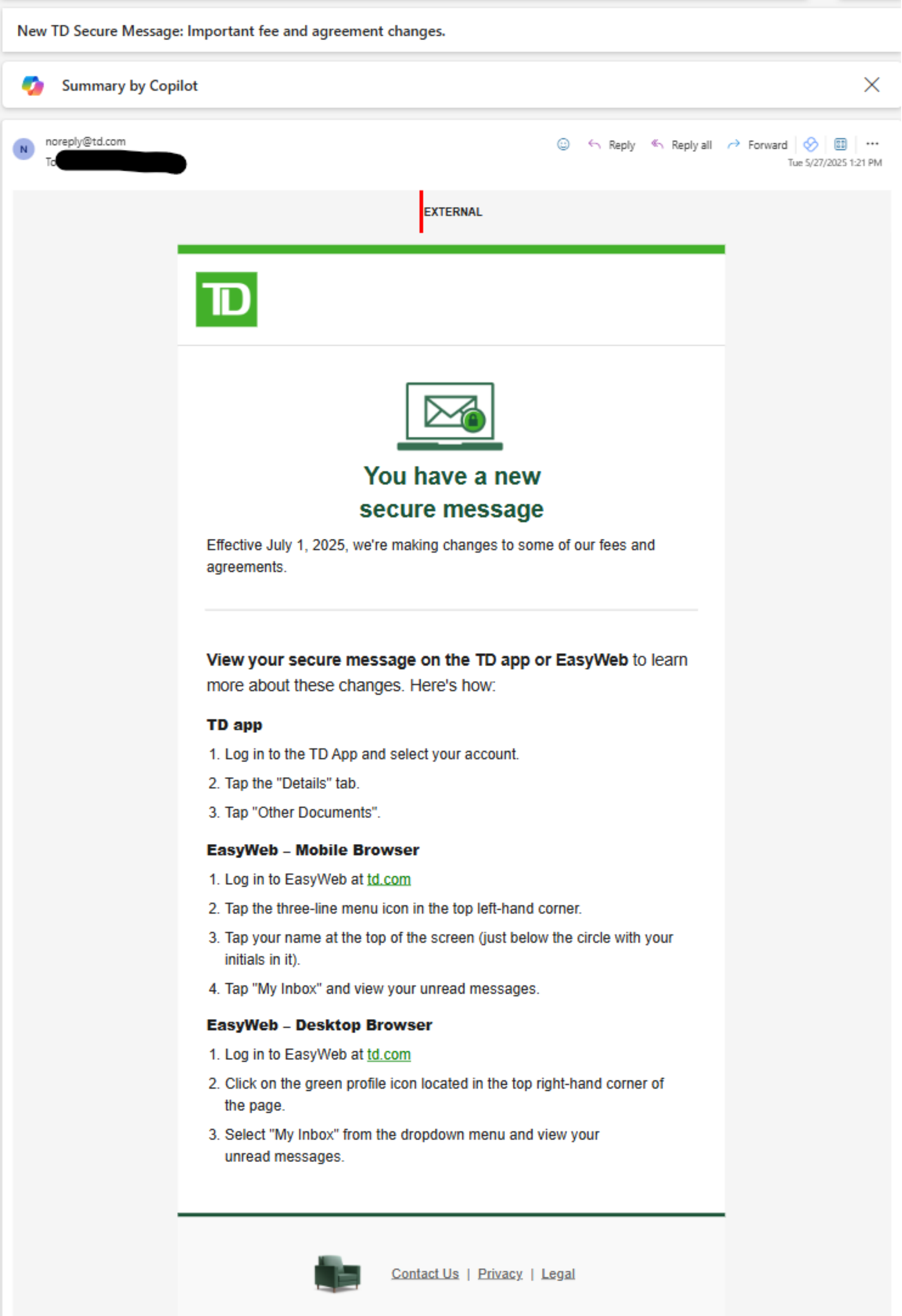
Available until: Friday, May 31, 2025

To view your complete pay and benefits details, please click below:

This is an automated message. Please do not reply to this email.

© 2025[redacted] All rights reserved.

[redacted]



New TD Secure Message: Important fee and agreement changes.

noreply@td.com
To [redacted]

Tue 5/27/2025 1:21 PM

EXTERNAL

TD

You have a new secure message

Effective July 1, 2025, we're making changes to some of our fees and agreements.

View your secure message on the TD app or EasyWeb to learn more about these changes. Here's how:

TD app

1. Log in to the TD App and select your account.
2. Tap the "Details" tab.
3. Tap "Other Documents".

EasyWeb – Mobile Browser

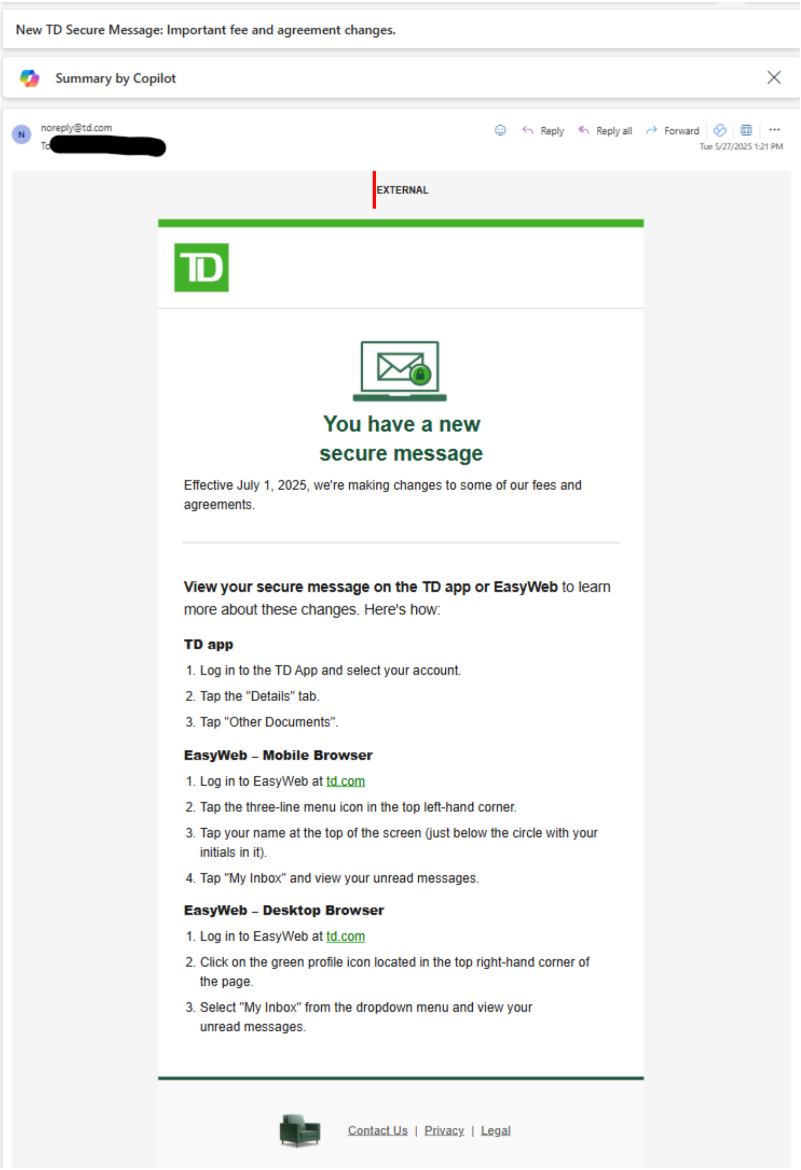
1. Log in to EasyWeb at td.com
2. Tap the three-line menu icon in the top left-hand corner.
3. Tap your name at the top of the screen (just below the circle with your initials in it).
4. Tap "My Inbox" and view your unread messages.

EasyWeb – Desktop Browser

1. Log in to EasyWeb at td.com
2. Click on the green profile icon located in the top right-hand corner of the page.
3. Select "My Inbox" from the dropdown menu and view your unread messages.

Contact Us | Privacy | Legal

Not Phishing!
(the from is from td.com and they are giving directions to login to their portal and only including links for convenience, but you should still hover over them to make sure they re not redirecting to somewhere malicious)



New TD Secure Message: Important fee and agreement changes.

noreply@td.com
To [redacted]

Tue 5/27/2025 1:21 PM

EXTERNAL

You have a new secure message

Effective July 1, 2025, we're making changes to some of our fees and agreements.

View your secure message on the TD app or EasyWeb to learn more about these changes. Here's how:

TD app

1. Log in to the TD App and select your account.
2. Tap the "Details" tab.
3. Tap "Other Documents".

EasyWeb – Mobile Browser

1. Log in to EasyWeb at td.com
2. Tap the three-line menu icon in the top left-hand corner.
3. Tap your name at the top of the screen (just below the circle with your initials in it).
4. Tap "My Inbox" and view your unread messages.

EasyWeb – Desktop Browser

1. Log in to EasyWeb at td.com
2. Click on the green profile icon located in the top right-hand corner of the page.
3. Select "My Inbox" from the dropdown menu and view your unread messages.

Contact Us | Privacy | Legal

Cyber Hygiene in Caregiving

- Cyber Hygiene Comparisons
- Outbreak Examples with parallels demonstrated

1. Passwords and Toothbrushes (Protecting Credentials and Authentication Data)

Cyber Hygiene

Passwords shouldn’t be shared, reused or left exposed. They are personal and if shared, can lead to cyber vulnerabilities.

Personal Hygiene

You wouldn’t share your toothbrush with others due to the germs and potential for illness. You also don't use the same toothbrush forever...

CIS CSC v8 Controls:

5 - Account Management

2. Security Practices and Physical Exercise (Maintaining System and Network Health)

Cyber Hygiene

Adopting and maintaining regular cybersecurity practices, such as updating systems, reviewing logs, or running vulnerability scans, strengthens the security posture of an organization, making it more resilient against potential cyber threats.

Personal Hygiene

Engaging in regular physical exercise strengthens the body, increases stamina, and boosts overall health, helping to ward off many diseases.

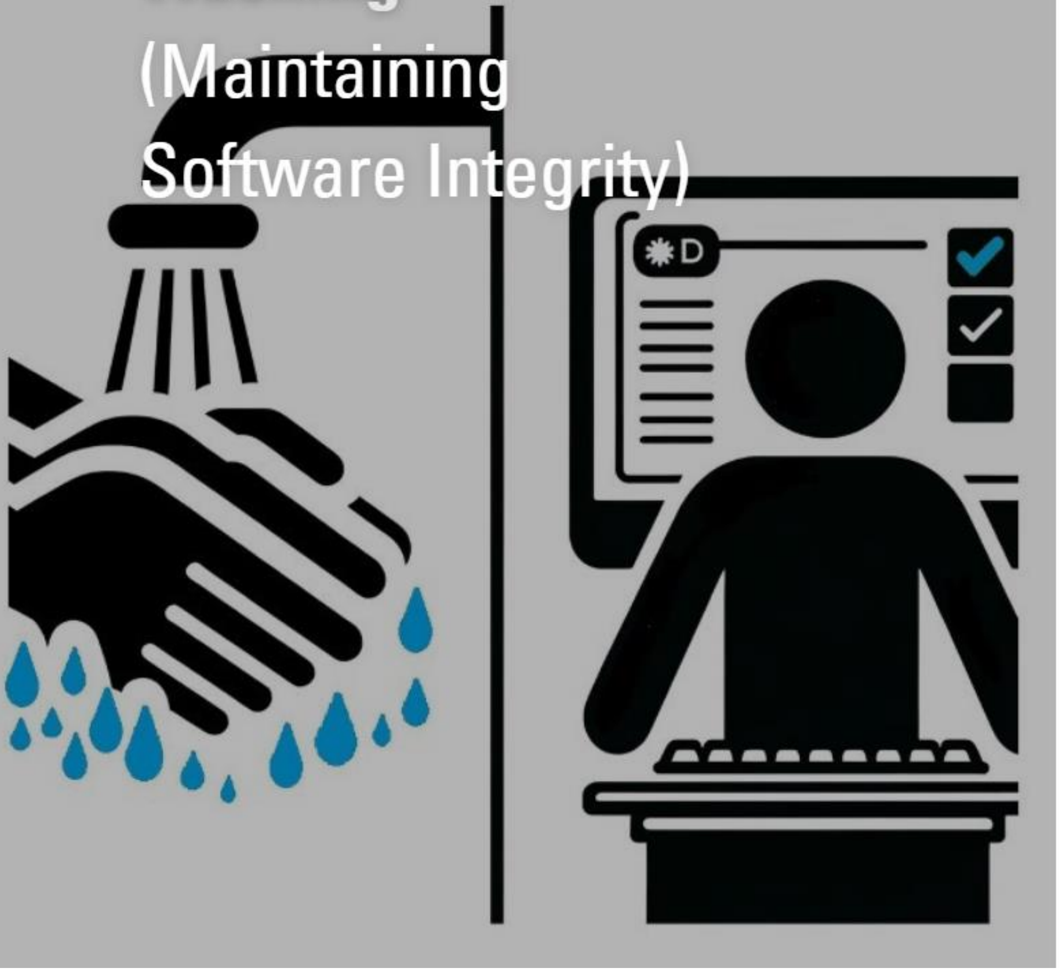
CIS CSC v8 Controls:

1 - Inventory and Control of Enterprise Assets

2 - Inventory and Control of Software Assets

15 - Service Provider Management

3. Software Updating and Hand Washing (Maintaining Software Integrity)



Cyber Hygiene

Regularly updating software ensures that known vulnerabilities are patched, preventing cyber infections.

Personal Hygiene

Regularly washing your hands can help prevent the spread of diseases.

CIS CSC v8 Controls:

7 - Continuous Vulnerability Management

12 - Network Infrastructure Management

4. Antivirus and Hand Sanitizers (Detecting and Neutralizing Threats)

Cyber Hygiene

Antivirus & EDR (Endpoint Detection & Response) programs detect and neutralize threats, providing a secondary layer of defense when other measures might fail.

Personal Hygiene

Hand sanitizers kill bacteria and viruses when soap and water aren’t available.

CIS CSC v8 Controls:

10 - Malware Defenses

5. Phishing and Junk Food (Avoiding DeceptiveThreats)

Cyber Hygiene

One should be wary of web popups & phishing emails that look legitimate but can harm our digital environment.

Personal Hygiene

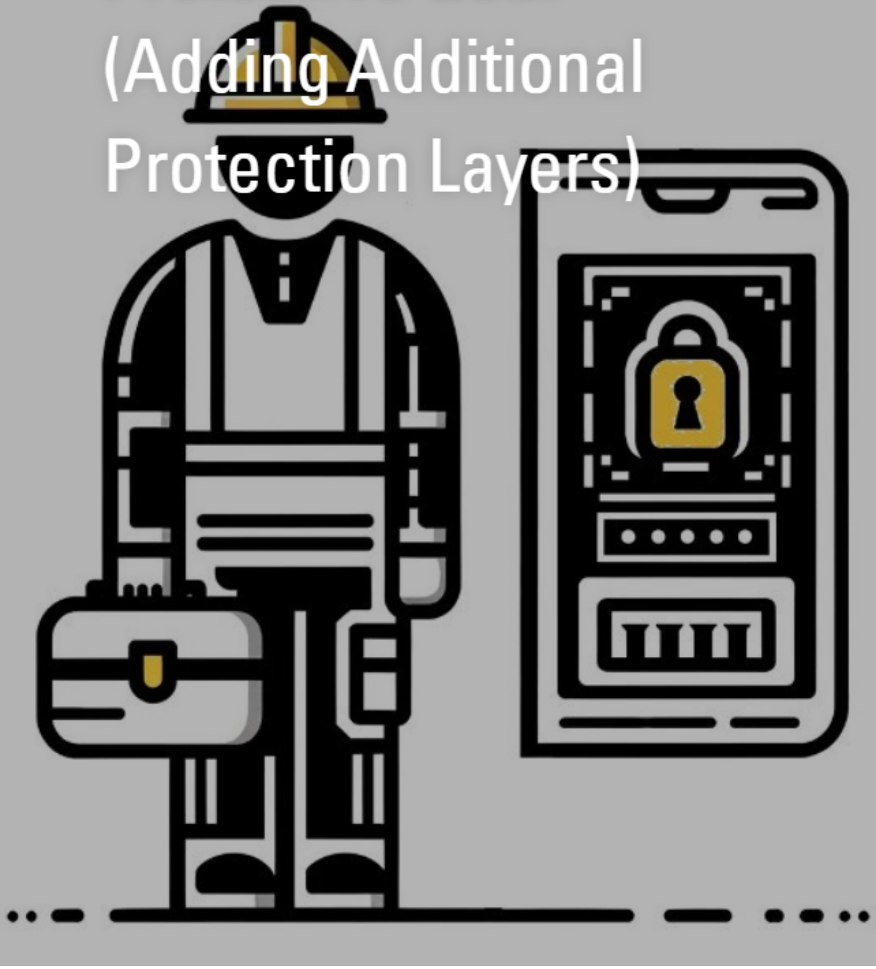
Just like we avoid junk food which might seem tempting but is bad for health.

CIS CSC v8 Controls:

9 - Email and Web Browser Protections

6. Multifactor Authentication and Protective Gear

(Adding Additional Protection Layers)



Cyber Hygiene

Multifactor authentication is an extra layer of protection, ensuring that even if a password is compromised, there’s another barrier in place.

Personal Hygiene

When doing risky tasks, we wear protective gear like helmets and pads.

CIS CSC v8 Controls:

6 - Access Control Management

7. Firewalls and Masks (Establishing Protective Barriers)

Cyber Hygiene

Firewalls act as barriers, reducing harmful data or unauthorized users from entering a network.

Personal Hygiene

Wearing a mask can filter out harmful particles and protect from airborne diseases.

CIS CSC v8 Controls:

4 - Secure Configuration of Enterprise Assets and Software

13 - Network Monitoring & Defense

8. Regular Check-ups (Routine Monitoring and Analysis)

Cyber Hygiene

Regularly auditing and assessing IT environments can identify vulnerabilities before they are exploited.

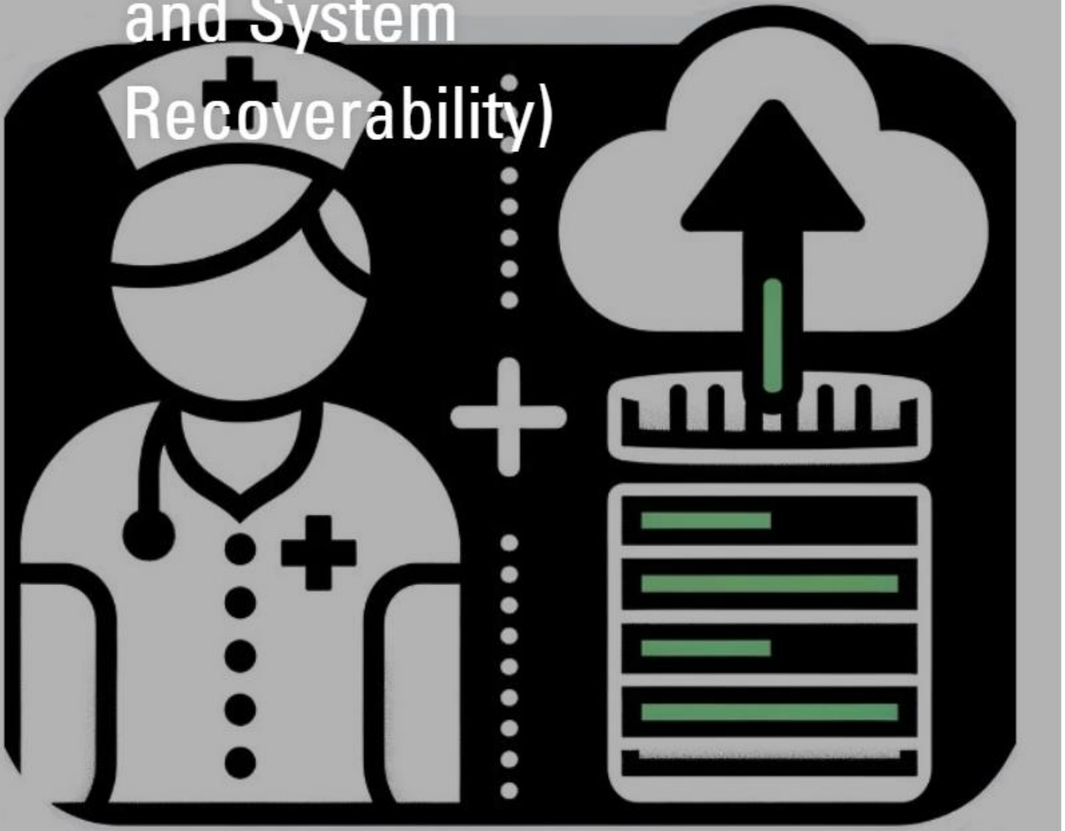
Personal Hygiene

Regular health check-ups catch potential issues early, ensuring they don't develop into more serious conditions.

CIS CSC v8 Controls:

8 - Audit Log Management

9. Backups and Vaccinations (Preventing Data Loss and System Recoverability)



Cyber Hygiene

Backing up data prepares companies to restore information if a cyberattack or data loss occurs.

Personal Hygiene

Vaccinations prepare your immune system to fight off diseases.

CIS CSC v8 Controls:

3 - Data Protection

11 - Data Recovery

10. Employee Training and Personal Health Education (Educating to Prevent Issues)

Cyber Hygiene

Regularly training employees about cyber threats and how to recognize and avoid them ensures they don't accidentally compromise security.

Personal Hygiene

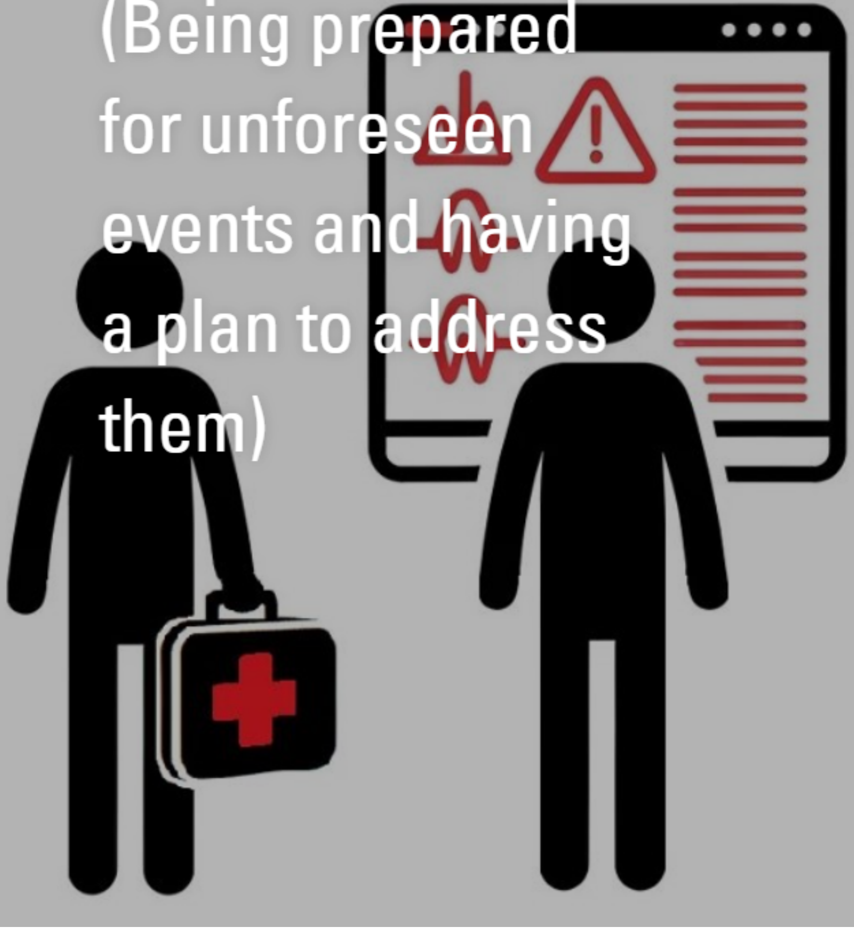
Educating individuals about health risks and how to maintain good health can reduce illnesses.

CIS CSC v8 Controls:

14 - Security Awareness and Skills Training

11. Emergency Responses and First Aid Kits

(Being prepared for unforeseen events and having a plan to address them)



Cyber Hygiene

Organizations prepare with incident response strategies, equipped with tools and protocols, to quickly address and learn from cyber incidents.

Personal Hygiene

Individuals keep first aid kits and emergency plans ready for unexpected physical mishaps, ensuring rapid response to injuries or threats.

CIS CSC v8 Controls:

17 - Incident Response Management

12. PenTesting and Blood Work (Uncover Hidden Threats) *IG2 Non Essential

Cyber Hygiene

While not classified as an Essential Control in the framework, penetration testing can uncover hidden vulnerabilities within an organization's systems, networks, and applications.

Personal Hygiene

Blood work can identify internal health issues that aren't always visible from the outside.

CIS CSC v8 Controls:

18 - Penetration Testing

Cyber Hygiene in Caregiving

- Cyber Hygiene Comparisons
- Outbreak Examples with parallels demonstrated

UnityPoint Health: Patient Zero

- Date: March 14, 2018

- A billing clerk opens a spoofed executive email (Patient Zero).

- Credentials harvested and phishing links sent to colleagues.

Clinical Analogy: Asymptomatic carrier introduces a virus.

UnityPoint Health: Spread & Delay

- Malware moves laterally through email systems, infecting staff.

- Detection delayed until May 31, 2018; 1.4M records exposed.

Analogy: Airborne pathogens spreading before detection.

UnityPoint Health: Containment

- Implemented two-factor authentication and email filters.

Analogy: Digital vaccination and masks to prevent reinfection.

Key Takeaway: Early training & MFA halt spread.

Source: UnityPoint Health agrees to $2.8M settlement in 2018 data breach case | Fierce Healthcare

UVM Health: Off-Site Exposure

- Date: October 2020

- On-call nurse opens compromised HOA email on vacation.

- Malware installed (TrickBot/BazarLoader) remains dormant.

Analogy: Clinician bringing home a contagious pathogen.

UVM Health: Epidemic & Lockdown

- VPN reconnection triggers ransomware outbreak.

- 1,300 servers & 600 apps disabled; procedures halted.

Analogy: ICU overwhelmed by critically ill patients.

UVM Health: Quarantine & Recovery

- Network lockdown as quarantine measure.

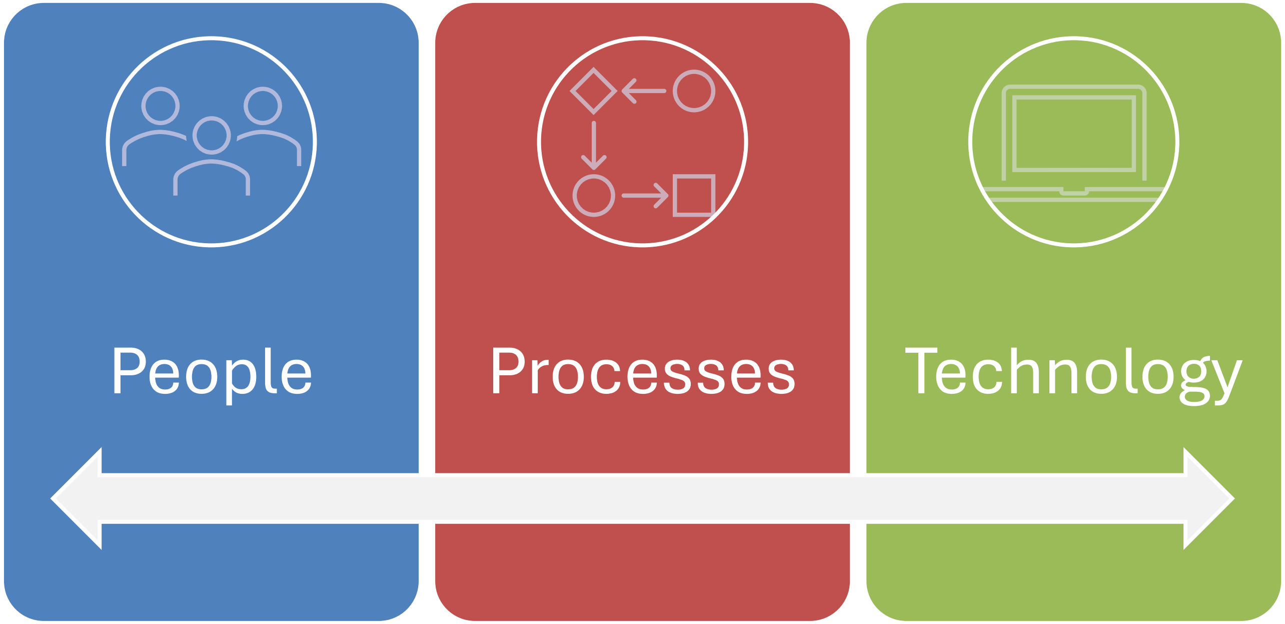
- Restored from backups without paying ransom.

Key Takeaway: Regular backups & segmentation for recovery.

Source: Statement from UVM Health Network on Cyberattack

“How secure am I?”

Cybersecurity is a team sport



People

Processes

Technology

People

Internal and external success factors

Help employees & leaders understand risks

- Continuous education

Create a cybersecurity culture

- Nominate an internal cyber leader
- Normalize incidents

Seek out third party expertise

- Skills shortage / expensive to staff internal
- Use to guide or augment approach
- Can include exercises

Processes

What does good process look like?

- Implement procedures – e.g. offboarding, privilege review
- Perform cyber framework assessments
- Mitigation of technical risks – vulnerability management
- Document actions taken & residual risk

Technology

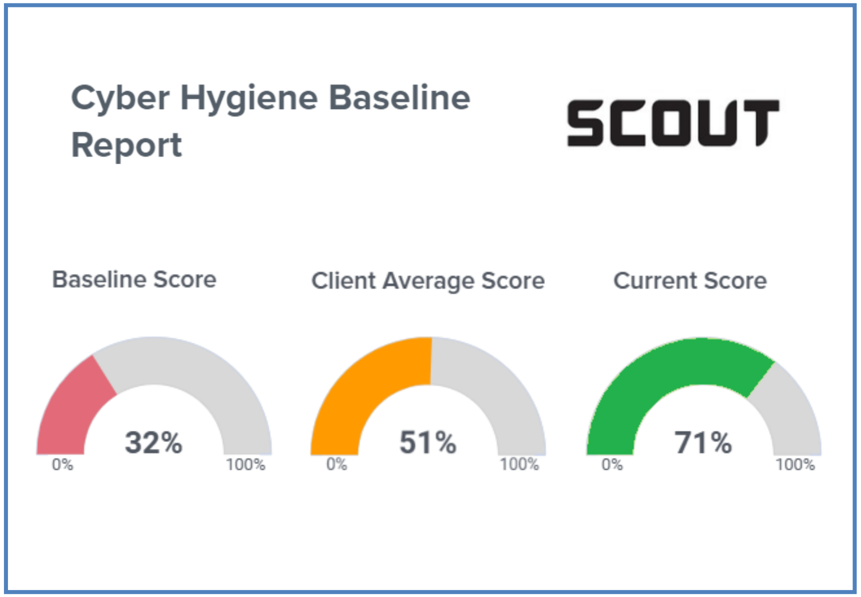
What does good cybersecurity look like?

- 24/7 risk management & monitoring
- Early detection & blocking of threats
- Integration with leading cloud services (M365, Google)
- Cyber Hygiene best practices

Complete visibility with Scout

24/7 Monitoring, Detection, and Response across your full IT environment.

Endpoints + **Network** + **Cloud**



Cyber Hygiene Baseline Report

SCOUT

Baseline Score 32%

Client Average Score 51%

Current Score 71%

Key Takeaways from the Workshop

- Enhanced understanding of password security.
- Improved identification of phishing threats.
- Increased awareness of cyber hygiene practices.
- Importance of multi-factor authentication.

Healthy Cyber Hygiene Top 10 Staff Action Sheet:

Keep your facility secure by treating cyber hygiene as everyone's responsibility—much like daily handwashing reduces infections. Follow these high-level practices that every team member can adopt to support IT and protect resident data.

1. **Use unique passwords**
   Like assigning each patient a unique ID bracelet to avoid mix-ups
2. **Use MFA with an authenticator app or token**
   Equivalent to requiring both ID badge and fingerprint ID for secure area access
3. **Think before you click – hover over links & avoid unexpected attachments**
   Similar to verifying a medication label before administration
4. **Report suspicious emails immediately to IT/security**
   Just as reporting a patient fall risk prevents further incidents
5. **Lock your screen when away – don't leave workstations open**
   Like closing and locking medicine cabinets when not in use
6. **Notify IT about update prompts or unusual pop-ups**
   Similar to informing maintenance when medical equipment displays error codes
7. **Use only approved channels for sharing sensitive data**
   Like using secure hospital pneumatic tubes rather than open corridors
8. **Close sensitive documents and clear clipboard after use**
   Analogous to sanitizing and returning medical instruments after procedures
9. **Speak up early – report odd behavior or login prompts**
   Just as alerting a supervisor at first sign of patient distress
10. **Know your incident response steps & practice the drill**
    Like participating in regular fire and code blue drills

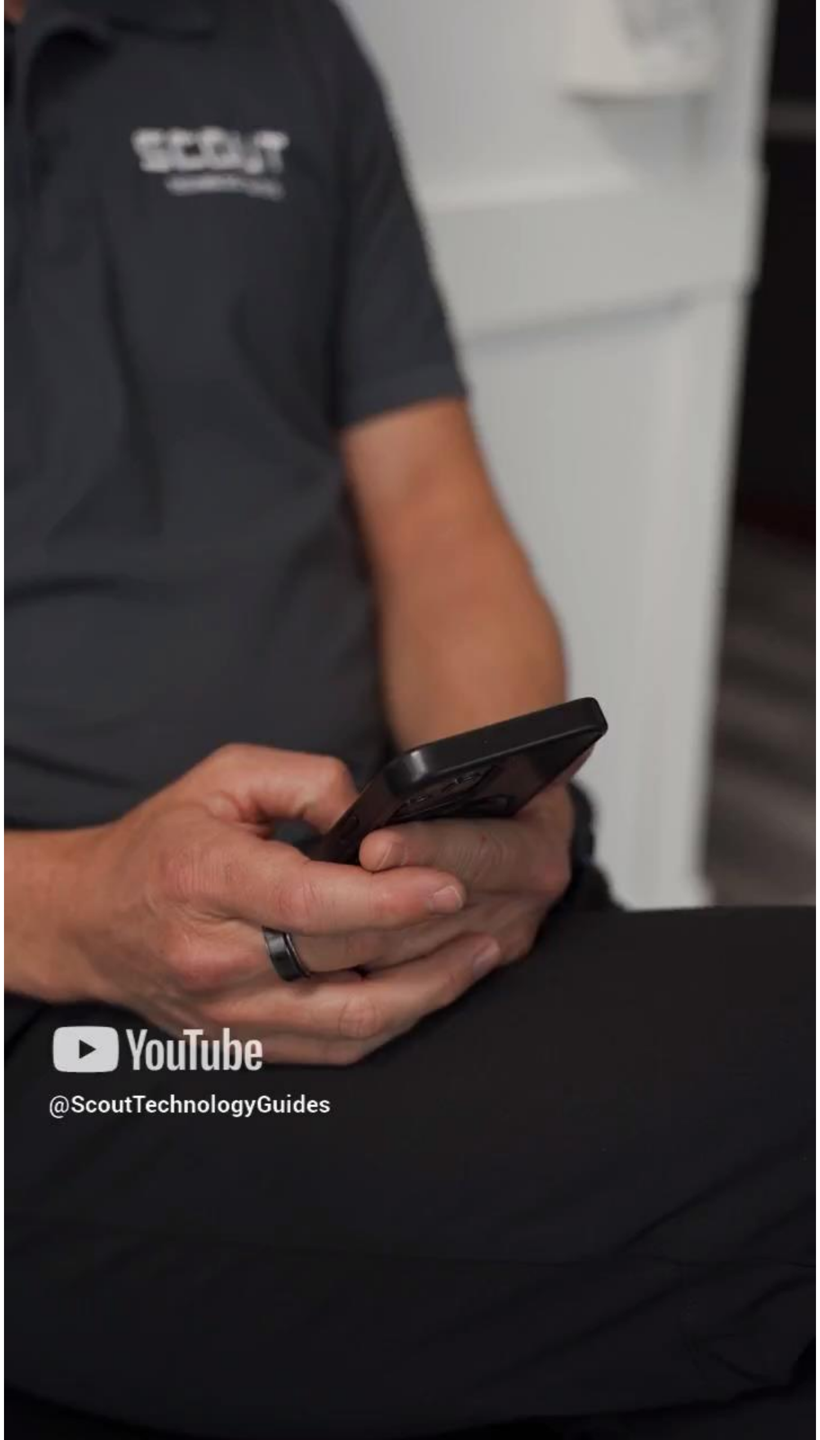
"Cyber hygiene is a team sport—small, consistent actions by all staff keep our data and residents safe."

Post this sheet at nurse stations and break rooms to remind everyone: everyday habits make a secure environment.

SCOUT
TECHNOLOGY GUIDES

Scout Cyber Hygiene Tip!

See them all: [Scout Technology Guides - YouTube]



SCOUT

TECHNOLOGY GUIDES

We’re on a mission to simplify cybersecurity!

Get your free cyber hygiene assessment here:
scouttg.com/services/cyber-hygiene-framework

Thank you for coming!

matt@scouttg.com

Q&A