AGENDA

BAY ARENAC BEHAVIORAL HEALTH
BOARD OF DIRECTORS
PROGRAM COMMITTEE MEETING

Thursday, September 12, 2024 at 5:00 pm
Room 225, Behavioral Health Center, 201 Mulholland Street, Bay City, MI 48708

Committee Members:	Present	Excused	Absent	Committee Members:	Present	Excused	Absent	Others Present:
Chris Girard, Ch				Pam Schumacher				BABH: Heather Beson, Joelin Hahn, Chris Pinter, Pam Van Wormer, and Sara McRae
Sally Mrozinski, V Ch				Robert Pawlak, Ex Off				
Jerome Crete				Richard Byrne, Ex Off				
Toni Reese								Legend: M-Motion; S-Support; MA-Motion Adopted; AB-Abstained

	Agenda Item	Discussion	Motion/Action
1.	Call To Order & Roll Call		
2.	Public Input (Maximum of 3 Minutes)		
3.	Clinical Program Review 3.1) Arenac Center Services, P. Van Wormer		3.1) No action necessary
4.	Unfinished Business 4.1) None		
5.	New Business 5.1) Rose Adult Foster Care Home Update, C. Pinter 5.2) Advocacy Update, C. Pinter		5.1) No action necessary 5.2) No action necessary

AGENDA

BAY ARENAC BEHAVIORAL HEALTH
BOARD OF DIRECTORS
PROGRAM COMMITTEE MEETING

Thursday, September 12, 2024 at 5:00 pm
Room 225, Behavioral Health Center, 201 Mulholland Street, Bay City, MI 48708

	5.3) Phishing Education, S. McRae		5.3) No action necessary
6.	Adjournment	M - S -	pm MA

Email Security Training for Board members

September 2024

Topics Covered

- What is phishing
- Types of phishing attacks
- How to spot a phishing attack
- What to do if you receive a suspicious message
- What to do if you click on a phishing link or attachment
- Security best practices
- Phishing examples

What is phishing

- Phishing is a social engineering scam whereby intruders seek access to your personal information or passwords by posing as a legitimate business or organization with legitimate reason to request information
- Social Engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purpose
- Malware (short for malicious software) is software that is intended to damage or disable computer systems, gather sensitive information, gain access to private computer systems, or display unwanted advertising

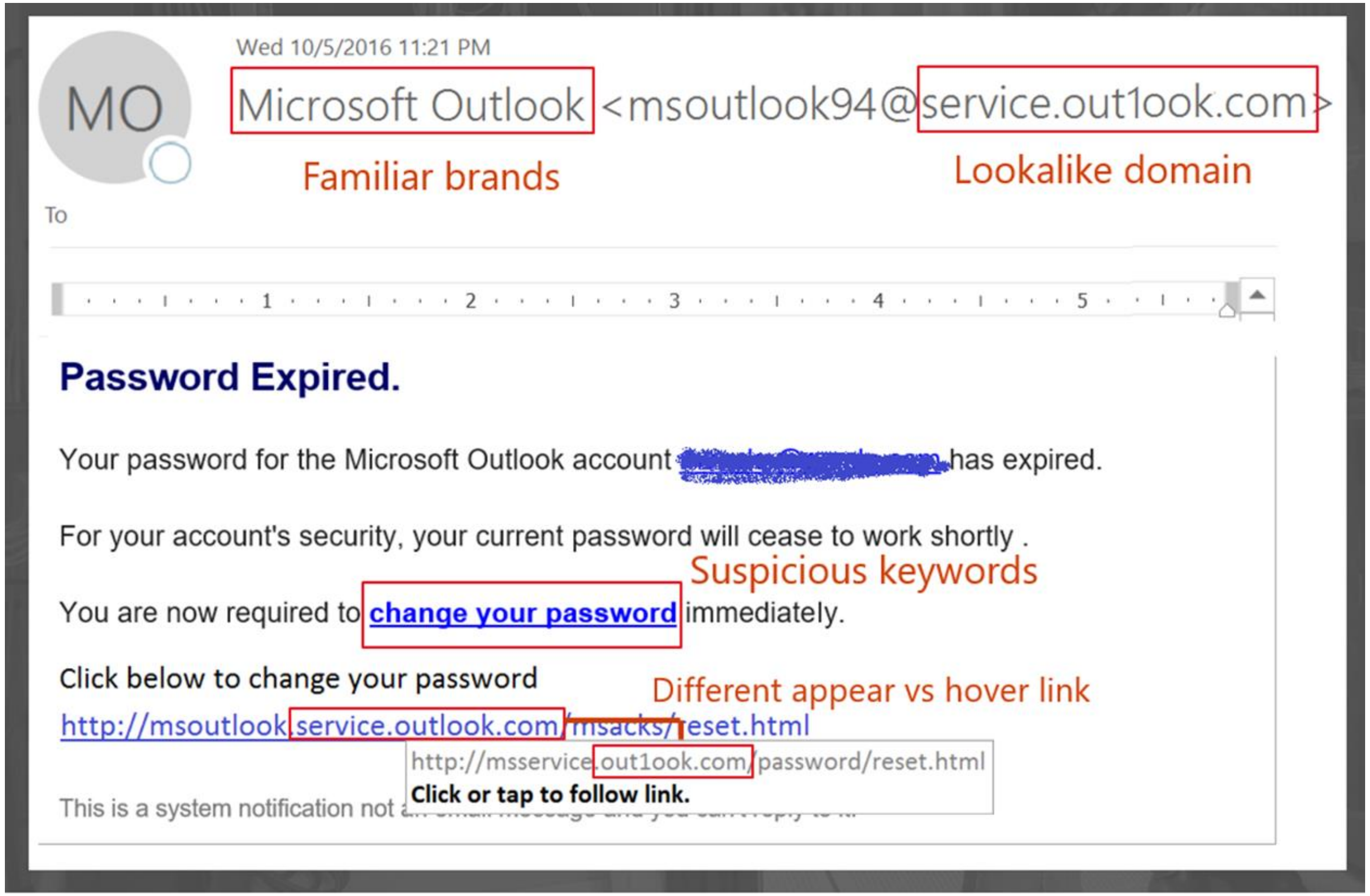
Types of phishing attacks

- Email phishing
  - An email is sent to trick people into revealing sensitive info or clicking on a link or attachment
- Smishing
  - Phishing that is delivered via a text message
- Vishing
  - Phishing that is delivered via a phone call
- Spear phishing
  - A targeted phishing attack that takes extra effort to customize it to the intended victim to appear more legitimate
- CEO fraud
  - Phishing attempt (via email, text, or phone) where the attacker impersonates the CEO or other higher ups to trick others into participating in a scam, such as sending money for a supposedly urgent expense

How to spot a phishing attack

- Watch out for messages that try to create a sense of urgency to gain something of value or to avoid a negative consequence
- Watch out for messages that come from generic senders, or from someone you don’t know
- Watch out for messages that appear to come from someone you know, but is out of character for them – they are likely being impersonated
- Watch out for messages with spelling, grammar, or formatting errors
- Watch out for messages with requests for personal information, login details, or asking for money
- Watch out for messages that request you to change your password or update an “expiring” account
- Watch out for links that display a different URL when you hover your mouse over them
- Remember to slow down and ask yourself “is this email legitimate”? Often, something will feel “off” about a phishing attempt

Phishing examples



MO

Wed 10/5/2016 11:21 PM

Microsoft Outlook <msoutlook94@service.out1ook.com>

Familiar brands

Lookalike domain

To

Password Expired.

Your password for the Microsoft Outlook account [redacted] has expired.

For your account's security, your current password will cease to work shortly .

Suspicious keywords

You are now required to change your password immediately.

Click below to change your password

Different appear vs hover link

http://msoutlook.service.outlook.com/msacks/reset.html

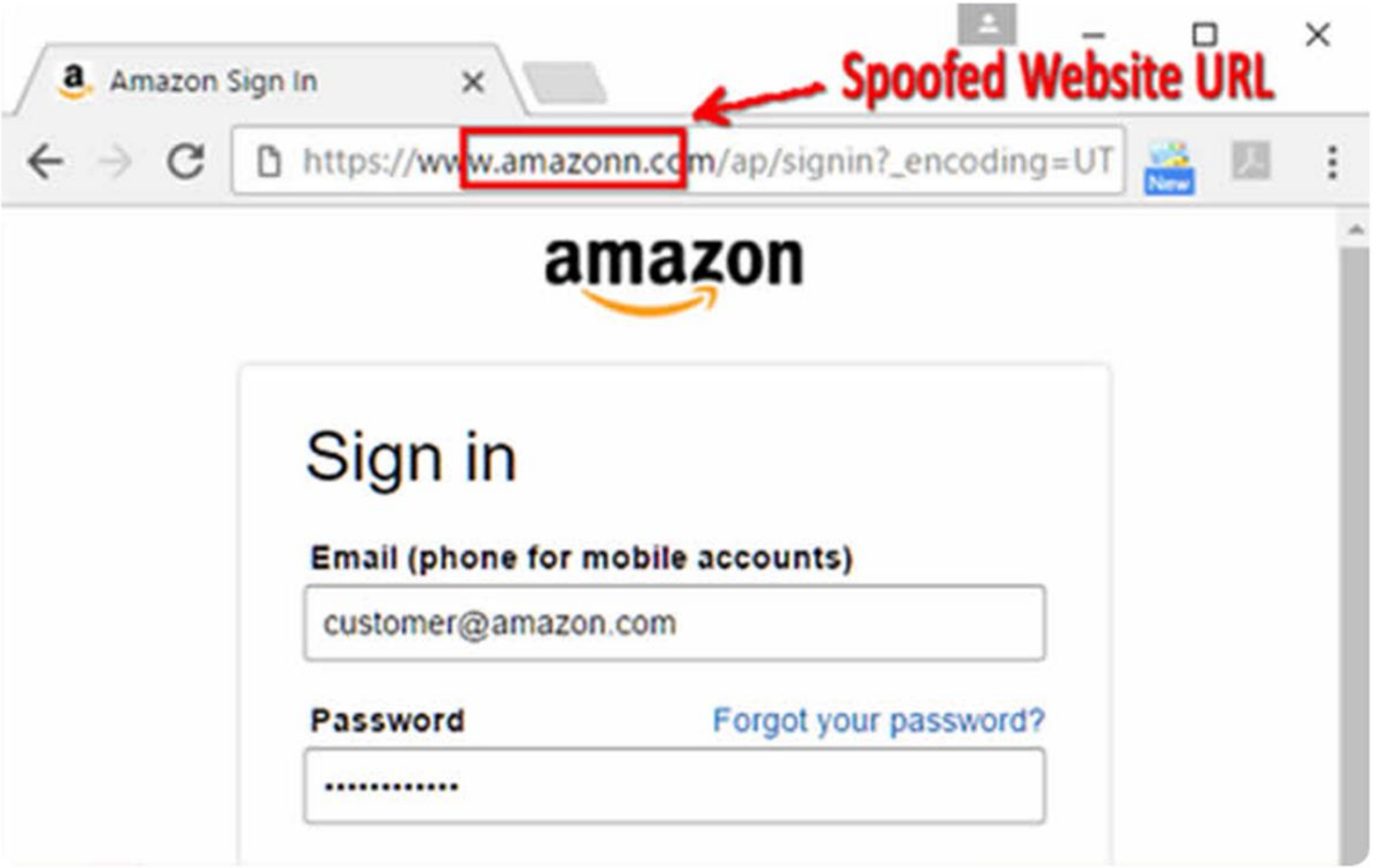
http://msservice.out1ook.com/password/reset.html
Click or tap to follow link.

This is a system notification not a

The lookalike domain is particularly notable here. They tried to pass off service.out1ook.com as if it were service.outlook.com

Often a subtle misspelling will go unnoticed.

Here we have another example of a misspelled URL being presented as the real deal. The extra n in amazon could easily be overlooked.



Sign in

Email (phone for mobile accounts)

customer@amazon.com

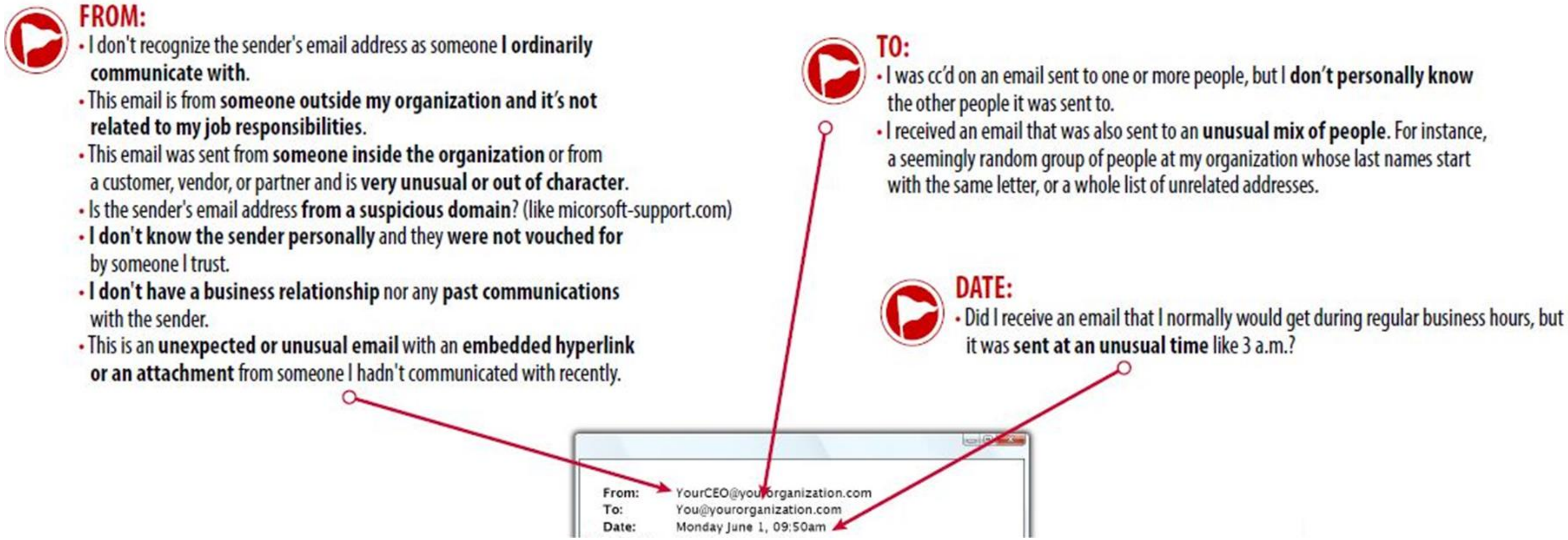
Password

Forgot your password?

·············

In this example, some important red flags to call out are:

- Emails sent at an unusual time, such as 3:00 am
- Emails sent to an unusual group of people



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 hadn't communicated with recently.

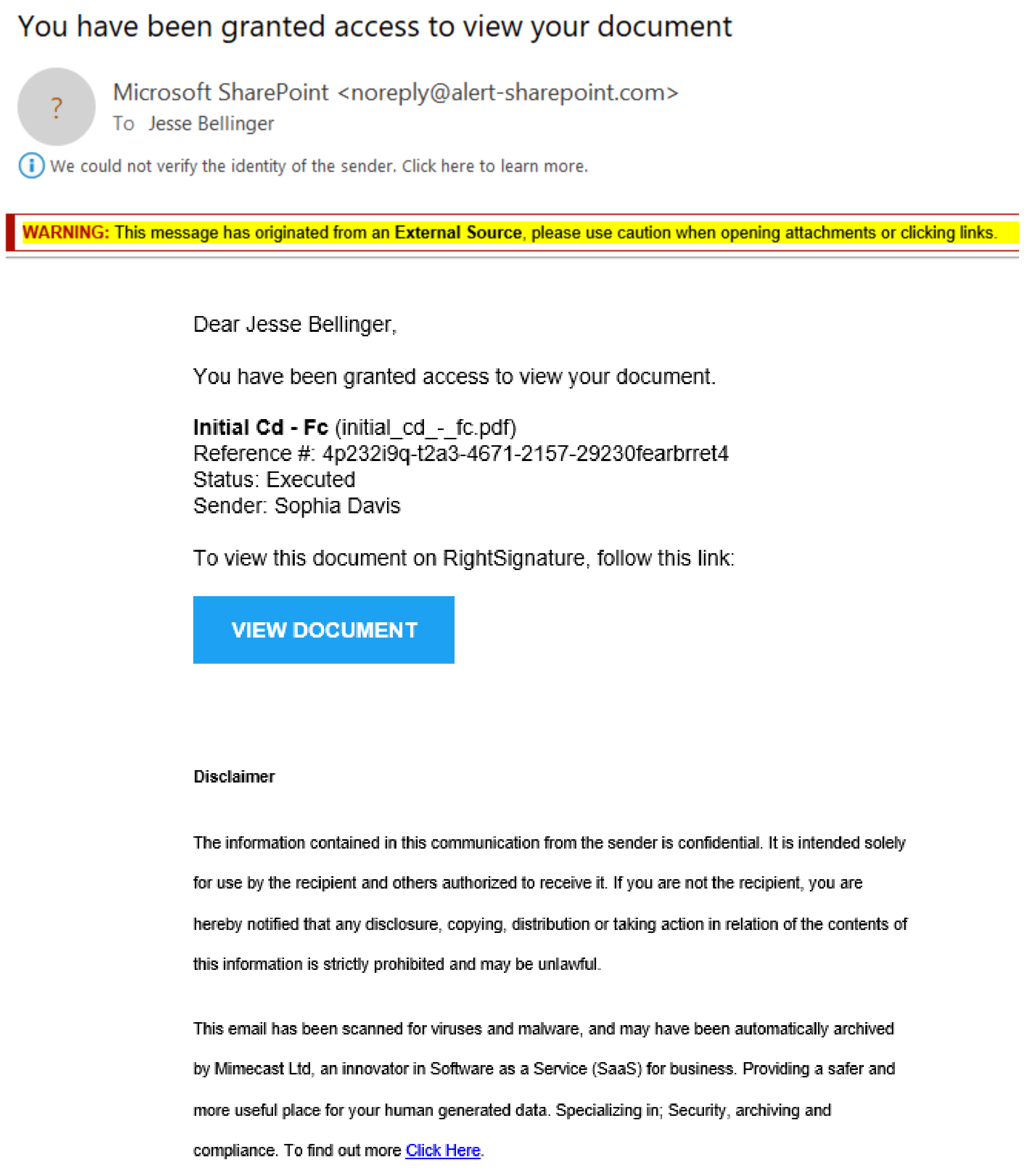
TO:

- 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, a seemingly random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

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.?

From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday June 1, 09:50am



You have been granted access to view your document

Microsoft SharePoint <noreply@alert-sharepoint.com>
To Jesse Bellinger

We could not verify the identity of the sender. Click here to learn more.

WARNING: This message has originated from an **External Source**, please use caution when opening attachments or clicking links.

Dear Jesse Bellinger,

You have been granted access to view your document.

Initial Cd - Fc (initial_cd_-_fc.pdf)
Reference #: 4p232i9q-t2a3-4671-2157-29230fearbrret4
Status: Executed
Sender: Sophia Davis

To view this document on RightSignature, follow this link:

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

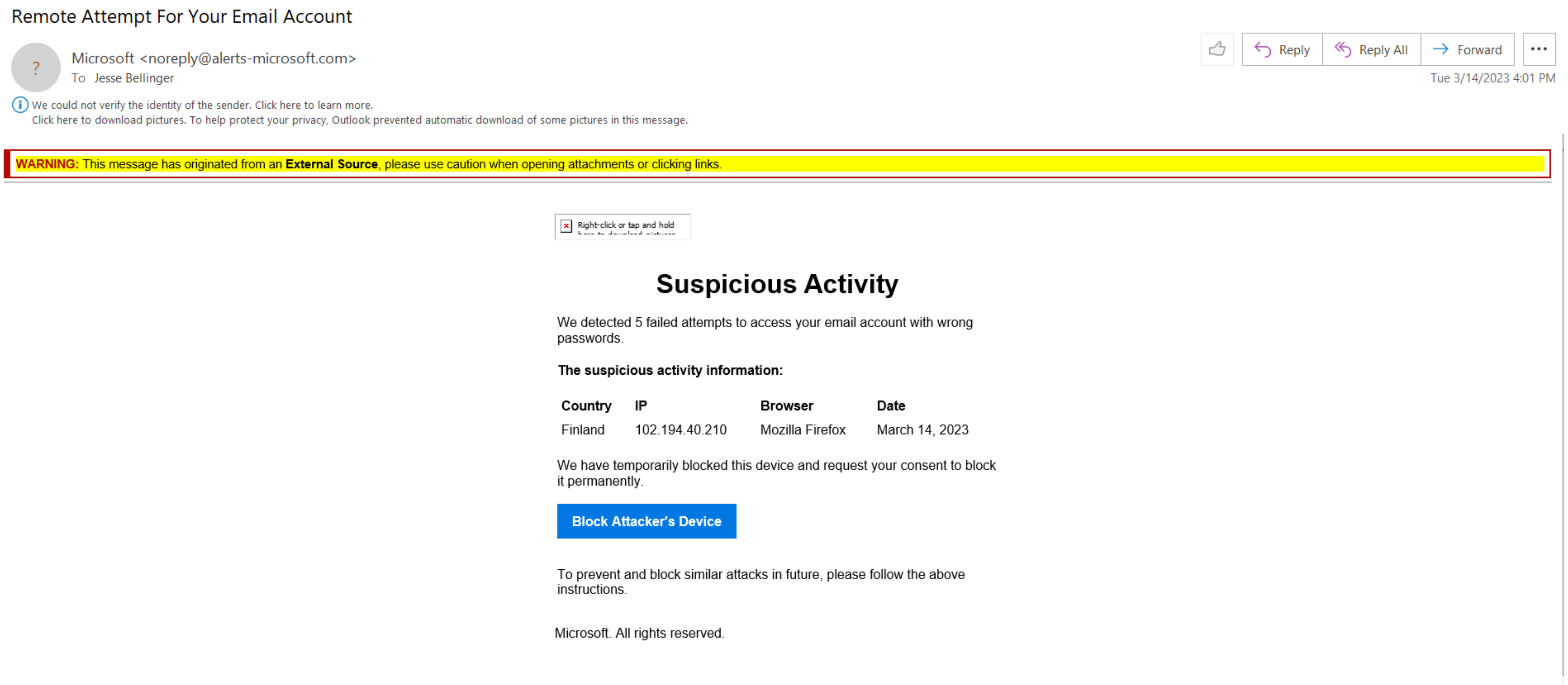
This email has been scanned for viruses and malware, and may have been automatically archived by Mimecast Ltd, an innovator in Software as a Service (SaaS) for business. Providing a safer and more useful place for your human generated data. Specializing in; Security, archiving and compliance. To find out more Click Here.

Here we have an example of a phish that tries to disguise itself as a document that needs to be signed.

Make sure that you only open documents from trusted sources and are currently expecting a document.

You can always reach out to the person directly with previously established contact details to confirm if the email is legitimate. Do not reply to the email or use contact info contained within the email to do this.

Especially important would be hovering over the link with your mouse and verifying the URL will take you to the location in which you would expect it to.



Remote Attempt For Your Email Account

Microsoft <noreply@alerts-microsoft.com>
To Jesse Bellinger

Tue 3/14/2023 4:01 PM

We could not verify the identity of the sender. Click here to learn more.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

WARNING: This message has originated from an **External Source**, please use caution when opening attachments or clicking links.

☒ Right-click or tap and hold

Suspicious Activity

We detected 5 failed attempts to access your email account with wrong passwords.

The suspicious activity information:

Country	IP	Browser	Date
Finland	102.194.40.210	Mozilla Firefox	March 14, 2023

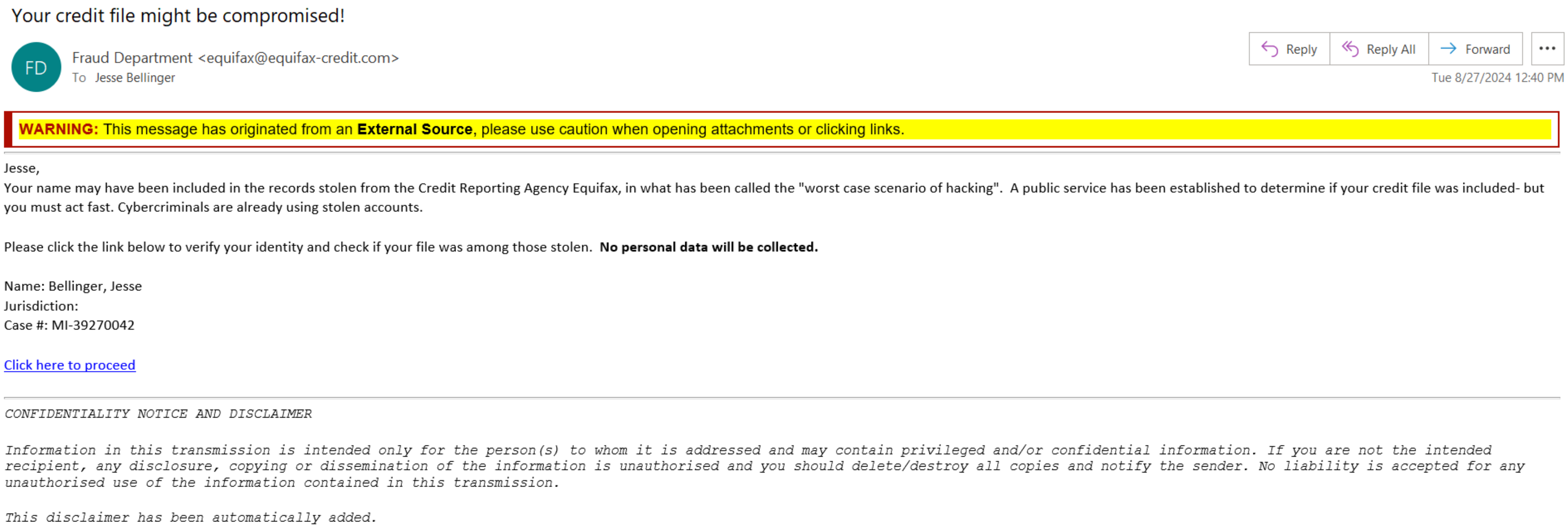
We have temporarily blocked this device and request your consent to block it permanently.

Block Attacker's Device

To prevent and block similar attacks in future, please follow the above instructions.

Microsoft. All rights reserved.

Here is a phish that attempts to trick you into thinking your account is under attack and provides a link to “block the attacker’s device” but is actually a link to capture your login details or to install malware on your system.



Your credit file might be compromised!

Fraud Department <equifax@equifax-credit.com>
To Jesse Bellinger

Tue 8/27/2024 12:40 PM

WARNING: This message has originated from an **External Source**, please use caution when opening attachments or clicking links.

Jesse,
Your name may have been included in the records stolen from the Credit Reporting Agency Equifax, in what has been called the "worst case scenario of hacking". A public service has been established to determine if your credit file was included- but you must act fast. Cybercriminals are already using stolen accounts.

Please click the link below to verify your identity and check if your file was among those stolen. **No personal data will be collected.**

Name: Bellinger, Jesse
Jurisdiction:
Case #: MI-39270042

Click here to proceed

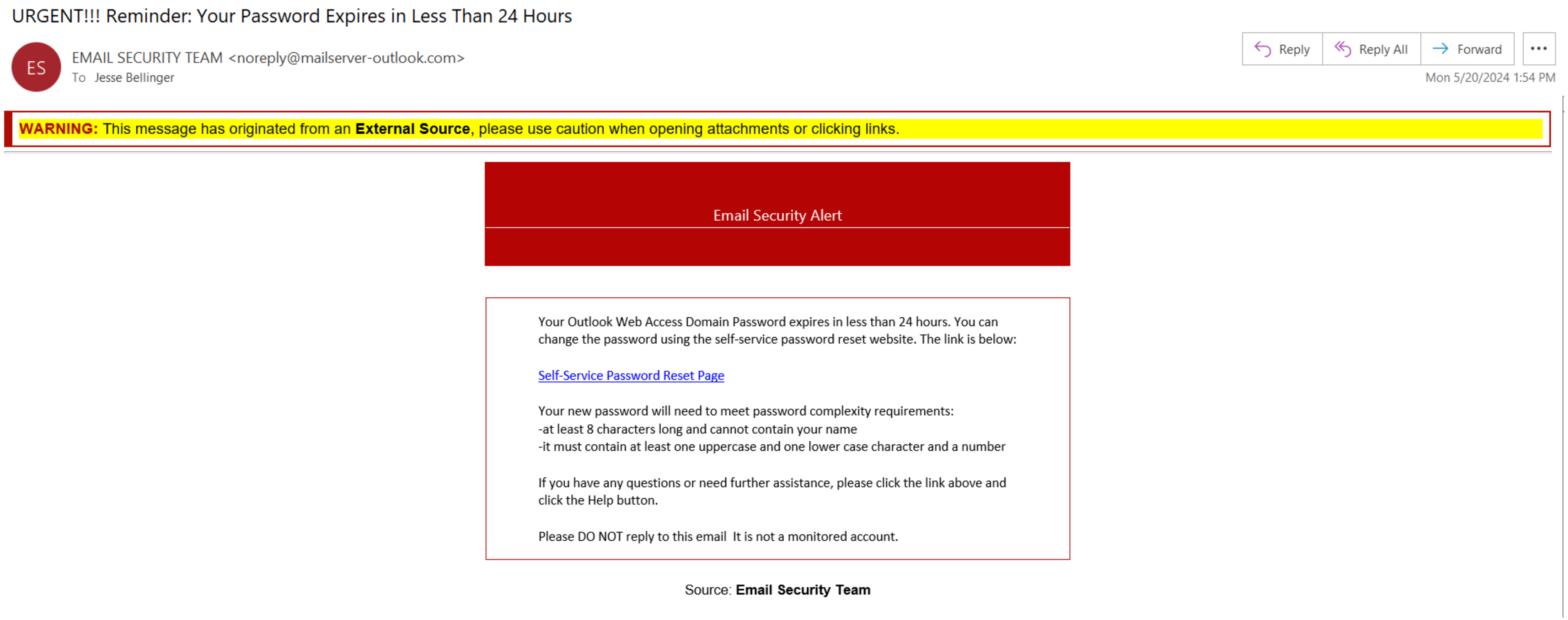
CONFIDENTIALITY NOTICE AND DISCLAIMER

Information in this transmission is intended only for the person(s) to whom it is addressed and may contain privileged and/or confidential information. If you are not the intended recipient, any disclosure, copying or dissemination of the information is unauthorised and you should delete/destroy all copies and notify the sender. No liability is accepted for any unauthorised use of the information contained in this transmission.

This disclaimer has been automatically added.

In this example the phish attempts to convince you this is from Equifax and that you need to click on the link to verify your identity and check if your identity was stolen.

Equifax will tell you to login to your account and check out their report, not click on a link in an email. Hovering over the link in the email above will reveal the URL will not take you to Equifax's website.



URGENT!!! Reminder: Your Password Expires in Less Than 24 Hours

ES EMAIL SECURITY TEAM <noreply@mailserver-outlook.com>
To Jesse Bellinger

Mon 5/20/2024 1:54 PM

WARNING: This message has originated from an **External Source**, please use caution when opening attachments or clicking links.

Email Security Alert

Your Outlook Web Access Domain Password expires in less than 24 hours. You can change the password using the self-service password reset website. The link is below:

Self-Service Password Reset Page

Your new password will need to meet password complexity requirements:
-at least 8 characters long and cannot contain your name
-it must contain at least one uppercase and one lower case character and a number

If you have any questions or need further assistance, please click the link above and click the Help button.

Please DO NOT reply to this email It is not a monitored account.

Source: **Email Security Team**

This example tries to convince you that your password is about to expire, and you need to click on the link to reset it. It will instead harvest your login details.

You will not receive emails about your password expiring, and you should always navigate directly to the system/website and change your password there, never from a link in an email.

If your password does expire, typically systems will just require you to change it the next time you login.

What to do if you receive a suspicious message

- Don’t click on any links or attachments
- Don’t respond to requests for personal information or login details
- Report the email if possible – how to do this will vary depending on what email service you use
- If you are unsure if the email might be legitimate, reach out to the person or company directly – not using a link or contact details contained in the message
- Delete the message

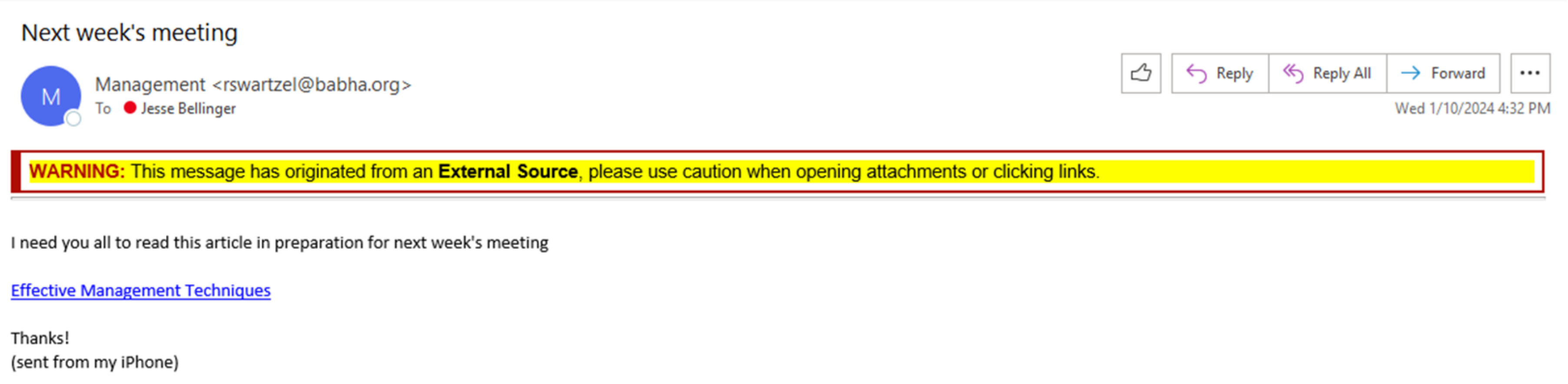
What to do if you click on a phishing link or attachment

- If this was on a work device, contact your IT department immediately
- Change your password, and remember to change any other passwords if you re-used that password somewhere else (it is a bad idea to re-use passwords)
- Scan your device for malware if possible
- Keep an eye out for suspicious activity

Security best practices

- Always follow the tips for how to spot a phishing attack and what to do if you receive a suspicious message
- Use a different, strong password for each account
  - 12+ characters, uppercase, lowercase, number, symbol, not a dictionary word, and not something easily found on social media like names of kids or pets
  - A password manager or note on your phone can help keep track of them
- Setup multifactor authentication on your accounts
  - Most services support this now; consider switching services if yours does not
  - MFA setup is usually found in "account", and "security"; although where to find the setting varies from service to service
  - MFA can usually text you a code or can use an authenticator app such as "Duo Mobile", "Microsoft Authenticator", or Google Authenticator".

Phishing examples continued



Next week's meeting

Management <rswartzel@babha.org>
To ● Jesse Bellinger

Wed 1/10/2024 4:32 PM

WARNING: This message has originated from an **External Source**, please use caution when opening attachments or clicking links.

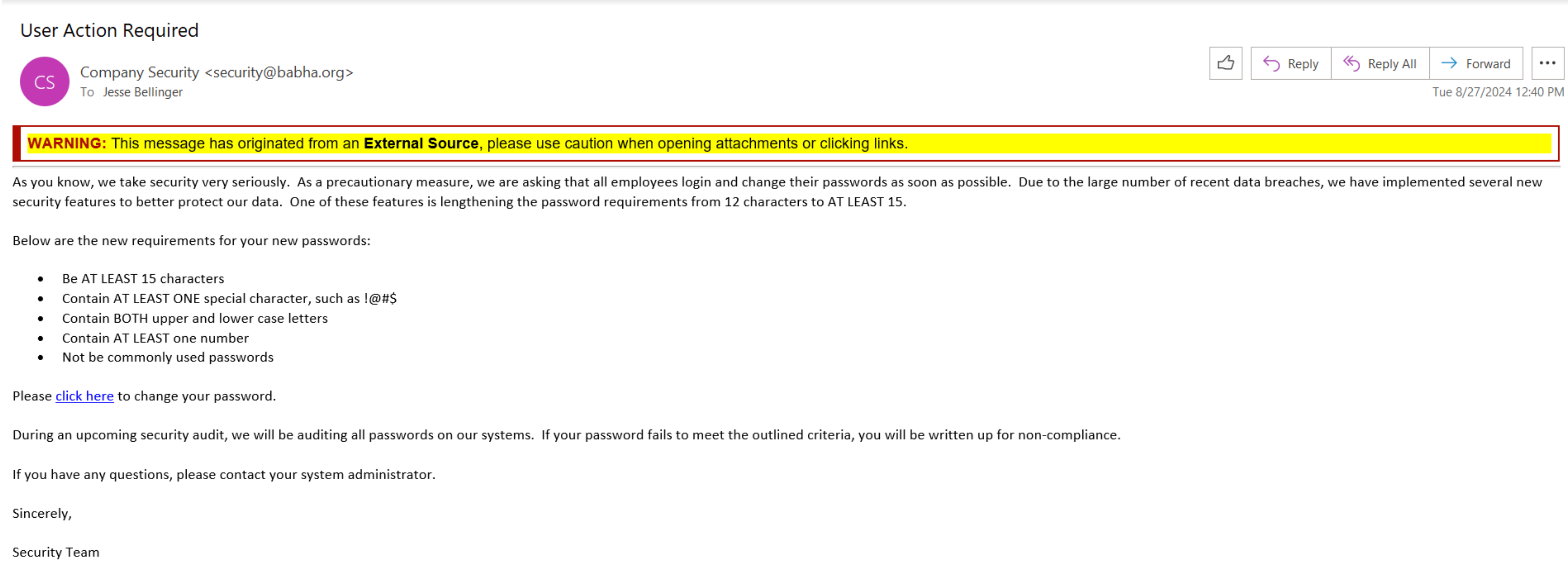
I need you all to read this article in preparation for next week's meeting

Effective Management Techniques

Thanks!
(sent from my iPhone)

Red flags:

- External source warning on an email from an internal address (this is only present on BABH email accounts and is a security feature on our system)
- Email is from a generic sender, and "spoofs" an email address
- Hovering your mouse over the link will reveal it will take you to an unknown/untrusted location
- The email tries to create a sense of urgency, and implies a negative consequence (a deadline given by management to complete a task)



User Action Required

Company Security <security@babha.org>
To Jesse Bellinger

Tue 8/27/2024 12:40 PM

WARNING: This message has originated from an **External Source**, please use caution when opening attachments or clicking links.

As you know, we take security very seriously. As a precautionary measure, we are asking that all employees login and change their passwords as soon as possible. Due to the large number of recent data breaches, we have implemented several new security features to better protect our data. One of these features is lengthening the password requirements from 12 characters to AT LEAST 15.

Below are the new requirements for your new passwords:

- Be AT LEAST 15 characters
- Contain AT LEAST ONE special character, such as !@#$
- Contain BOTH upper and lower case letters
- Contain AT LEAST one number
- Not be commonly used passwords

Please click here to change your password.

During an upcoming security audit, we will be auditing all passwords on our systems. If your password fails to meet the outlined criteria, you will be written up for non-compliance.

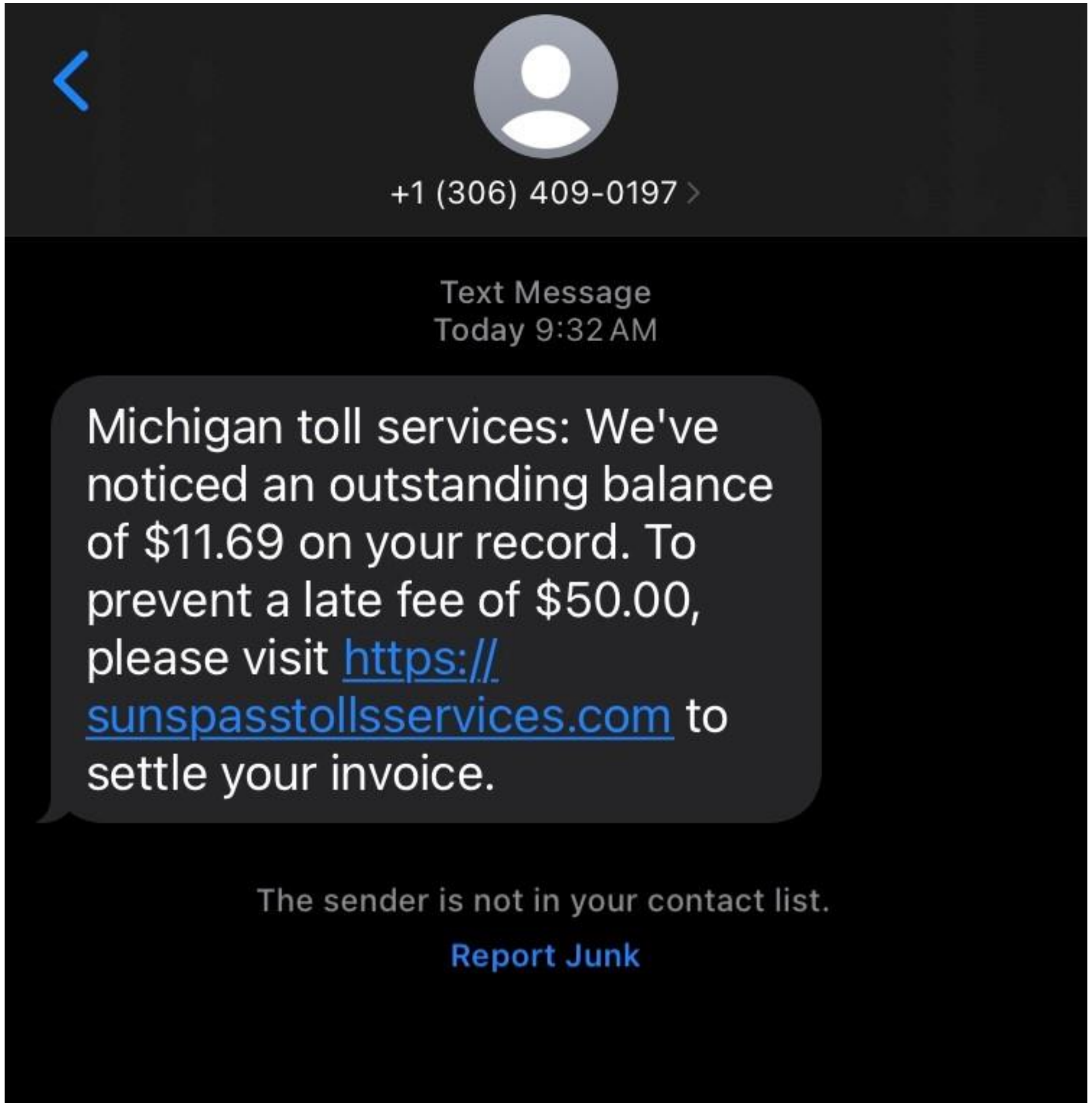
If you have any questions, please contact your system administrator.

Sincerely,

Security Team

Red Flags:

- External source banner (BABH emails only)
- Generic Sender
- Link that reveals it will take you to an unknown/untrusted location when hovering your mouse over it
- Email creates a sense of urgency to avoid a negative consequence. In this case entering your login details to avoid getting written up



Text Message
Today 9:32 AM

Michigan toll services: We've noticed an outstanding balance of $11.69 on your record. To prevent a late fee of $50.00, please visit https://sunspasstollsservices.com to settle your invoice.

The sender is not in your contact list.

This is a real SMISH

- The message impersonates a toll collection agency
- It creates a sense of urgency to avoid a consequence, in this case a late fee
- This is attempting to scam you out of $11.69, and potentially steal your payment information to run up more charges on your card later, or perhaps steal your identity

Thank you for reviewing this training!

If you have any questions, feel free to reach out to me

Jesse Bellinger

jbellinger@babha.org

989-497-1373