

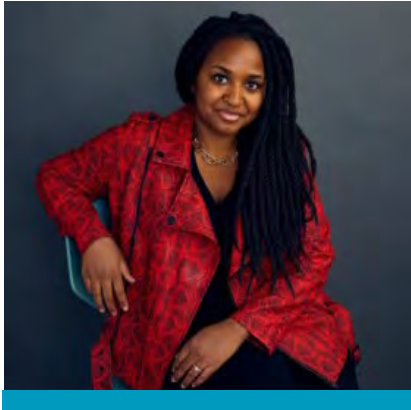
Cybersecurity 101

The Fundamentals of Protecting Sensitive Data
in Health & Human Services

October 2023



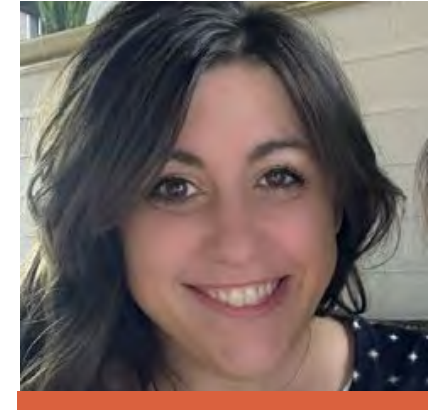
Presenters



Nalisa Familusi
Sr. Cybersecurity Analyst



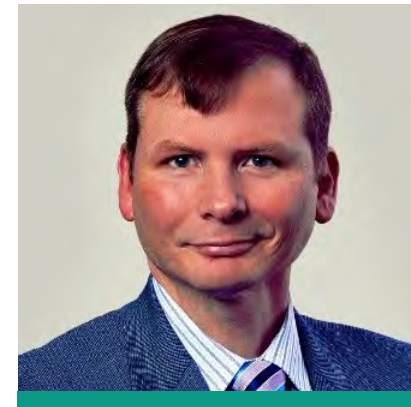
Kirsten Hanson
Cybersecurity Analyst



Sara Sofia
Sr. Cybersecurity
Engineer



Luke Franzelas
Cybersecurity Network
Engineer



Shayne Champion
CISO

Agenda

Phishing

01

Remote Work
Security

03

Q&A

05

02

Basic Work
Security

04

Your Job in
Cybersecurity

Protecting Everybody



**Your organization's
products contain
data for over
12.1 million people**

10.37 connected devices per person²



Total Global Impact of Cyber Crime [has risen to] US \$3 Trillion, making it more profitable than the global trade in marijuana, cocaine and heroin combined.³



Cybercrime Losses [reported in the US] Exceeded **\$10 Billion** in 2022.⁴



54.7% of US information security pros told not to report incidents.⁵

Sources:

1. <https://cybermap.kaspersky.com/>
2. <https://www.statista.com/statistics/1107206/average-number-of-connected-devices-us-house/>
3. <https://www.europol.europa.eu/iocta/2018>
4. <https://www.securityweek.com/cybercrime-losses-exceeded-10-billion-in-2022-fbi/>
5. https://www.theregister.com/2023/04/11/in_brief_security/

The Weakest Link

Firewalls?

E-mail?

Web Browser?

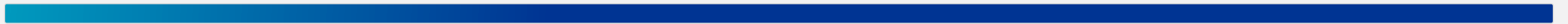
Passwords?



Endpoints?



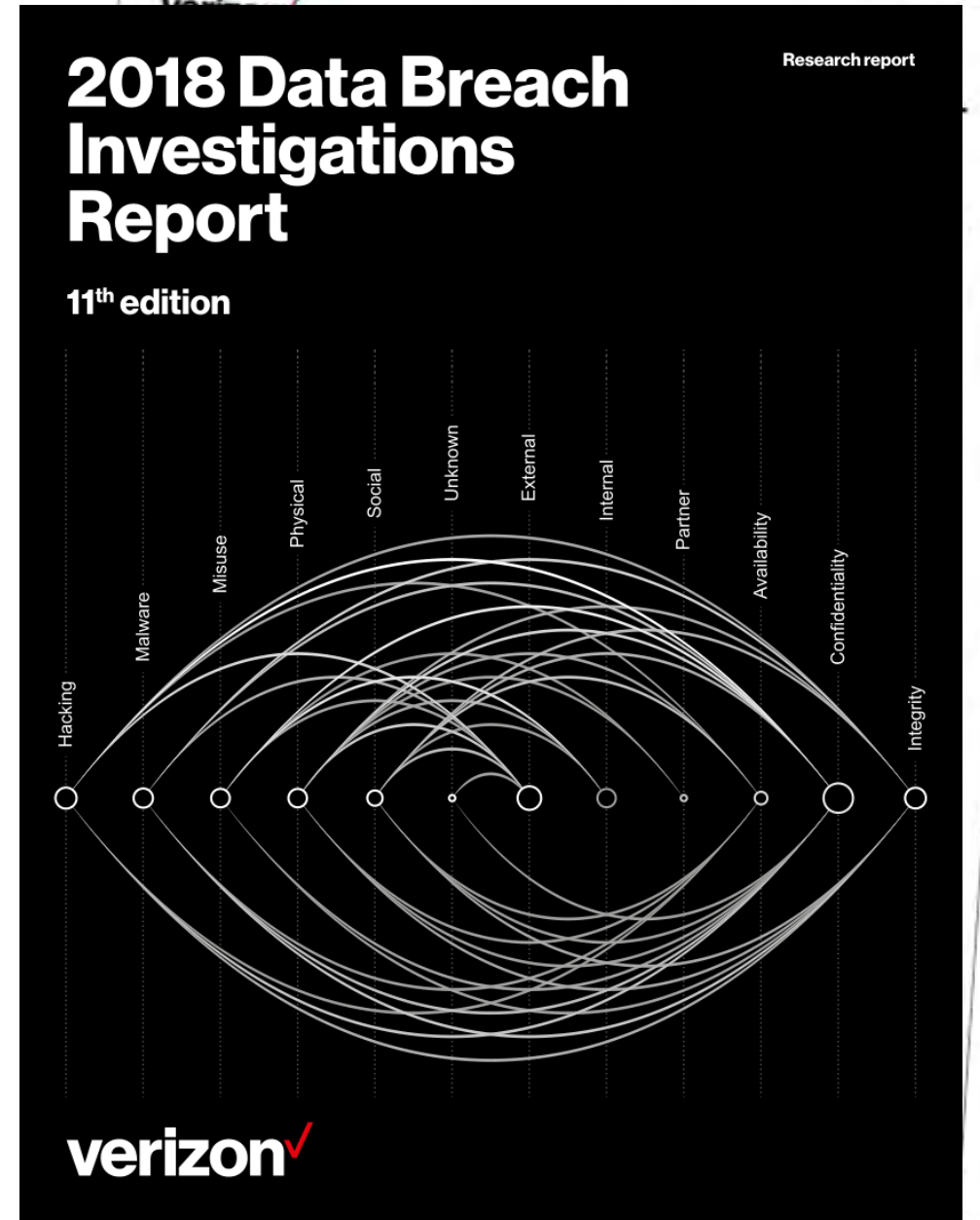
Phishing



✉ How Does It Happen?

”

Phishing and pretexting represent ... **93%** of breaches. Email continues to be the most common vector (**96%**).

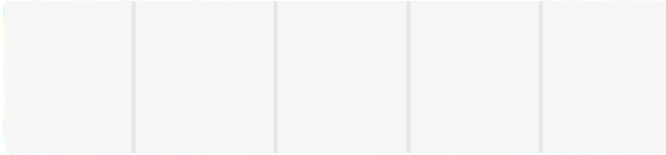


Source: <https://www.verizon.com/business/resources/reports/data-breach-digest/>

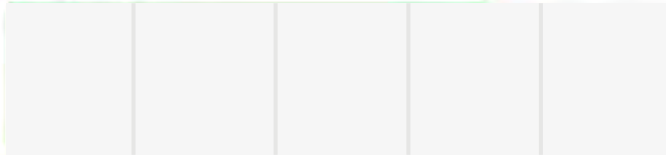
✉ Social Engineering

Social Engineering Attacks

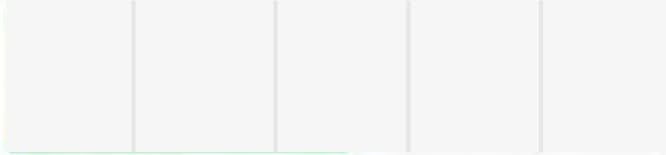
83% of breaches involved External actors (n=5,177)



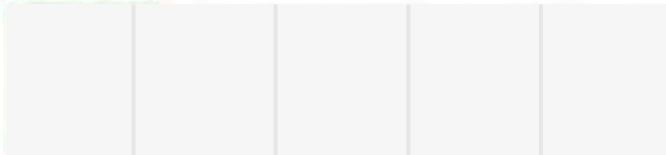
74% of breaches involved a human element (n=4,482)



49% of breaches involved credentials (n=4,396)



24% of breaches involved Ransomware (n=4,354)



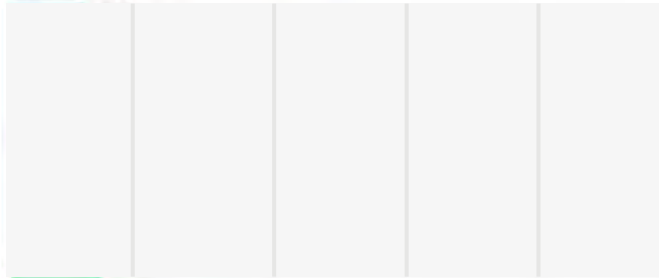
0% 20% 40% 60% 80% 100%

What They Are Doing With It

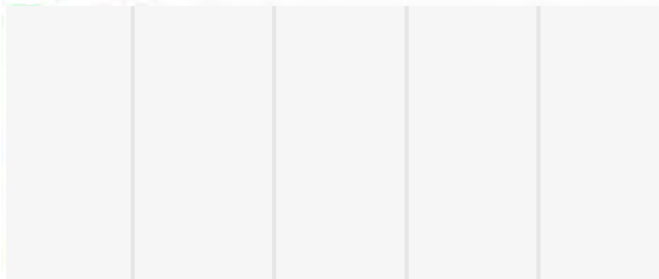
Creds



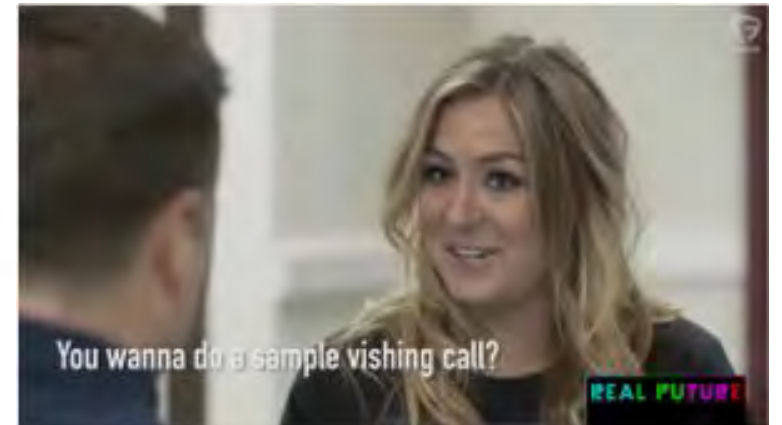
Phishing



Exploit vuln



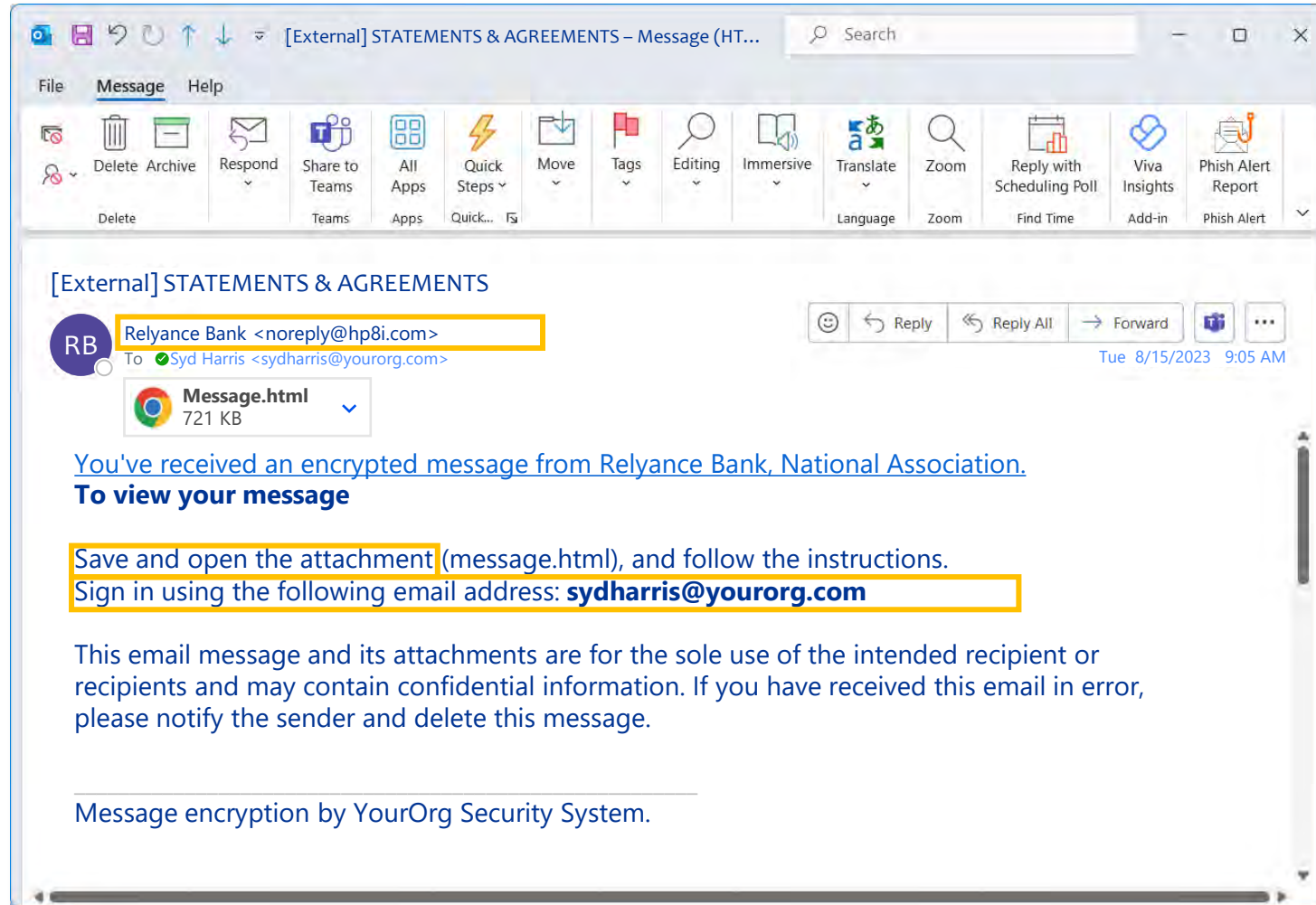
0% 20% 40% 60% 80% 100%



Phishing and Spear Phishing

A malicious use of **email messaging** to either penetrate a network, gather sensitive information, or elicit unapproved goods or services from the company.

Phishing

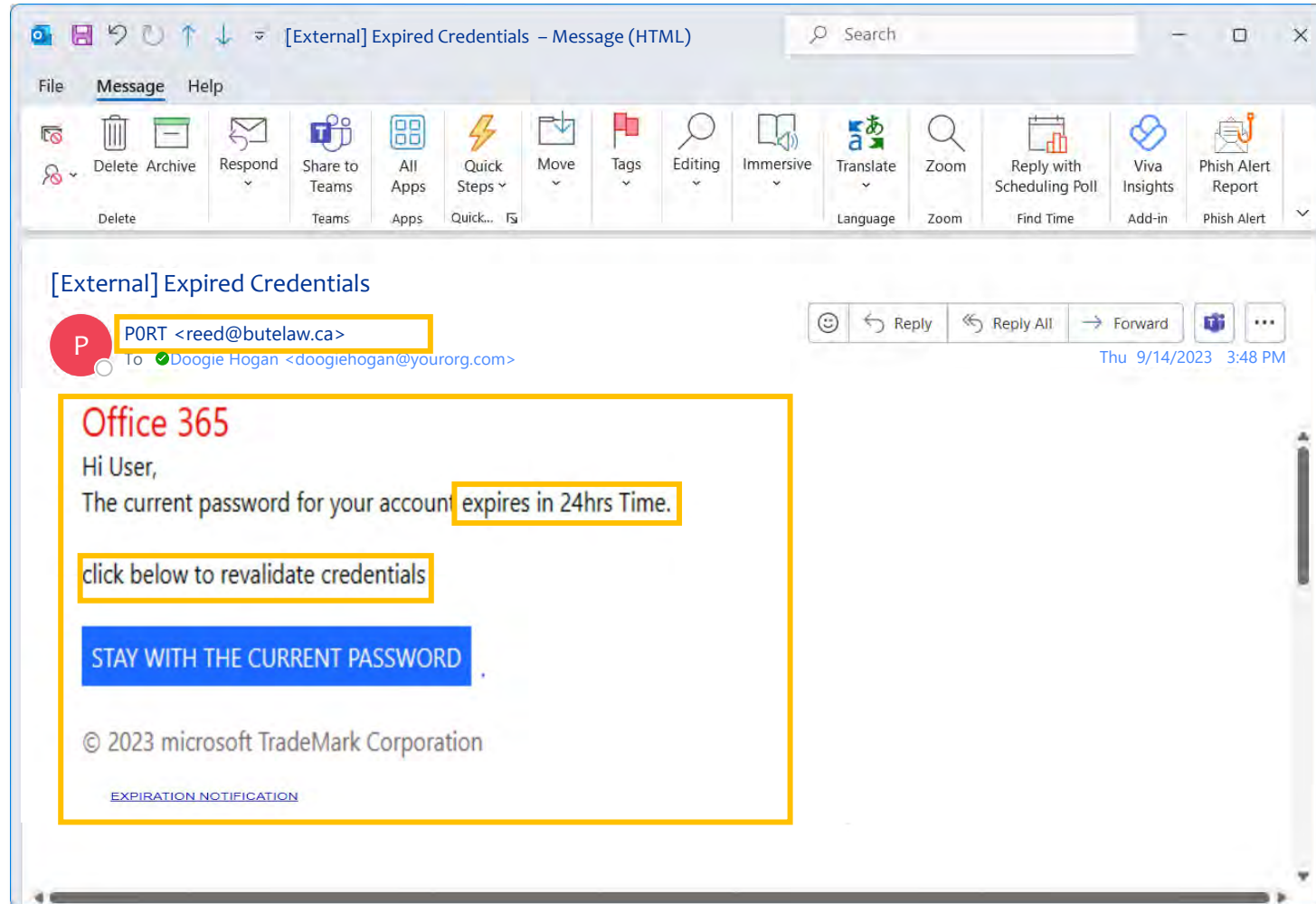


Phishing and Spear Phishing

A malicious use of **email messaging** to either penetrate a network, gather sensitive information, or elicit unapproved goods or services from the company.

Phishing

Weak Form
Spearphishing



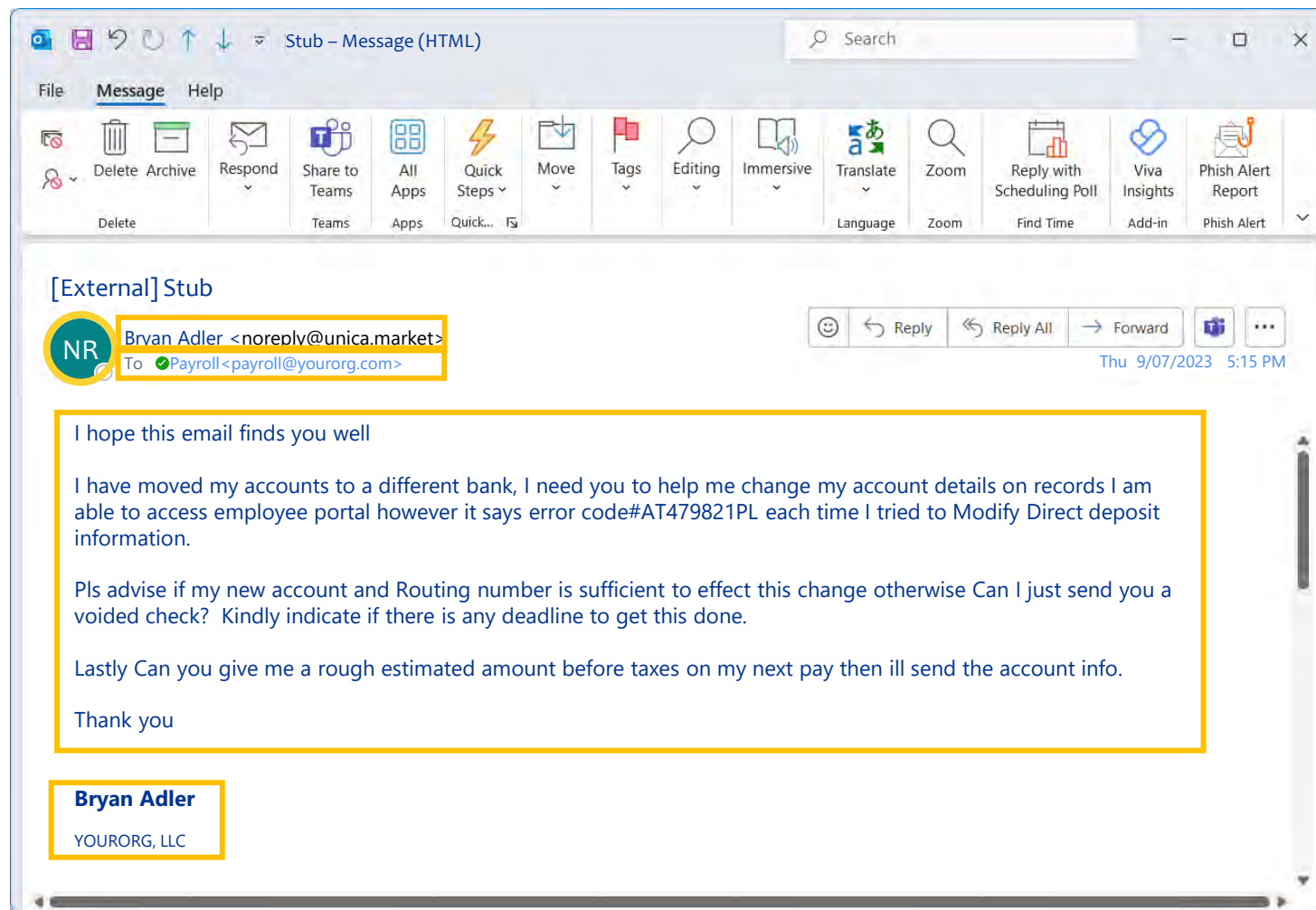
Phishing and Spear Phishing

A malicious use of **email messaging** to either penetrate a network, gather sensitive information, or elicit unapproved goods or services from the company.

Phishing

Weak Form
Spearphishing

Strong Form
Spearphishing



Phishing and Spear Phishing

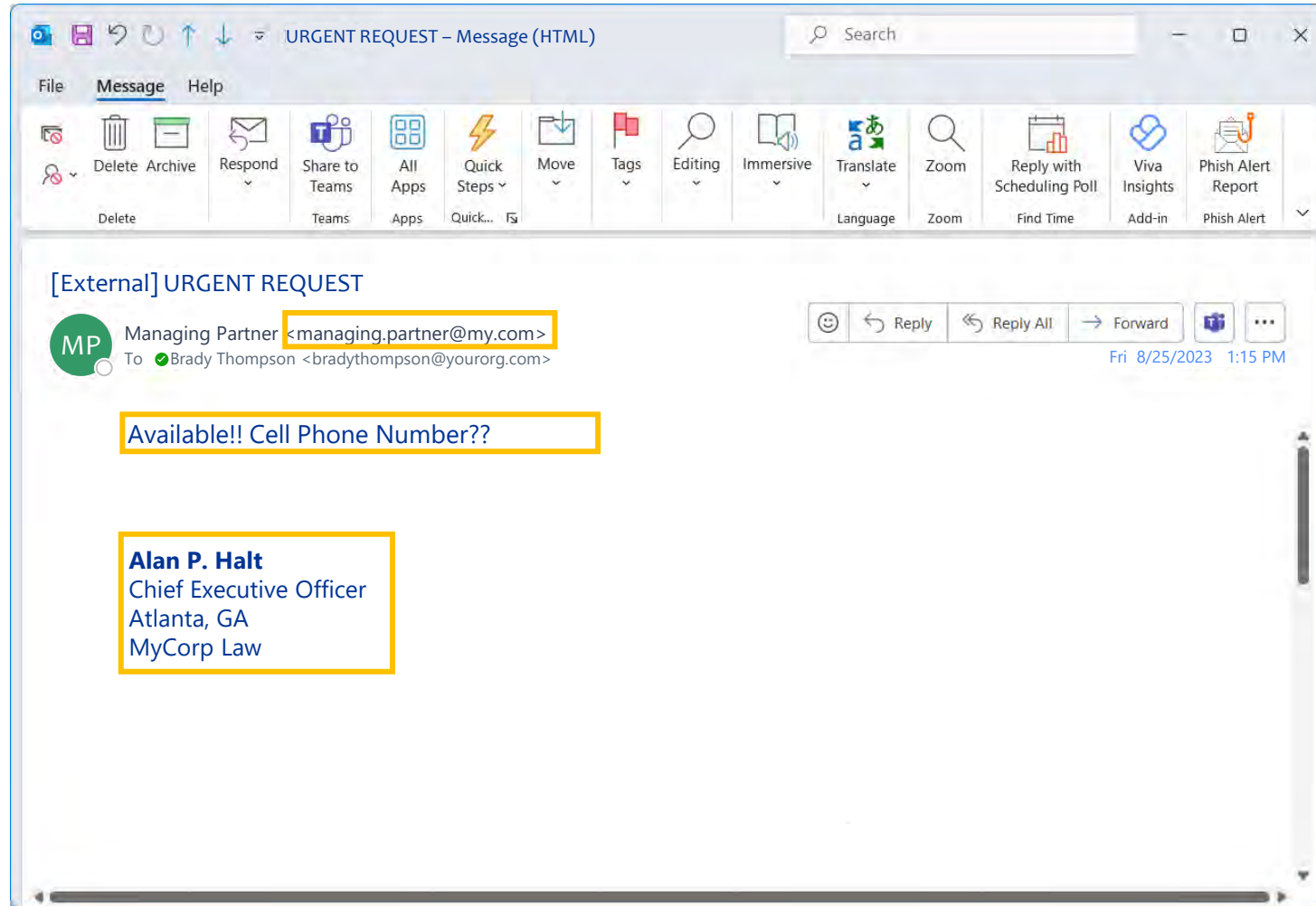
A malicious use of **email messaging** to either penetrate a network, gather sensitive information, or elicit unapproved goods or services from the company.

Phishing

Weak Form
Spearphishing

Strong Form
Spearphishing

Whale
Phishing





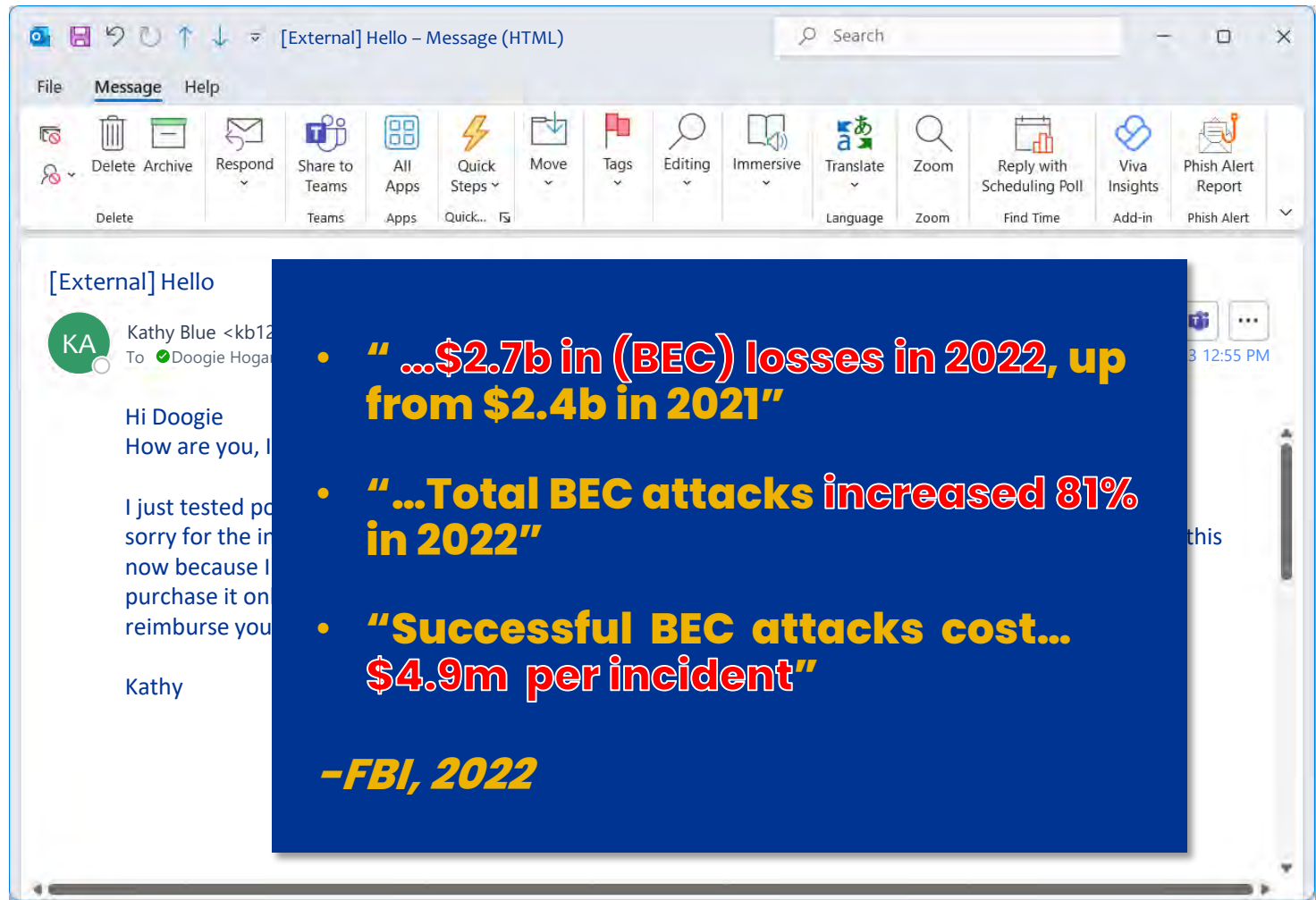
What Phishing Looks Like IRL



Source: <https://www.youtube.com/watch?v=wcXw3q9IL7M>

✉ What Can They Do?

Business Email Compromise (BEC)



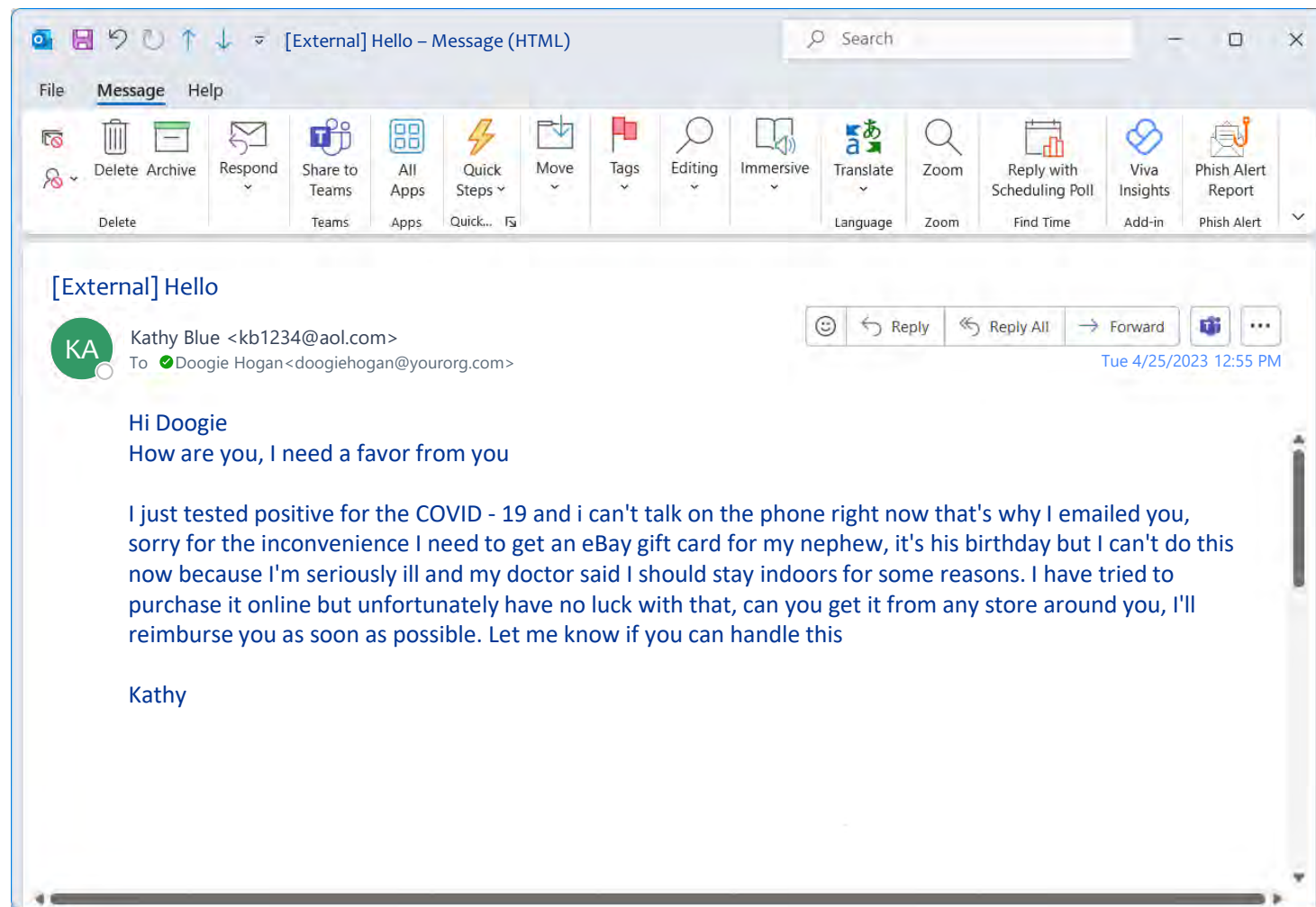
The screenshot shows an Outlook window titled "[External] Hello - Message (HTML)". The ribbon includes "File", "Message", and "Help" tabs. The "Message" tab is active, showing various actions like Delete, Archive, Respond, Share to Teams, All Apps, Quick Steps, Move, Tags, Editing, Immersive, Translate, Zoom, Reply with Scheduling Poll, Viva Insights, and Phish Alert Report. The email content shows a message from "Kathy Blue <kb12>" to "Doogie Hogar". The text of the email is partially visible: "Hi Doogie", "How are you, I", "I just tested po", "sorry for the in", "now because I", "purchase it on", "reimburse you".

Statistics on Business Email Compromise (BEC) attacks:

- **"...\$2.7b in (BEC) losses in 2022, up from \$2.4b in 2021"**
- **"...Total BEC attacks increased 81% in 2022"**
- **"Successful BEC attacks cost... \$4.9m per incident"**

-FBI, 2022

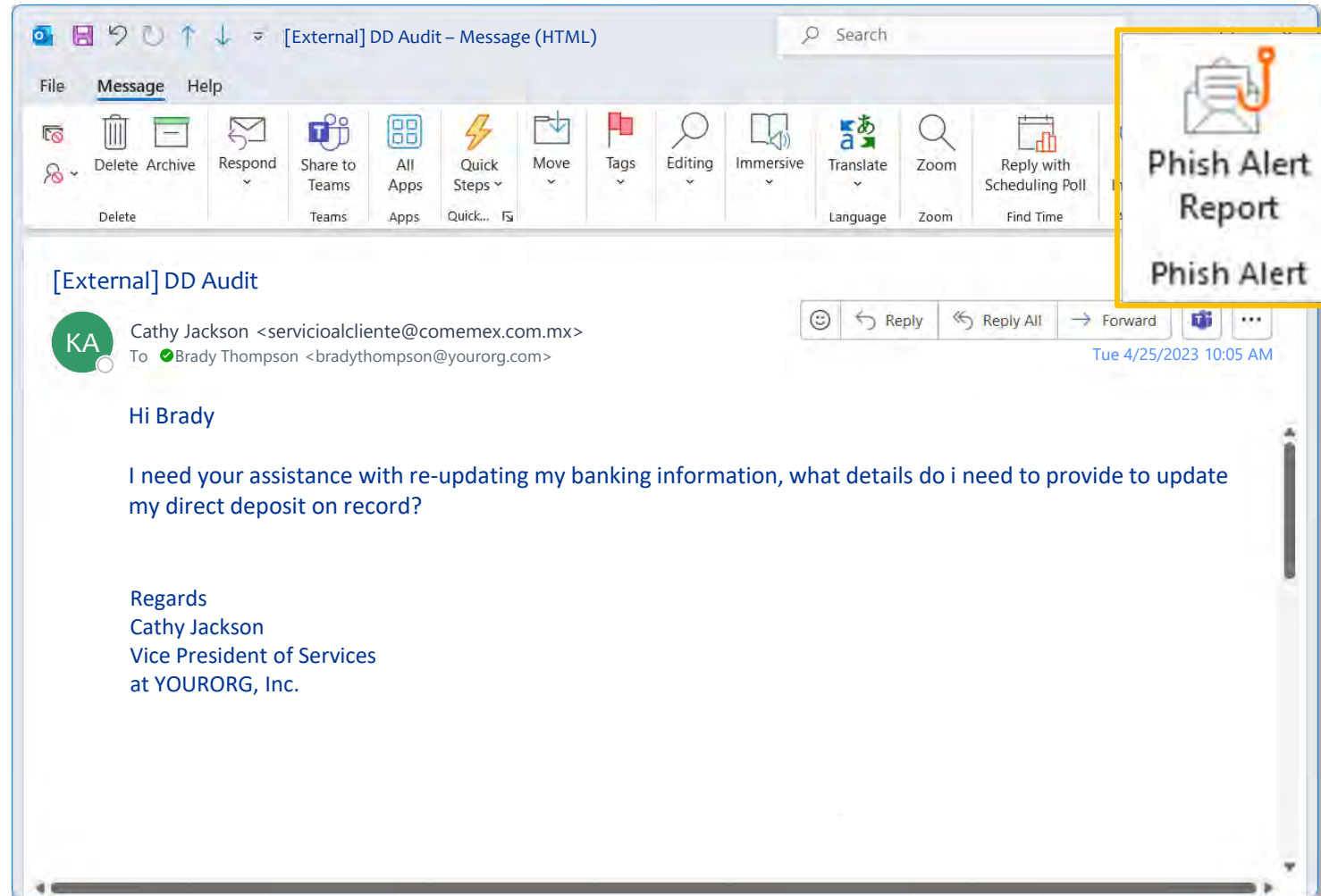
The OTHER Major BEC Threat



- Trick employees into sending gift cards
- Low Value (<\$250)
- Difficult to Trace
- Favorite Targets: Google Play, eBay, Target, iTunes, Walmart, Best Buy, Amazon, Steam, & the Apple Store

Report Phishing

Reporting a suspected phishing email is easy!



The screenshot shows an Outlook window titled "[External] DD Audit - Message (HTML)". The ribbon includes "File", "Message", and "Help". The "Message" ribbon has various actions like Delete, Archive, Respond, Share to Teams, All Apps, Quick Steps, Move, Tags, Editing, Immersive, Translate, Zoom, and Reply with Scheduling Poll. The email content is from Cathy Jackson to Brady Thompson, asking for assistance with updating banking information. A yellow-bordered overlay on the right side of the window contains the text "Phish Alert Report" and "Phish Alert" with a corresponding icon of a document with a red checkmark and a magnifying glass.

[External] DD Audit

Cathy Jackson <servicioalcliente@comemex.com.mx>
To: Brady Thompson <bradythompson@yourorg.com>

Tue 4/25/2023 10:05 AM

Hi Brady

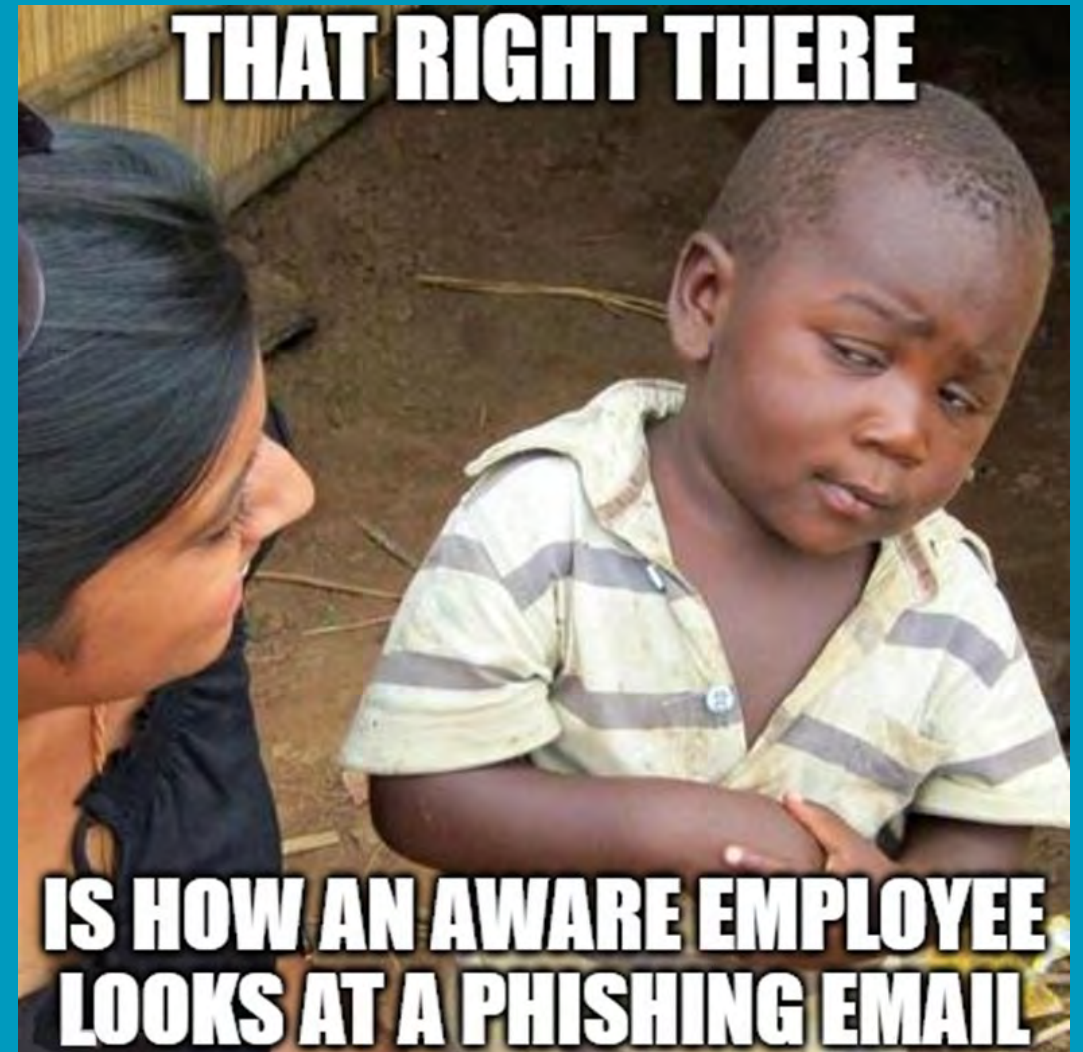
I need your assistance with re-updating my banking information, what details do i need to provide to update my direct deposit on record?

Regards
Cathy Jackson
Vice President of Services
at YOURORG, Inc.

Phish Alert Report
Phish Alert

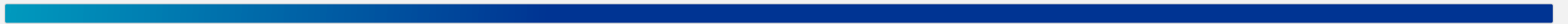
✉ Phishing Review

- What Threat Actors Want
- Phishing Types
 - Phishing
 - Weak-Form Spear Phishing
 - Strong-Form Spear Phishing
 - Whale Phishing
- Business Email Compromise
- Reporting Phishing





Basic Work Security





Newest Technology to Help Track Your Passwords



Source: https://www.youtube.com/watch?v=Srh_TV_J144



Normal Passwords

Property	Requirements
Characters allowed	A – Z a – z 0 – 9 @ # \$ % ^ & * - _ ! + = [] { } \ : ' , . ? / ` ~ " () ; blank space
Length constraints	A minimum of 8 characters and a maximum of 256 characters
Password restrictions	Requires three out of four of the following: Lowercase characters Uppercase characters Numbers (0-9) Symbols (no unicode)
Password expiration	Every 60 days Do not reuse passwords Keep Them Different





Best Password Requirements

- **Length** (min 15 chars)
- **No** complexity requirements
- Change once per **year**





Best Password Requirements

'Secure' 8-character password example:

R&2Lf^v!

TIME TO HACK: 3 Hours

Passphrases can be easier to remember:

The Hills Are Alive

Th3H1lls@r3@11v3!

TIME TO HACK: 205 Trillion Years





Clean Desk Policy

- Always protect the data
- Screens or documents should not be viewable when you're not there





Your Laptop

DO

- Store data in OneDrive/SharePoint
- Turn off Wi-Fi if not in use
- Lock it up if left in a hotel room
- Cover if left in a car

DO NOT

- Store data on the C:\ drive
- Let other people use it for anything
- Visit sites you do not want disclosed!
- Leave your laptop unattended



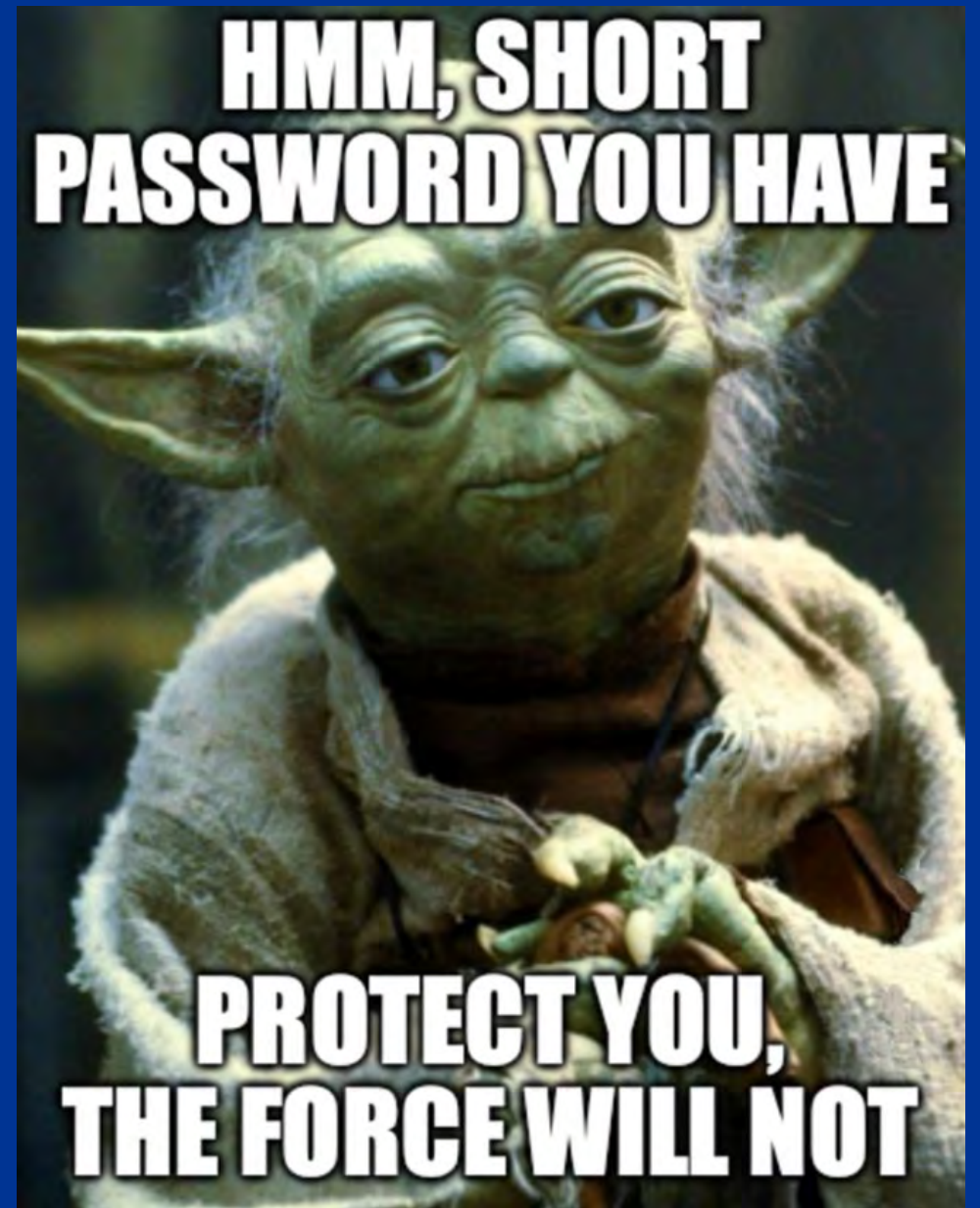
Your Laptop

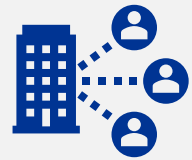




Basic Work Security Review

- Passwords
- Pass Phrases
- Clean Desk Policy
- Laptop Security





Remote Work Security



What Data Can You Lose in a Coffee Shop





Remote Work Considerations

How do you protect:

- Network Connection
 - To the Office
 - Wireless
- Eavesdropping
 - Shoulder Surfing
 - Phone Calls
- Confidential Data
- Portable Media





Remote Work Considerations

How do you protect:

- Network Connection
 - To the Office
 - Wireless
- Eavesdropping
 - Shoulder Surfing
 - Phone Calls
- Confidential Data
- Portable Media



**What Has
Changed?
Nothing.**

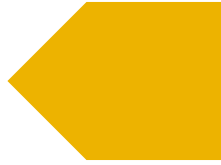
**Well, MOSTLY
nothing.**



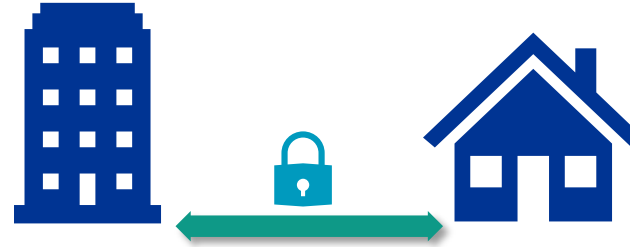
Remote Work Considerations

How do you protect:

- Network Connection
 - To the Office
 - Wireless
- Eavesdropping
 - Shoulder Surfing
 - Phone Calls
- Confidential Data
- Portable Media



- Use your company's VPN
- Do not use public Wi-Fi if possible
- Install updates quickly (including home routers)





Remote Work Considerations

How do you protect:

- Network Connection
 - To the Office
 - Wireless
- Eavesdropping
 - Shoulder Surfing
 - Phone Calls
- Confidential Data
- Portable Media

- Changes in threat actors
- Blocking visibility / shoulder surfing
- Stay vigilant!

According to the FBI Internet Crime Complaint Center (IC3), victims & subjects*:

- **85%** were in the same country
- **56%** were in the same state
- **35%** were even in the same city

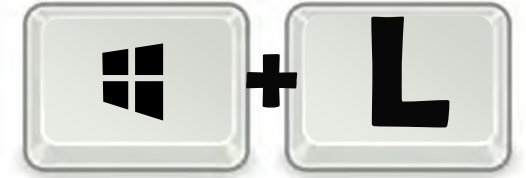
**Driven in part by high-population areas such as Los Angeles, CA, and New York City, NY*



Remote Work Considerations

How do you protect:

- Network Connection
 - To the Office
 - Wireless
- Eavesdropping
 - Shoulder Surfing
 - Phone Calls
- Confidential Data
- Portable Media



- Use corporate services for e-mail, messaging, & all other work
- Keep Work Data Off Non-Work Computers
- Lock your device before walking away





Remote Work Considerations

How do you protect:

- Network Connection
 - To the Office
 - Wireless
- Eavesdropping
 - Shoulder Surfing
 - Phone Calls
- Confidential Data
- Portable Media

Now is the time for all good men to come to the aid of their country.



- Data encryption
- Portable media





Remote Work Security

- Network Connection
- Eavesdropping
- Confidential Data
- Portable Media
- Physical Documents

**Me getting out of bed at 8:55 to
start working at 9**





**YOUR Job in
Cybersecurity**



Pop Quiz

What is the most important part of YOURORG's Cyber Security program?





What is Missing?



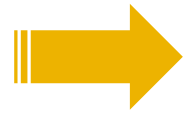
**See something.
Say something.**

Email: cyber_security@yourorg.com

Phone: (213) 321-1234



Good Security is Not Difficult



It's Not



**ROCKET
SURGERY!**



What is Missing? **YOU**



TEAMWORK
They'll never know what hit them



Key Resources

- **Kaspersky Cyber Map** <https://cybermap.kaspersky.com/>
- **2018 Verizon DBIR** <https://www.verizon.com/business/resources/reports/data-breach-digest>
- **2023 Verizon DBIR** <https://www.verizon.com/business/resources/reports/dbir>
- **Hacker Vishing Video** <https://www.youtube.com/watch?v=lc7scxvKQOo>
- **Phishing IRL Video** <https://www.youtube.com/watch?v=wcXw3q91L7M>
- **Microsoft Phishing Button** <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/submissions-outlook-report-messages>
- **Ellen Internet Password Video** https://www.youtube.com/watch?v=Srh_TV_J144
- **Time To Hack Passwords Link** <https://www.itsecurityguru.org/2023/05/18/time-taken-for-hackers-to-crack-passwords-revealed/>
- **Coffee Shop Video** <https://www.youtube.com/watch?v=yvjT8m0hcKU>

Q & A



Additional Resources!

CYBERSECURITY AWARENESS MONTH TOOLKIT

- White Paper – A Comprehensive **Guide to Cybersecurity Training** in Human Services
- New cybersecurity tip **posters** published weekly with corresponding **blogs** to tell you how to put the tip into action!
 - Print out this 8.5 x 11" mini-poster for your office – whether you're working from home or not, you'll want to keep these tips in mind year-round.



THANK YOU!

