NJCCIC

PREVENT | DETECT | RESPOND

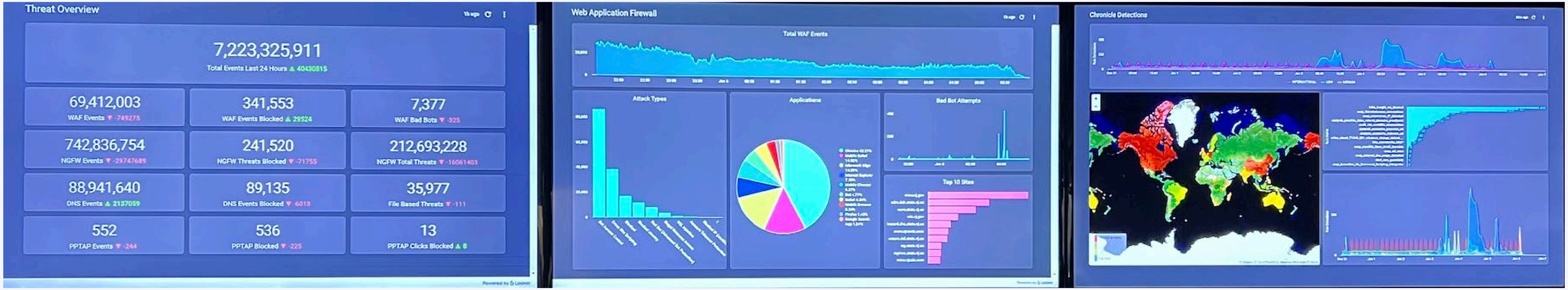
This presentation is TLP: CLEAR

The NJ CCIC

Governance, Risk, and Compliance

Cyber Threat Outreach and Partnerships

Security Engineering and Cyber Operations



Threat Overview

7,223,325,911
Total Events Last 24 Hours ▲ 40430815

69,412,003
WAF Events ▼ -749275

341,553
WAF Events Blocked ▲ 29524

7,377
WAF Bad Bots ▼ -325

742,836,754
NGFW Events ▼ -29747689

241,520
NGFW Threats Blocked ▼ -71755

212,693,228
NGFW Total Threats ▼ -16061403

88,941,640
DNS Events ▲ 2137059

89,135
DNS Events Blocked ▼ -6013

35,977
File Based Threats ▼ -111

552
PPTAP Events ▼ -244

536
PPTAP Blocked ▼ -225

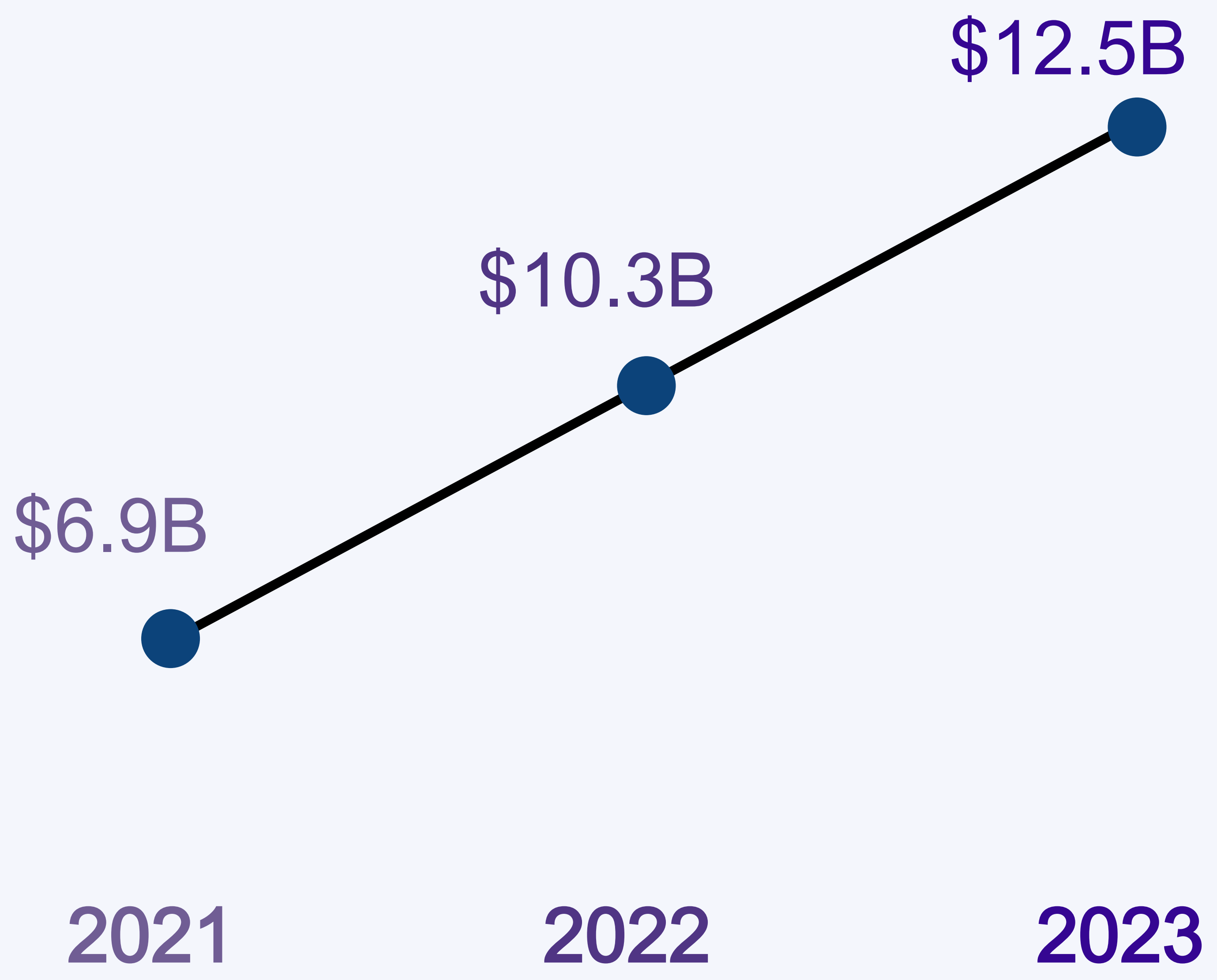
13
PPTAP Clicks Blocked ▲ 8

Cyber Threats and Best Practices

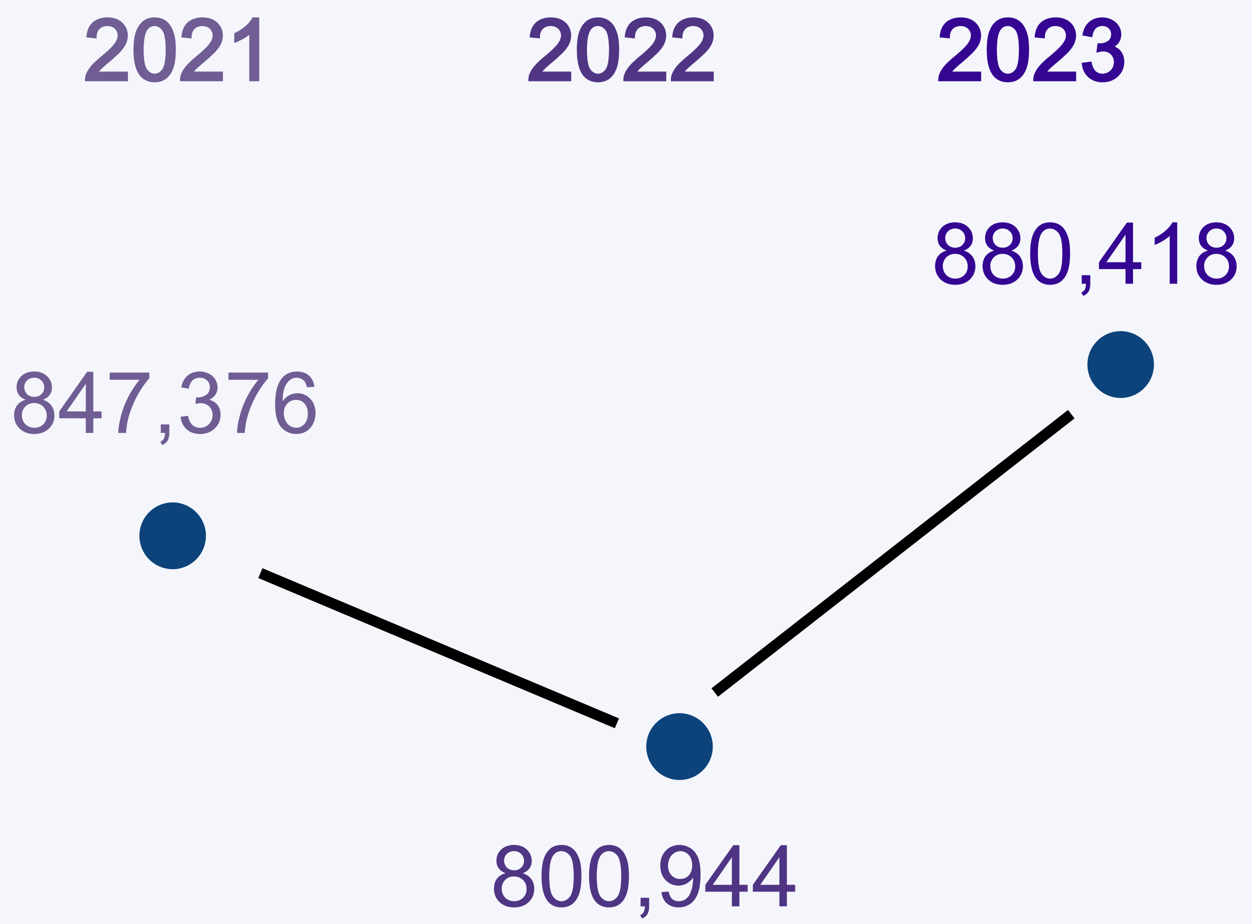
Impacts to the Healthcare and Public Health Sector

IC3 Annual Report

TOTAL CYBERCRIME LOSSES



TOTAL COMPLAINTS



IC3 Annual Report

Greatest Losses By Cybercrime Type

Investment - $4.57 B

Business Email Compromise - $2.9 B

Tech Support Scam - $924 M

Confidence/Romance Scam- $652 M

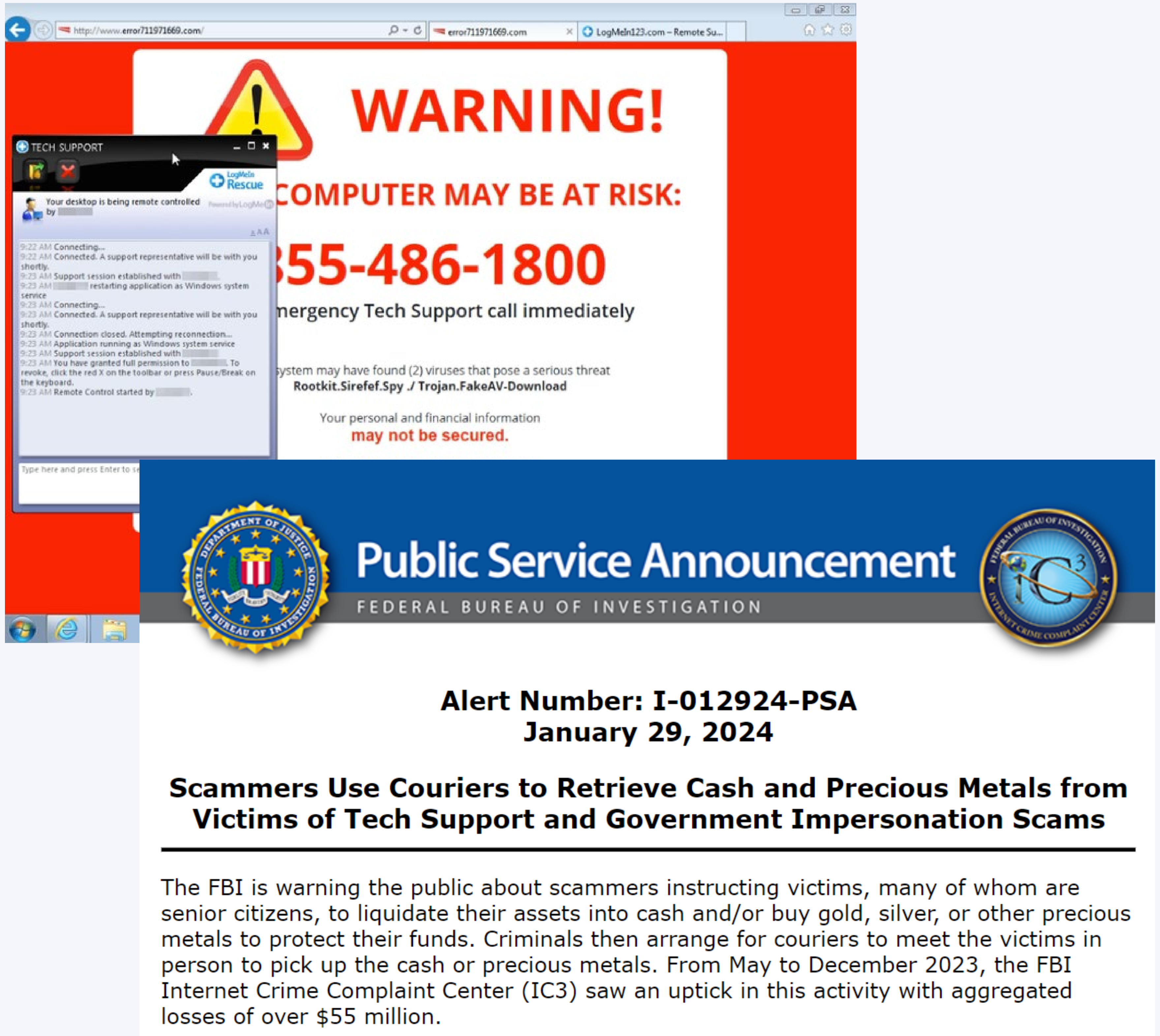
Government Impersonation - $394 M

Real Estate Transaction - $145 M

Extortion - $74.8 M

Tech Support Scam

IMPERSONATING THOSE YOU TRUST



WARNING!

COMPUTER MAY BE AT RISK:

355-486-1800

mergency Tech Support call immediately

ystem may have found (2) viruses that pose a serious threat
Rootkit.Sirefef.Spy ./ Trojan.FakeAV-Download

Your personal and financial information
may not be secured.

Your desktop is being remote controlled by [redacted]

```
9:22 AM Connecting...
9:22 AM Connected. A support representative will be with you shortly.
9:23 AM Support session established with [redacted].
9:23 AM [redacted] restarting application as Windows system service
9:23 AM Connecting...
9:23 AM Connected. A support representative will be with you shortly.
9:23 AM Connection closed. Attempting reconnection...
9:23 AM Application running as Windows system service
9:23 AM Support session established with [redacted]
9:23 AM You have granted full permission to [redacted]. To revoke, click the red X on the toolbar or press Pause/Break on the keyboard.
9:23 AM Remote Control started by [redacted].
```

Type here and press Enter to se

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-012924-PSA
January 29, 2024

Scammers Use Couriers to Retrieve Cash and Precious Metals from Victims of Tech Support and Government Impersonation Scams

The FBI is warning the public about scammers instructing victims, many of whom are senior citizens, to liquidate their assets into cash and/or buy gold, silver, or other precious metals to protect their funds. Criminals then arrange for couriers to meet the victims in person to pick up the cash or precious metals. From May to December 2023, the FBI Internet Crime Complaint Center (IC3) saw an uptick in this activity with aggregated losses of over $55 million.

Recent incident:

An employee was the target of a social engineering attack. This employee was deceived into believing that her computer was infected with a computer virus and that in order to prevent further damage, she should contact "Microsoft's" customer support. The scammer was not affiliated in any way with Microsoft. The employee unfortunately did contact this false number and shared her screen with the scammer. This phone call lasted approximately 30 minutes, during which time the scammer was able to access all of the files on the employee's computer. These files contained highly confidential information, including Social Security numbers, dates of birth, addresses, and financial information. The employee became suspicious when the scammer asked her to go to a local department store and purchase $20,000 in gift cards. It was then that the employee terminated her call and disconnected her computer.

Impacts:

- Access to sensitive organization information.
- Obtain credentials for the employee's online accounts.
- Ability to install malware onto the device – persistent access and opportunity to move laterally/compromise accounts on the network.
- Need to change passwords, ensure MFA is enabled, and revoke session tokens.

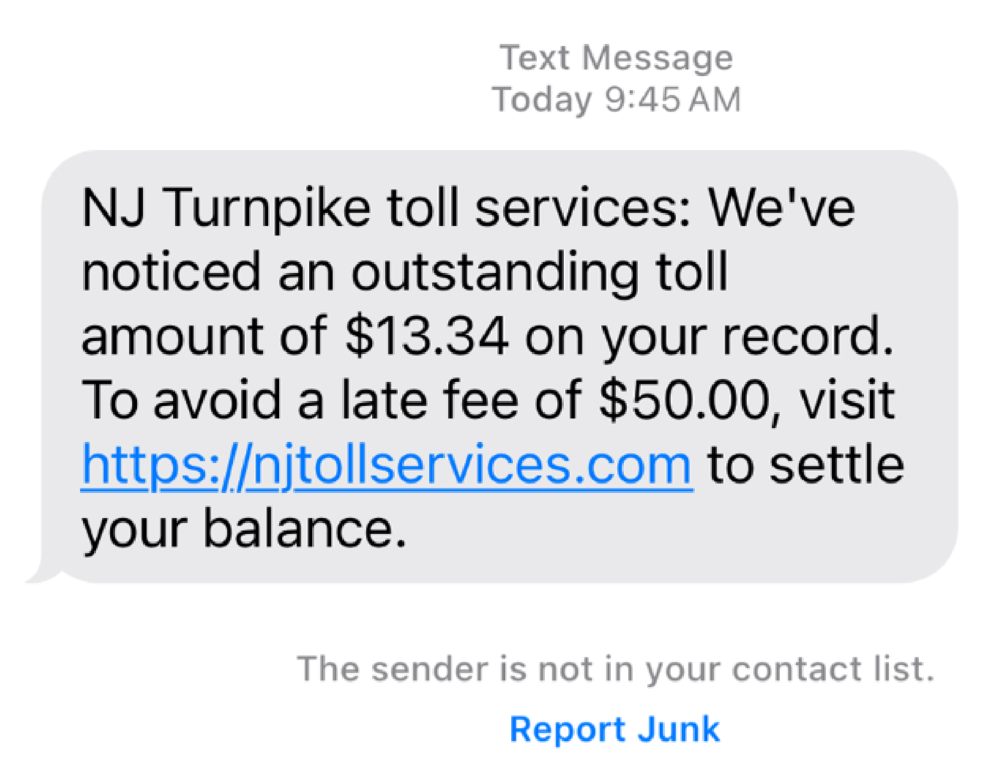
SMS Text Scam

Exploiting Legitimate Comms

- Missed delivery notifications
- “Is this you?” messages
- Text scams claiming that your bank is closing your account
- Texts claiming that you’ve won a prize
- Texts claiming that your debit or credit card has been locked
- Text messages supposedly from the IRS
- Text messages from your own number
- Texts claiming that your payment for subscription services didn’t go through
- Texts about purchases you didn’t make
- Two-factor authentication (2FA) scam messages

SMS Text Scam

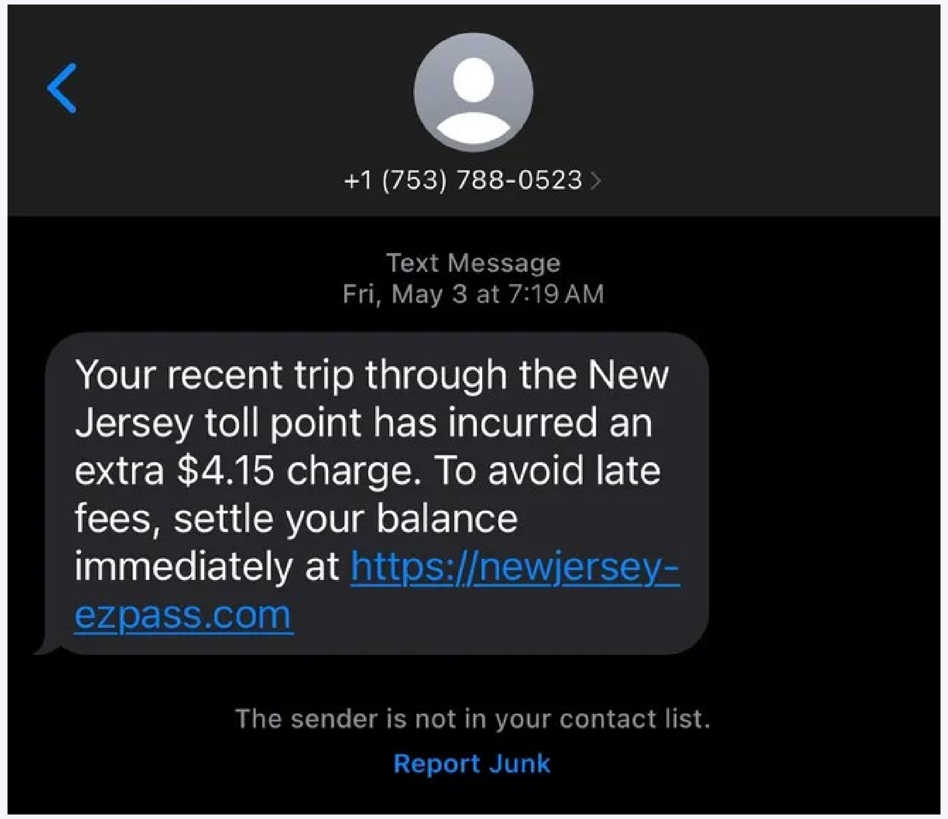
Exploiting Legitimate Comms



Text Message
Today 9:45 AM

NJ Turnpike toll services: We've noticed an outstanding toll amount of $13.34 on your record. To avoid a late fee of $50.00, visit https://njtollservices.com to settle your balance.

The sender is not in your contact list.

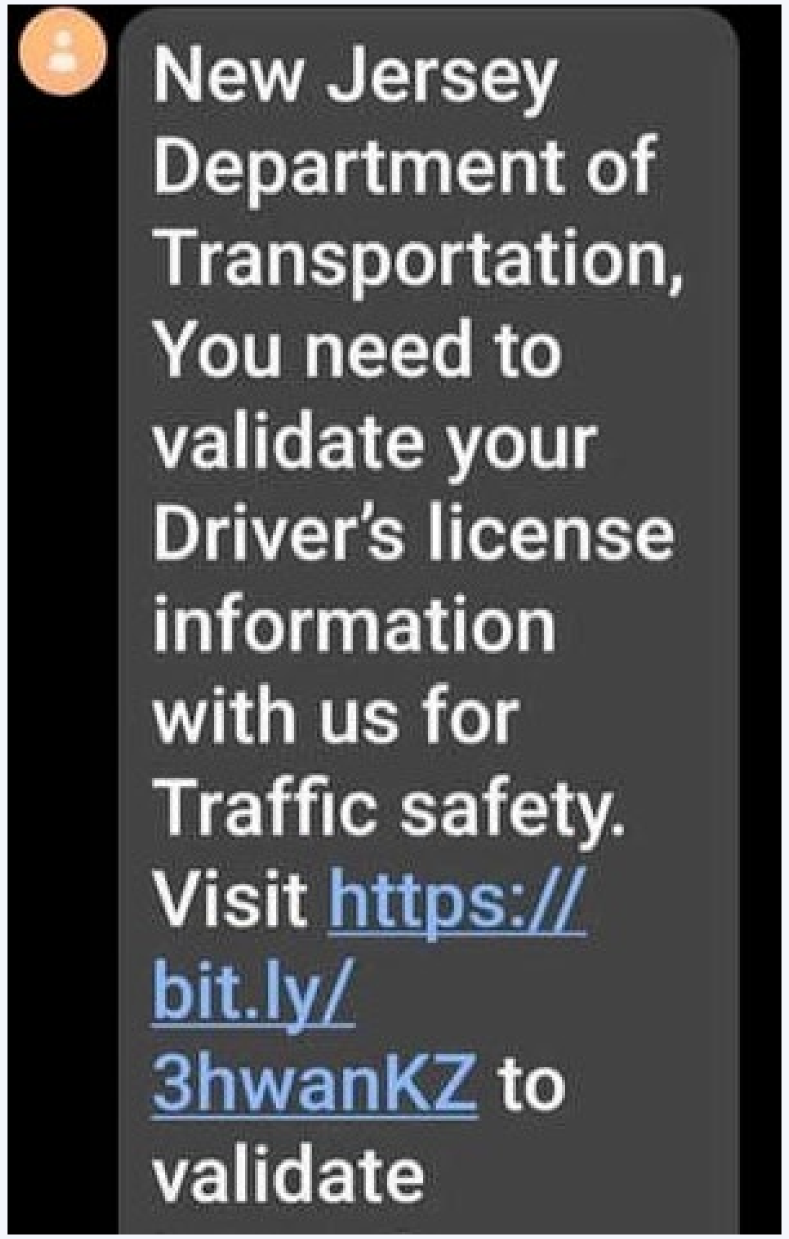


+1 (753) 788-0523

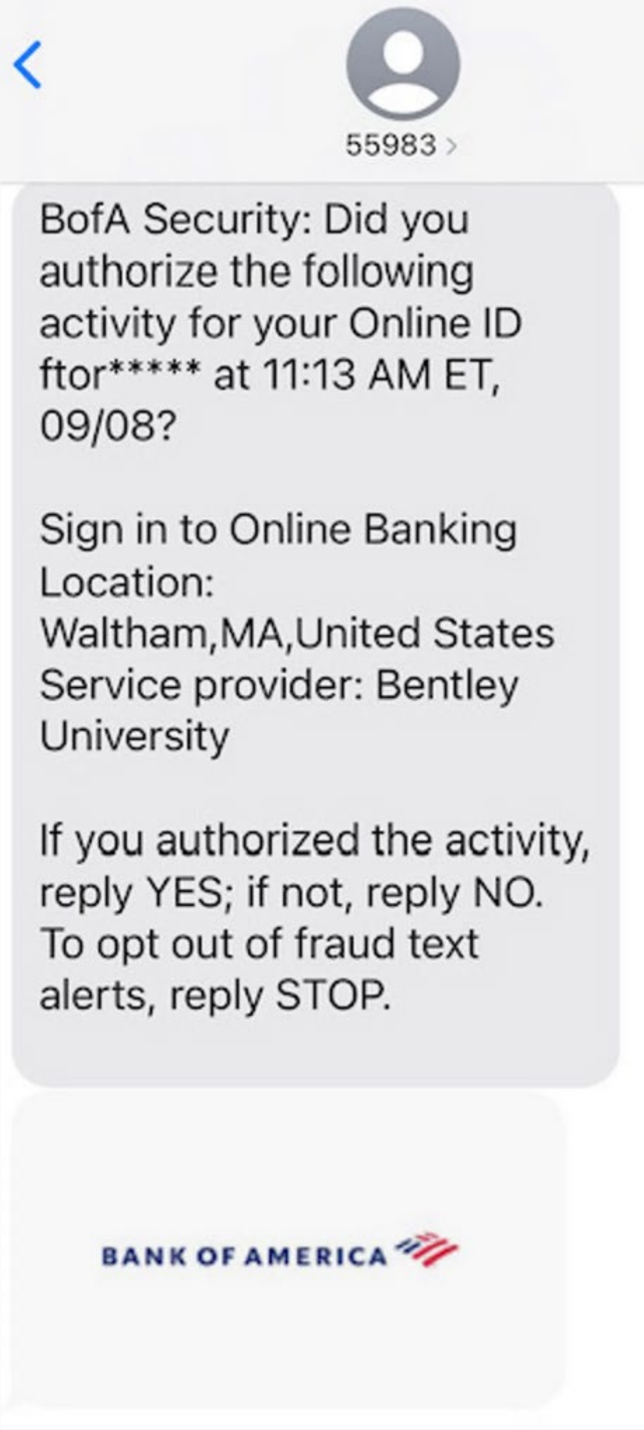
Text Message
Fri, May 3 at 7:19 AM

Your recent trip through the New Jersey toll point has incurred an extra $4.15 charge. To avoid late fees, settle your balance immediately at https://newjersey-ezpass.com

The sender is not in your contact list.



New Jersey Department of Transportation, You need to validate your Driver's license information with us for Traffic safety. Visit https://bit.ly/3hwanKZ to validate

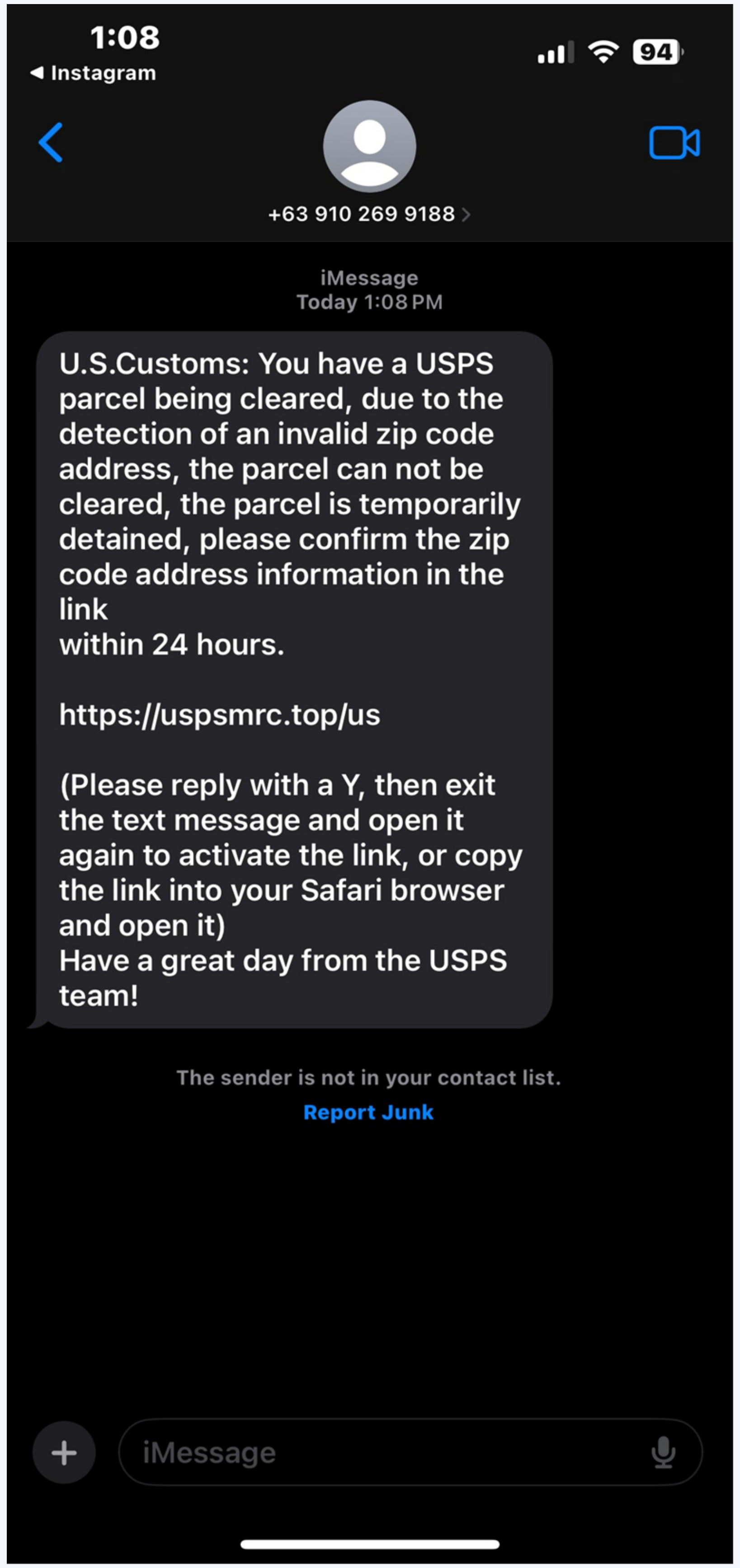


55983

BofA Security: Did you authorize the following activity for your Online ID ftor***** at 11:13 AM ET, 09/08?

Sign in to Online Banking
Location: Waltham,MA,United States
Service provider: Bentley University

If you authorized the activity, reply YES; if not, reply NO. To opt out of fraud text alerts, reply STOP.



+63 910 269 9188

iMessage
Today 1:08 PM

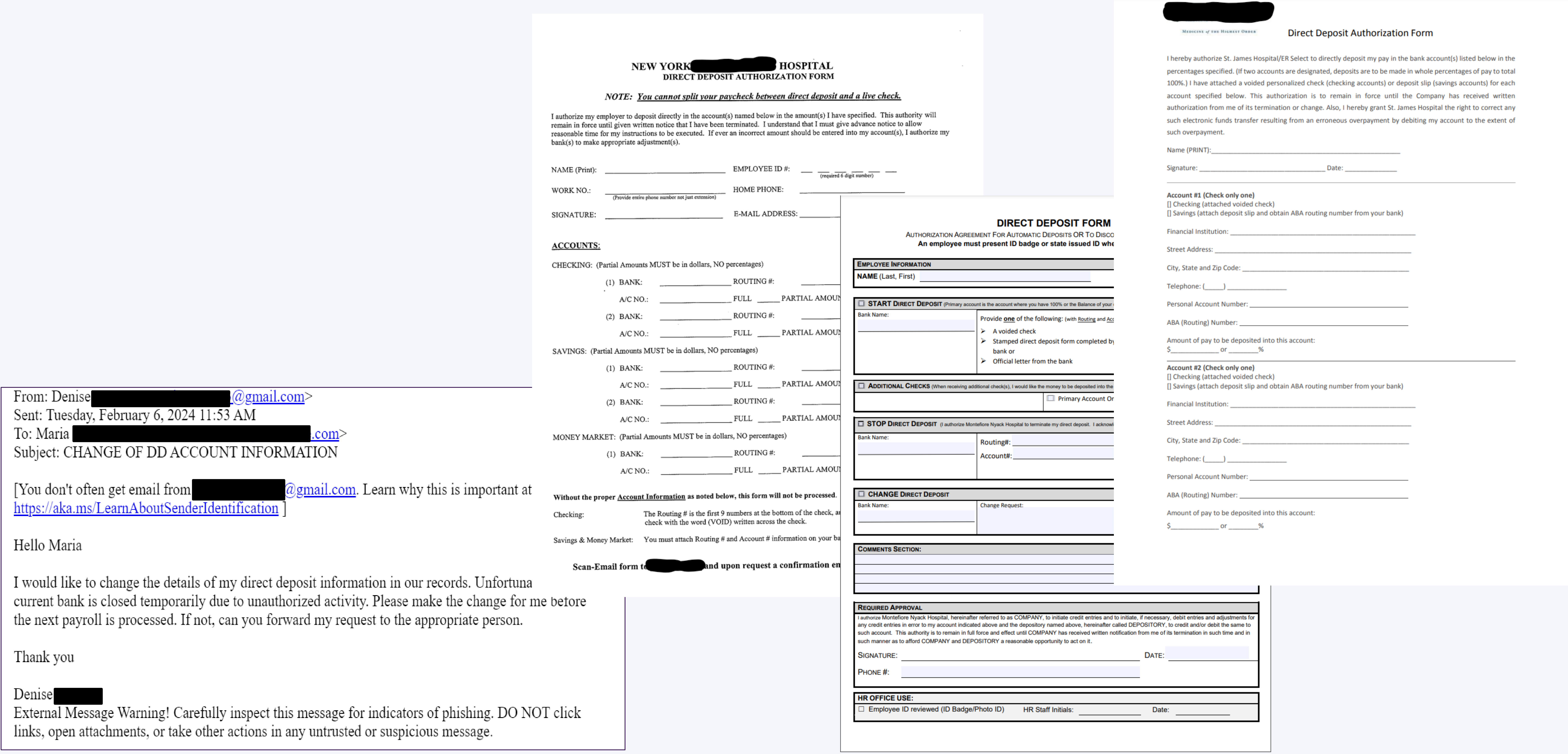
U.S.Customs: You have a USPS parcel being cleared, due to the detection of an invalid zip code address, the parcel can not be cleared, the parcel is temporarily detained, please confirm the zip code address information in the link
within 24 hours.

https://uspsmrc.top/us

(Please reply with a Y, then exit the text message and open it again to activate the link, or copy the link into your Safari browser and open it)
Have a great day from the USPS team!

The sender is not in your contact list.

Direct Deposit Scams



From: Denise [redacted]@gmail.com>
Sent: Tuesday, February 6, 2024 11:53 AM
To: Maria [redacted].com>
Subject: CHANGE OF DD ACCOUNT INFORMATION

[You don't often get email from [redacted]@gmail.com. Learn why this is important at https://aka.ms/LearnAboutSenderIdentification]

Hello Maria

I would like to change the details of my direct deposit information in our records. Unfortuna current bank is closed temporarily due to unauthorized activity. Please make the change for me before the next payroll is processed. If not, can you forward my request to the appropriate person.

Thank you

Denise [redacted]

External Message Warning! Carefully inspect this message for indicators of phishing. DO NOT click links, open attachments, or take other actions in any untrusted or suspicious message.

NEW YORK [redacted] HOSPITAL
DIRECT DEPOSIT AUTHORIZATION FORM

NOTE: ***You cannot split your paycheck between direct deposit and a live check.***

I authorize my employer to deposit directly in the account(s) named below in the amount(s) I have specified. This authority will remain in force until given written notice that I have been terminated. I understand that I must give advance notice to allow reasonable time for my instructions to be executed. If ever an incorrect amount should be entered into my account(s), I authorize my bank(s) to make appropriate adjustment(s).

NAME (Print): ____________ EMPLOYEE ID #: __ __ __ __ __ __ (required 6 digit number)

WORK NO.: ____________ (Provide entire phone number not just extension) HOME PHONE: ____________

SIGNATURE: ____________ E-MAIL ADDRESS: ____________

ACCOUNTS:

CHECKING: (Partial Amounts MUST be in dollars, NO percentages)

(1) BANK: ____________ ROUTING #: ____________
A/C NO.: ____________ FULL _____ PARTIAL AMOUN

(2) BANK: ____________ ROUTING #: ____________
A/C NO.: ____________ FULL _____ PARTIAL AMOUN

SAVINGS: (Partial Amounts MUST be in dollars, NO percentages)

(1) BANK: ____________ ROUTING #: ____________
A/C NO.: ____________ FULL _____ PARTIAL AMOUN

(2) BANK: ____________ ROUTING #: ____________
A/C NO.: ____________ FULL _____ PARTIAL AMOUN

MONEY MARKET: (Partial Amounts MUST be in dollars, NO percentages)

(1) BANK: ____________ ROUTING #: ____________
A/C NO.: ____________ FULL _____ PARTIAL AMOUN

Without the proper Account Information as noted below, this form will not be processed.

Checking: The Routing # is the first 9 numbers at the bottom of the check, ar check with the word (VOID) written across the check.

Savings & Money Market: You must attach Routing # and Account # information on your ba

Scan-Email form t[redacted]and upon request a confirmation en

DIRECT DEPOSIT FORM
AUTHORIZATION AGREEMENT FOR AUTOMATIC DEPOSITS OR TO DISCO
An employee must present ID badge or state issued ID whe

EMPLOYEE INFORMATION
NAME (Last, First) ____________

□ **START DIRECT DEPOSIT** (Primary account is the account where you have 100% or the Balance of your
Bank Name: ____________
Provide **one** of the following: (with Routing and Acc
- A voided check
- Stamped direct deposit form completed by bank or
- Official letter from the bank

□ **ADDITIONAL CHECKS** (When receiving additional check(s), I would like the money to be deposited into the
□ Primary Account Or

□ **STOP DIRECT DEPOSIT** (I authorize Montefiore Nyack Hospital to terminate my direct deposit. I acknowl
Bank Name: ____________
Routing#: ____________
Account#: ____________

□ **CHANGE DIRECT DEPOSIT**
Bank Name: ____________
Change Request:

COMMENTS SECTION:

REQUIRED APPROVAL
I authorize Montefiore Nyack Hospital, hereinafter referred to as COMPANY, to initiate credit entries and to initiate, if necessary, debit entries and adjustments for any credit entries in error to my account indicated above and the depository named above, hereinafter called DEPOSITORY, to credit and/or debit the same to such account. This authority is to remain in full force and effect until COMPANY has received written notification from me of its termination in such time and in such manner as to afford COMPANY and DEPOSITORY a reasonable opportunity to act on it.

SIGNATURE: ____________ DATE: ____________
PHONE #: ____________

HR OFFICE USE:
□ Employee ID reviewed (ID Badge/Photo ID) HR Staff Initials: ____________ Date: ____________

[redacted]
MEDICINE of THE HIGHEST ORDER

Direct Deposit Authorization Form

I hereby authorize St. James Hospital/ER Select to directly deposit my pay in the bank account(s) listed below in the percentages specified. (If two accounts are designated, deposits are to be made in whole percentages of pay to total 100%.) I have attached a voided personalized check (checking accounts) or deposit slip (savings accounts) for each account specified below. This authorization is to remain in force until the Company has received written authorization from me of its termination or change. Also, I hereby grant St. James Hospital the right to correct any such electronic funds transfer resulting from an erroneous overpayment by debiting my account to the extent of such overpayment.

Name (PRINT):____________

Signature: ____________ Date: ____________

Account #1 (Check only one)
[] Checking (attached voided check)
[] Savings (attach deposit slip and obtain ABA routing number from your bank)

Financial Institution: ____________

Street Address: ____________

City, State and Zip Code: ____________

Telephone: (_____) ____________

Personal Account Number: ____________

ABA (Routing) Number: ____________

Amount of pay to be deposited into this account:
$____________ or ________%

Account #2 (Check only one)
[] Checking (attached voided check)
[] Savings (attach deposit slip and obtain ABA routing number from your bank)

Financial Institution: ____________

Street Address: ____________

City, State and Zip Code: ____________

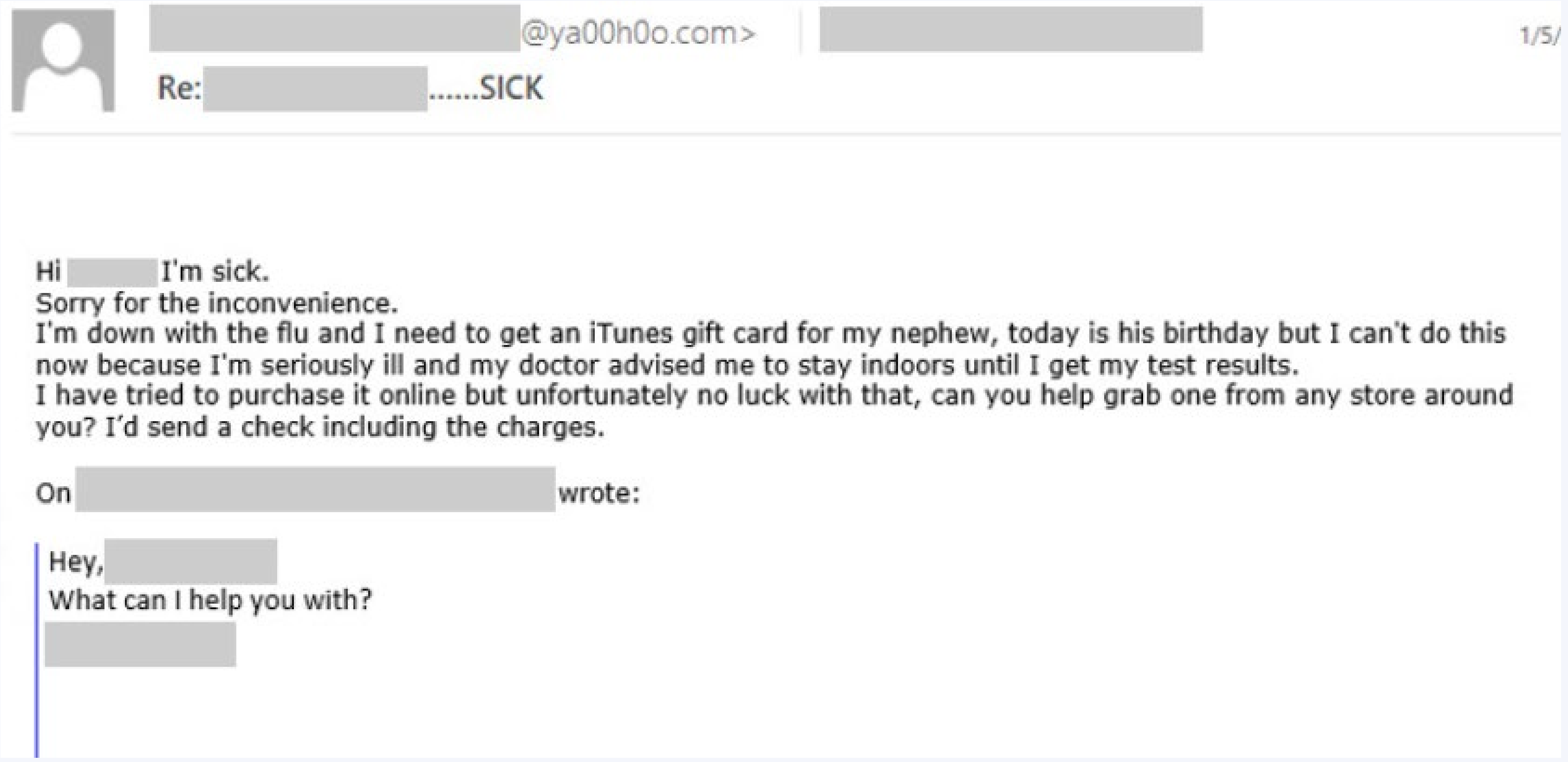
Telephone: (_____) ____________

Personal Account Number: ____________

ABA (Routing) Number: ____________

Amount of pay to be deposited into this account:
$____________ or ________%

Gift Card Scams



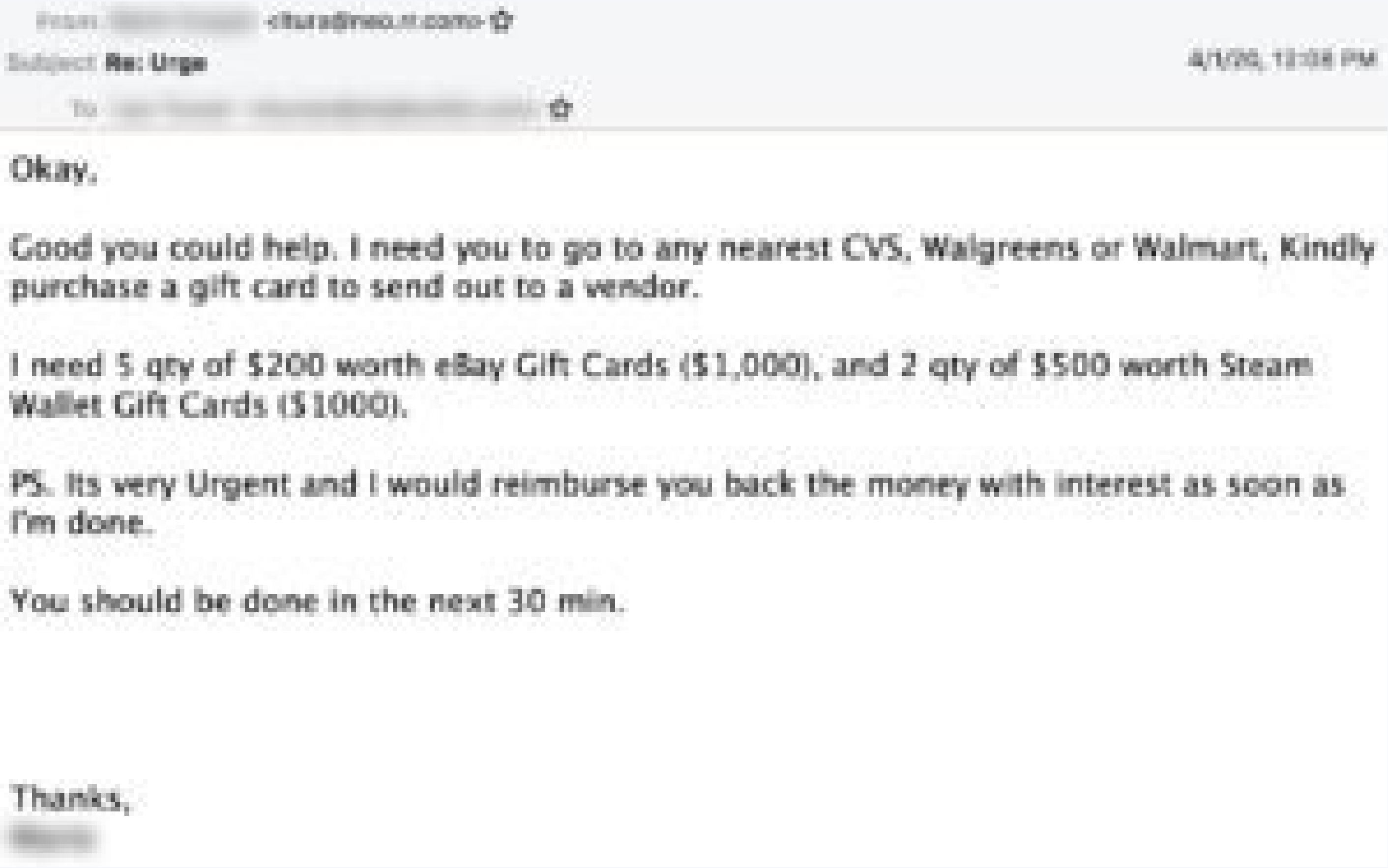
[redacted]@ya00h0o.com> [redacted] 1/5/

Re: [redacted]......SICK

Hi [redacted] I'm sick.
Sorry for the inconvenience.
I'm down with the flu and I need to get an iTunes gift card for my nephew, today is his birthday but I can't do this now because I'm seriously ill and my doctor advised me to stay indoors until I get my test results.
I have tried to purchase it online but unfortunately no luck with that, can you help grab one from any store around you? I'd send a check including the charges.

On [redacted] wrote:

> Hey, [redacted]
> What can I help you with?
> [redacted]



From: [redacted] <ltura@neo.rr.com> ✩
Subject: Re: Urge
4/1/20, 12:08 PM
To: [redacted] ✩

Okay,

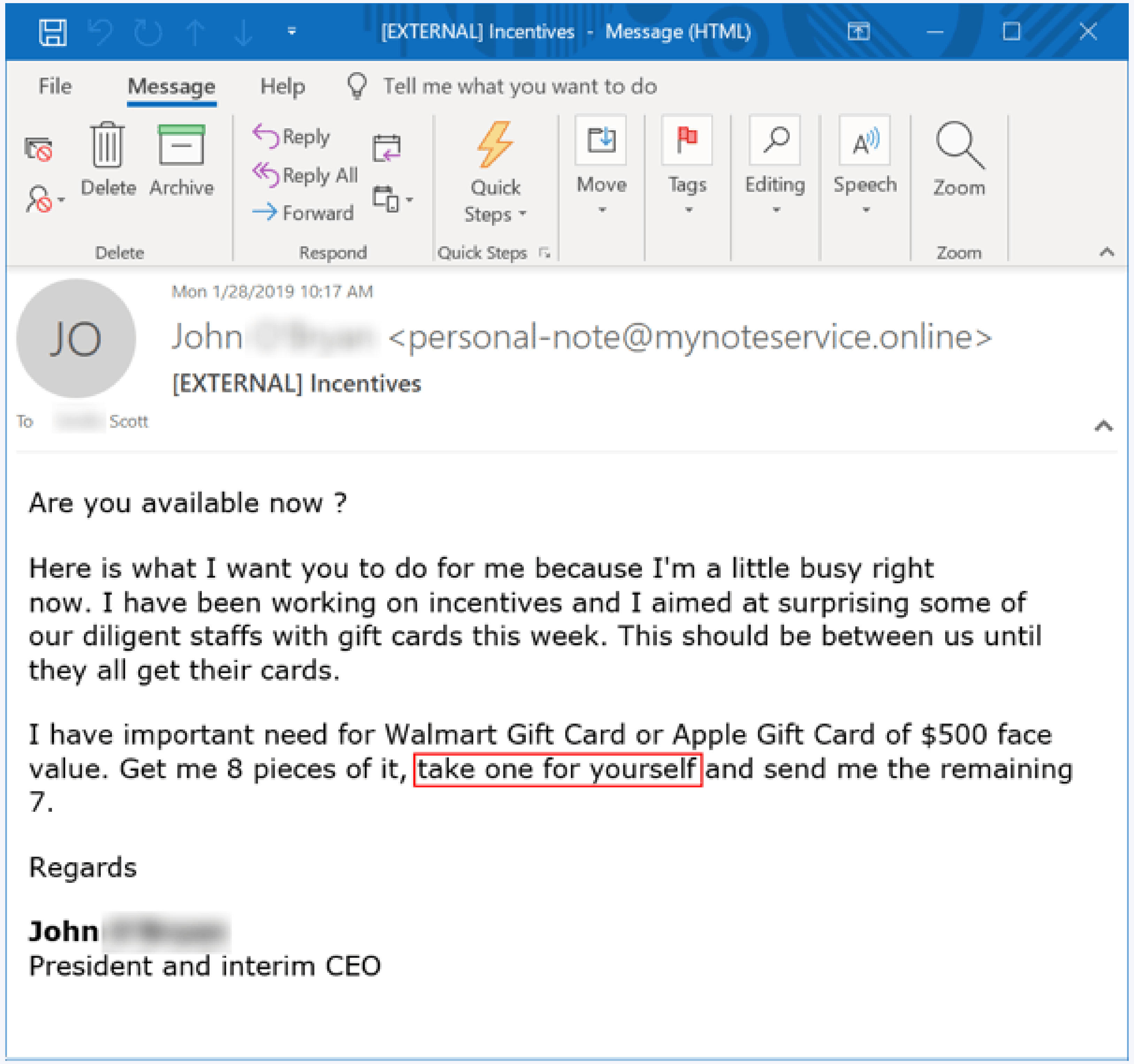
Good you could help. I need you to go to any nearest CVS, Walgreens or Walmart, Kindly purchase a gift card to send out to a vendor.

I need 5 qty of $200 worth eBay Gift Cards ($1,000), and 2 qty of $500 worth Steam Wallet Gift Cards ($1000).

PS. Its very Urgent and I would reimburse you back the money with interest as soon as I'm done.

You should be done in the next 30 min.

Thanks,
[redacted]



Mon 1/28/2019 10:17 AM
JO
John [redacted] <personal-note@mynoteservice.online>
[EXTERNAL] Incentives
To [redacted] Scott

Are you available now ?

Here is what I want you to do for me because I'm a little busy right now. I have been working on incentives and I aimed at surprising some of our diligent staffs with gift cards this week. This should be between us until they all get their cards.

I have important need for Walmart Gift Card or Apple Gift Card of $500 face value. Get me 8 pieces of it, take one for yourself and send me the remaining 7.

Regards

John [redacted]
President and interim CEO

Business Email Compromise

Healthcare and Public Health Sector

Social engineering attacks increased by **279%** in 2023

Business email compromise increased **167%** in 2023

Average cost of BEC is **$135,000**

Business Email Compromise

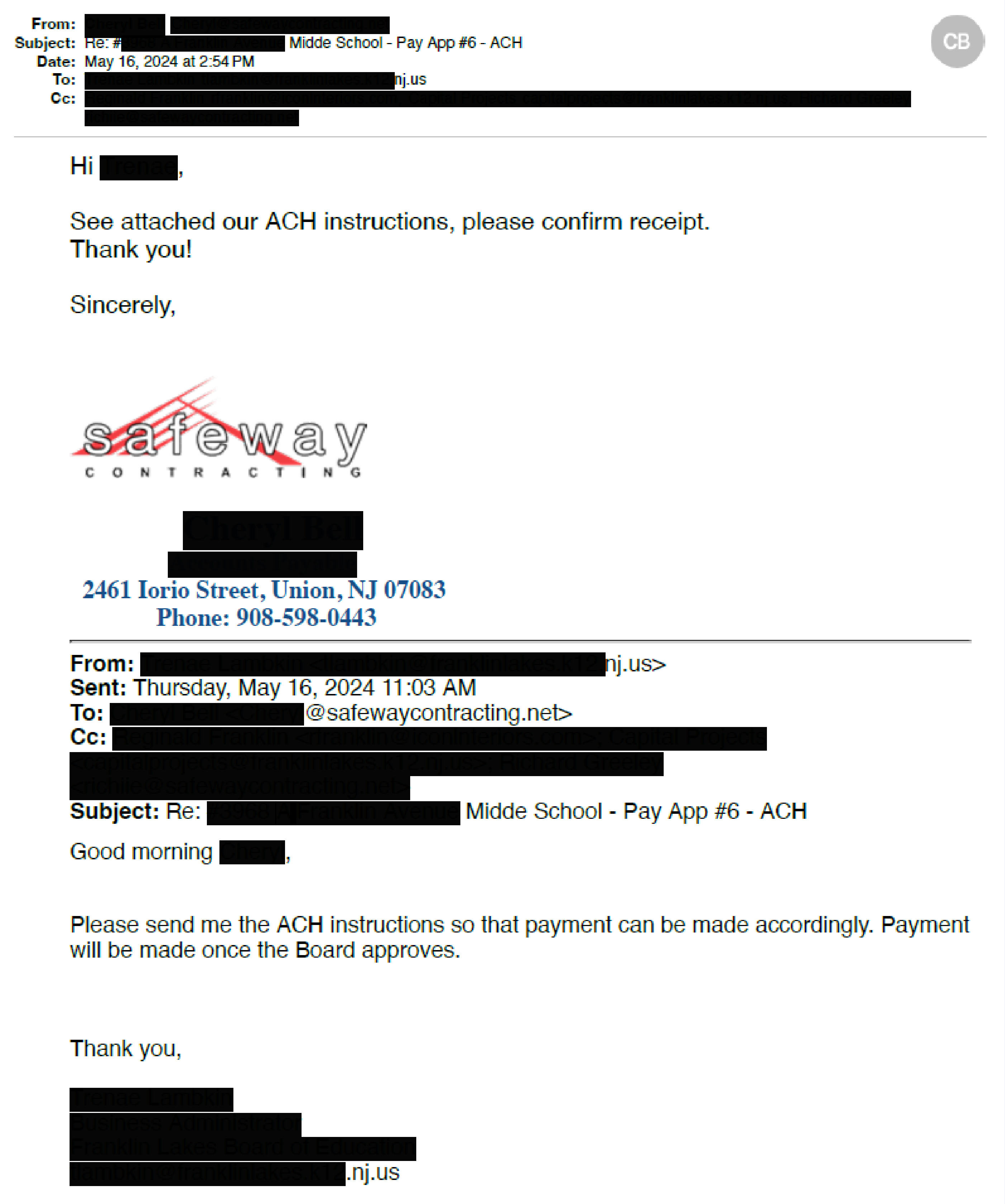
Why is BEC So Prevalent?

- Threat actor simply asks for something (money usually).
- No malicious links or attachments are included.
- Impersonation is easy – display name spoofing, stolen branding, etc.
- In public sector, so much information is publicly available.
- Procedural changes could thwart attempts.

Business Email Compromise

Recent Incident:

- School received email from vendor regarding a payment due.
- Instructed to ACH the payment as they could not process checks at that time.
- A >$100,000 payment was initiated to a fraudulent account.
- Luckily, the school realized the malicious attempt and went through their bank to reverse the transfer.
- The vendor email account had been compromised.



From: [redacted] [redacted]
Subject: Re: #[redacted] Midde School - Pay App #6 - ACH
Date: May 16, 2024 at 2:54 PM
To: [redacted]nj.us
Cc: [redacted]

Hi [redacted],

See attached our ACH instructions, please confirm receipt.
Thank you!

Sincerely,

safeway
CONTRACTING

[redacted]

2461 Iorio Street, Union, NJ 07083
Phone: 908-598-0443

From: [redacted]nj.us>
Sent: Thursday, May 16, 2024 11:03 AM
To: [redacted]@safewaycontracting.net>
Cc: [redacted]
Subject: Re: [redacted] Midde School - Pay App #6 - ACH

Good morning [redacted],

Please send me the ACH instructions so that payment can be made accordingly. Payment will be made once the Board approves.

Thank you,

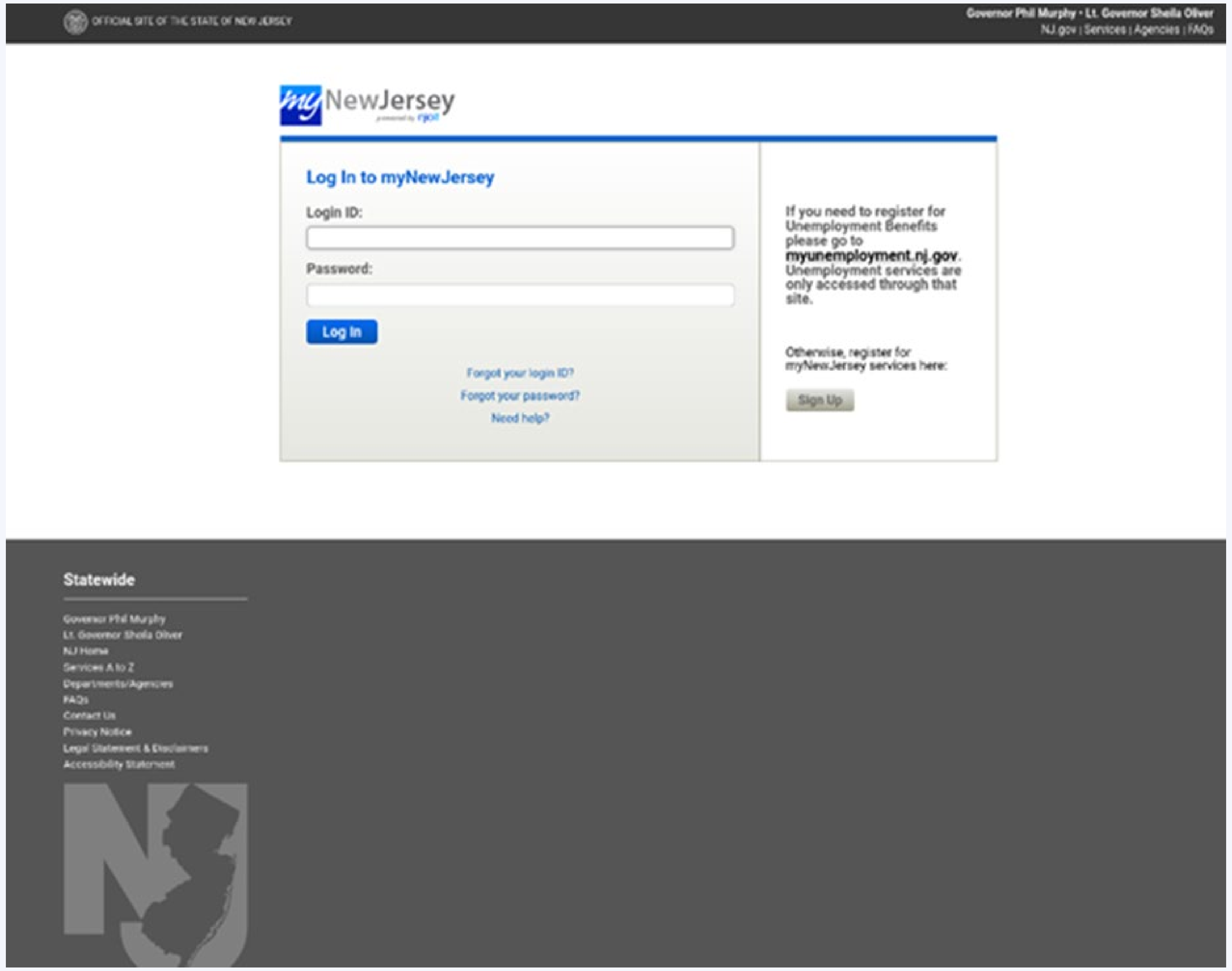
[redacted]
[redacted].nj.us

Credential Compromise

To help protect your privacy, PowerPoint has blocked automatic download of this picture.

Tricking Users

To help protect your privacy, PowerPoint has blocked automatic download of this picture.



Log In to myNewJersey

Login ID:

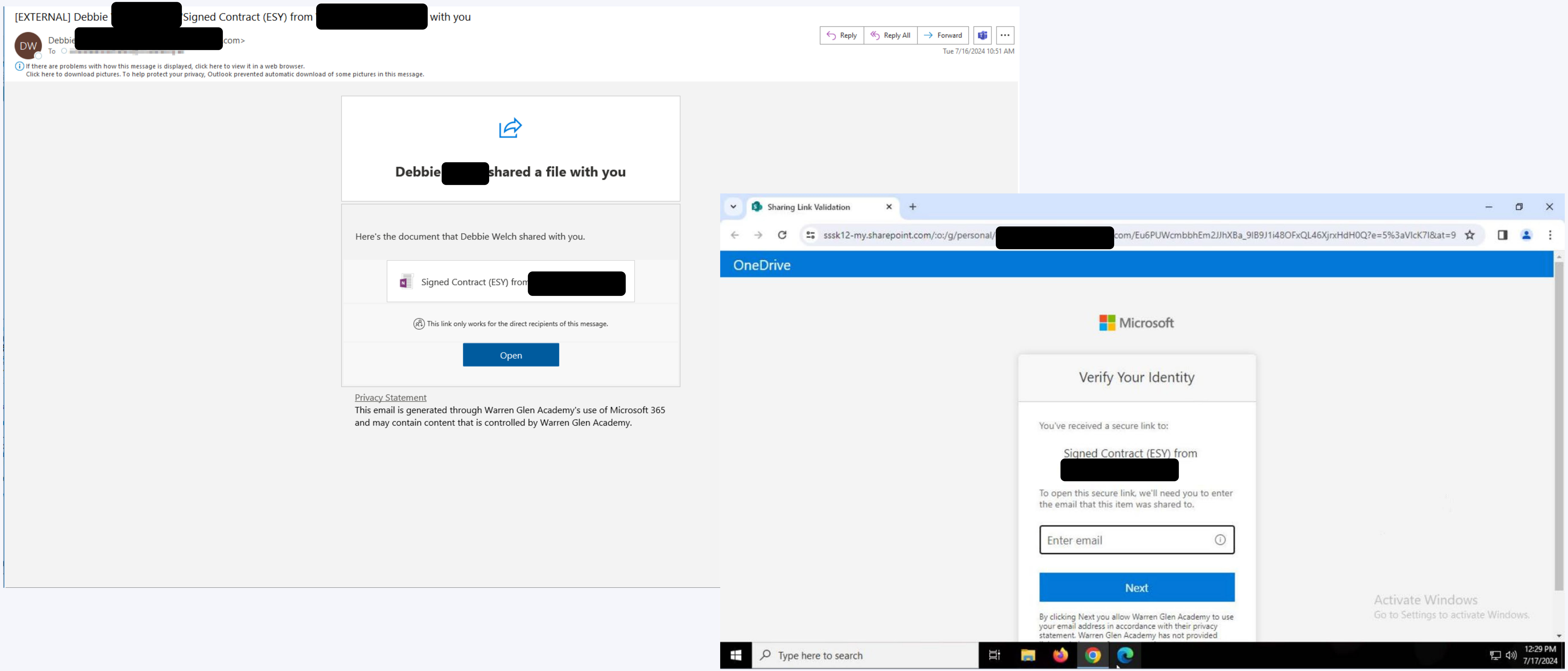
Password:

If you need to register for Unemployment Benefits please go to **myunemployment.nj.gov**. Unemployment services are only accessed through that site.

Otherwise, register for myNewJersey services here:

http://my-state-nj-us.plusandminues.com

Compromised Accounts



[EXTERNAL] Debbie [redacted] Signed Contract (ESY) from [redacted] with you

Debbie [redacted] com>

To

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.

Tue 7/16/2024 10:51 AM

Debbie [redacted] shared a file with you

Here's the document that Debbie Welch shared with you.

Signed Contract (ESY) from [redacted]

This link only works for the direct recipients of this message.

Privacy Statement
This email is generated through Warren Glen Academy's use of Microsoft 365 and may contain content that is controlled by Warren Glen Academy.

sssk12-my.sharepoint.com/:o:/g/personal/[redacted]com/Eu6PUWcmbbhEm2JJhXBa_9IB9J1i48OFxQL46XjrxHdH0Q?e=5%3aVlcK7I&at=9

Verify Your Identity

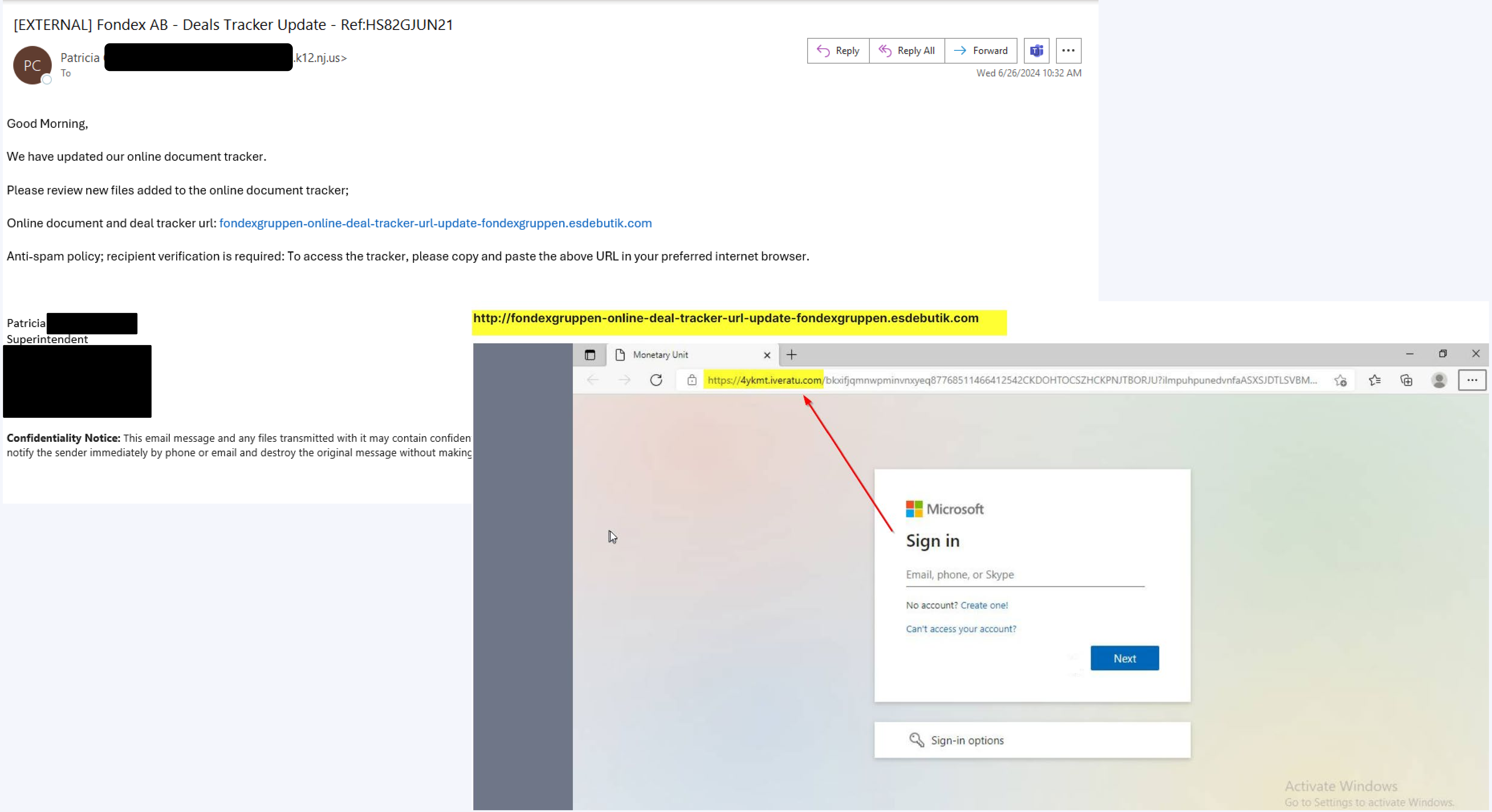
You've received a secure link to:

Signed Contract (ESY) from
[redacted]

To open this secure link, we'll need you to enter the email that this item was shared to.

Enter email

By clicking Next you allow Warren Glen Academy to use your email address in accordance with their privacy statement. Warren Glen Academy has not provided



[EXTERNAL] Fondex AB - Deals Tracker Update - Ref:HS82GJUN21

Patricia [redacted].k12.nj.us>
To

Wed 6/26/2024 10:32 AM

Good Morning,

We have updated our online document tracker.

Please review new files added to the online document tracker;

Online document and deal tracker url: fondexgruppen-online-deal-tracker-url-update-fondexgruppen.esdebutik.com

Anti-spam policy; recipient verification is required: To access the tracker, please copy and paste the above URL in your preferred internet browser.

Patricia [redacted]
Superintendent
[redacted]

Confidentiality Notice: This email message and any files transmitted with it may contain confiden
notify the sender immediately by phone or email and destroy the original message without making

http://fondexgruppen-online-deal-tracker-url-update-fondexgruppen.esdebutik.com

Monetary Unit

https://4ykmt.iveratu.com/bkxifjqmnwpminvnxyeq87768511466412542CKDOHTOCSZHCKPNJTBORJU?ilmpuhpunedvnfaASXSJDTLSVBM...

Microsoft

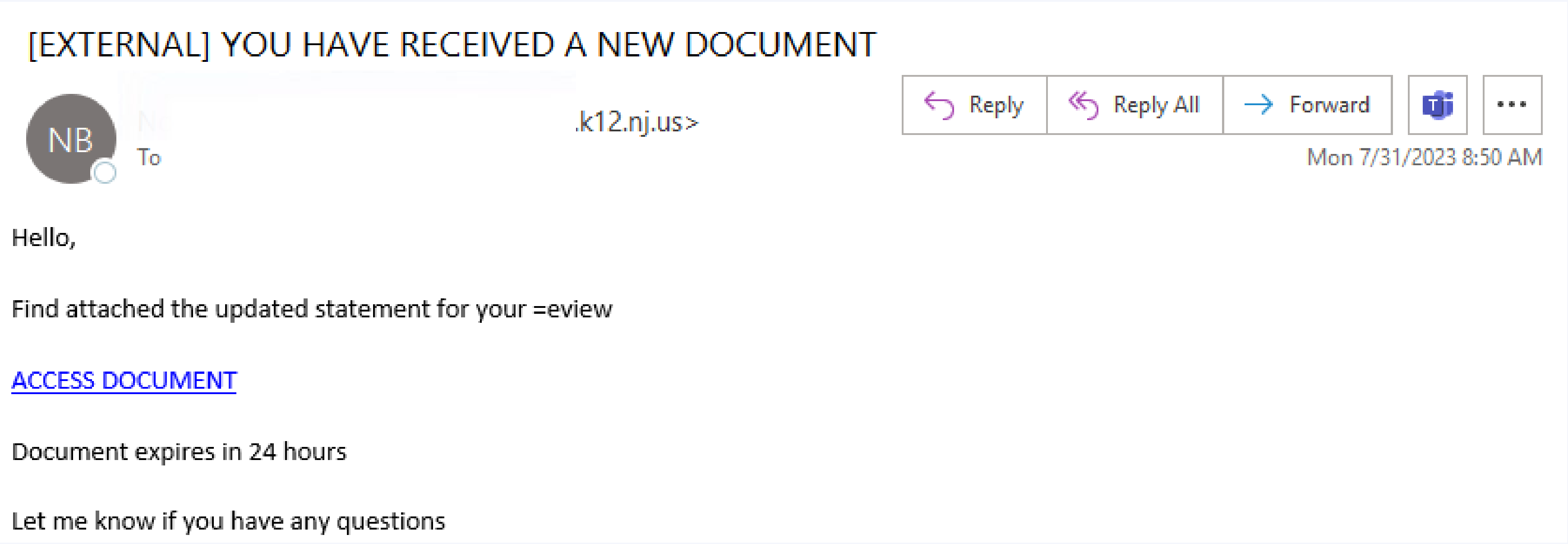
Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Using Compromised Accounts



[EXTERNAL] YOU HAVE RECEIVED A NEW DOCUMENT

[redacted] .k12.nj.us>

To

Mon 7/31/2023 8:50 AM

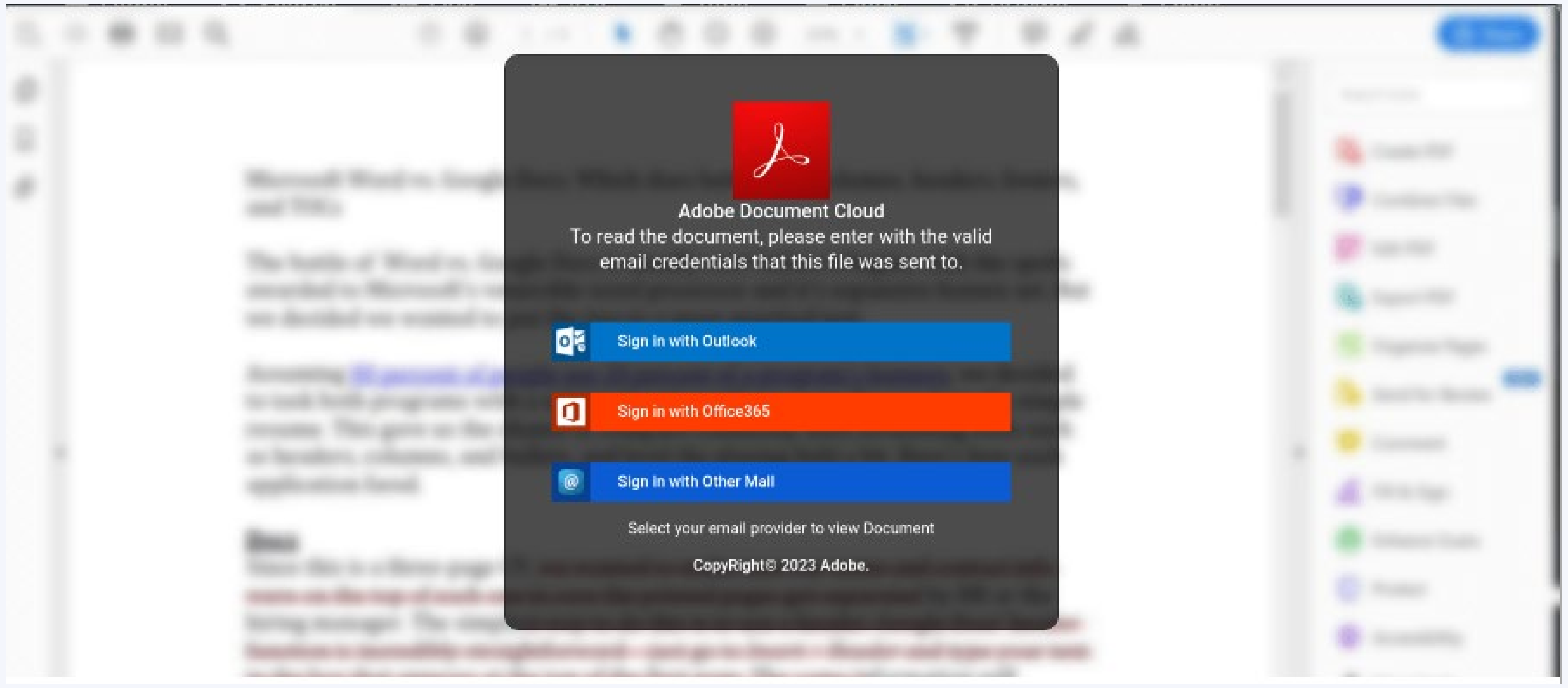
Hello,

Find attached the updated statement for your =eview

ACCESS DOCUMENT

Document expires in 24 hours

Let me know if you have any questions

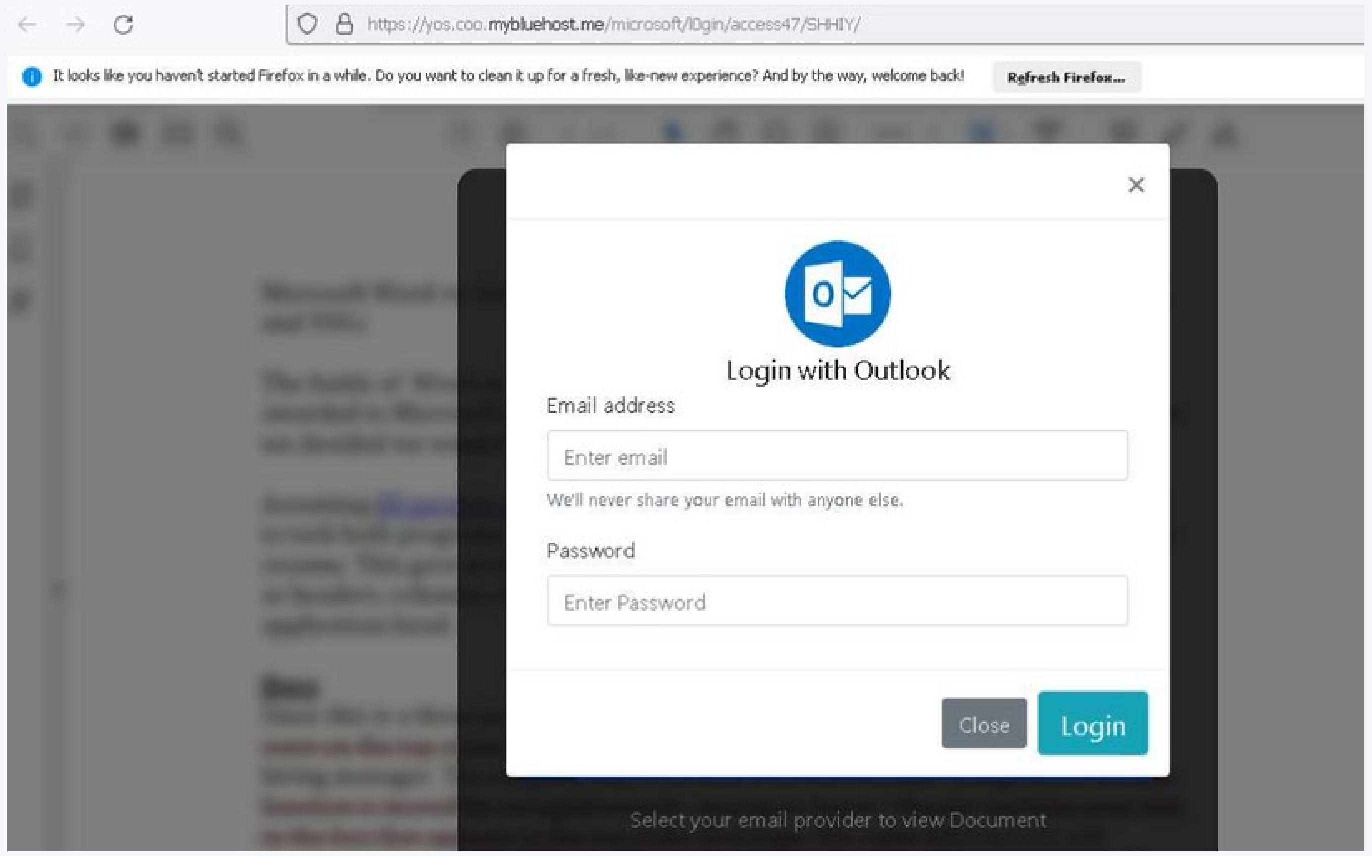


Adobe Document Cloud

To read the document, please enter with the valid email credentials that this file was sent to.

Select your email provider to view Document

CopyRight© 2023 Adobe.



https://yos.coo.mybluehost.me/microsoft/l0gin/access47/SHHIY/

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Login with Outlook

Email address

Enter email

We'll never share your email with anyone else.

Password

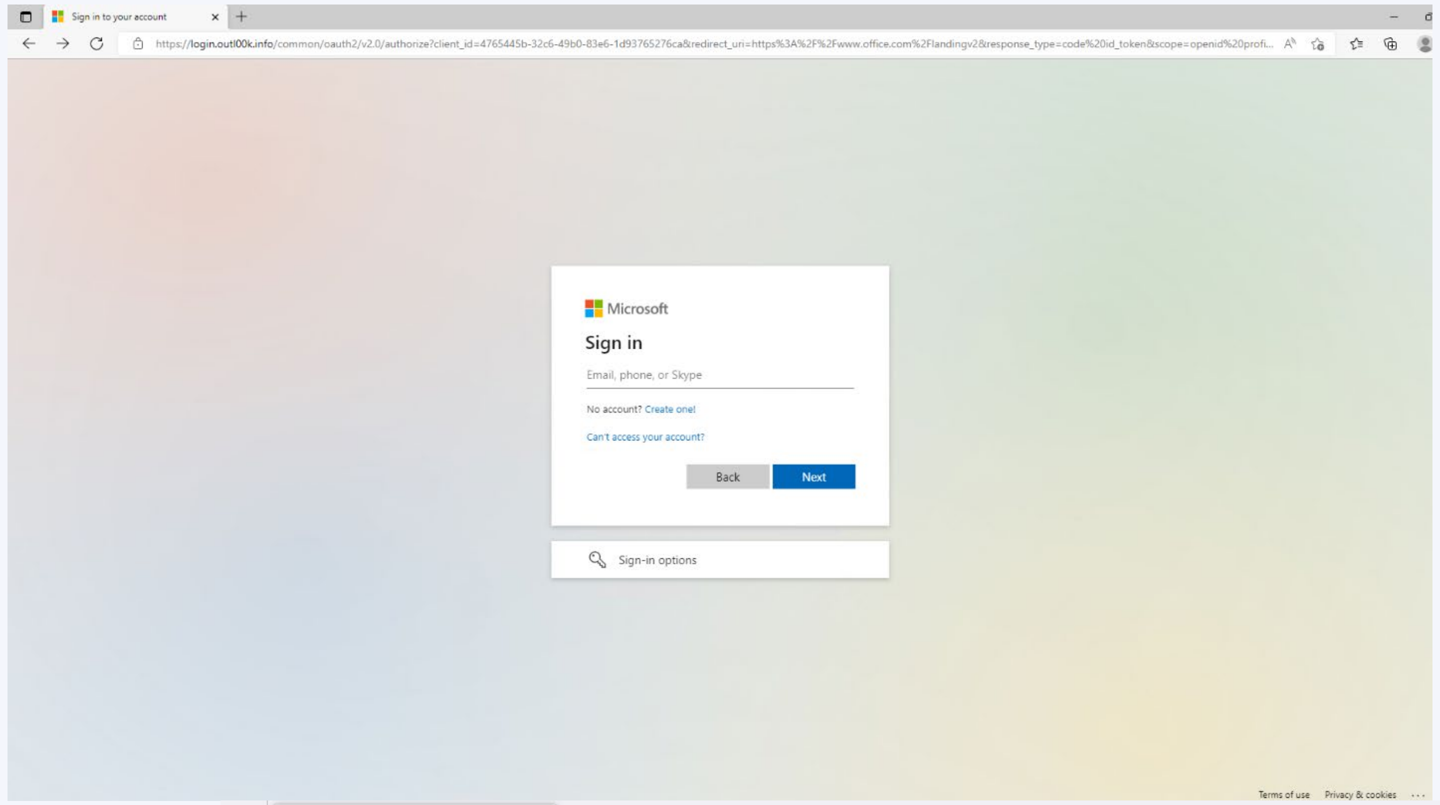
Enter Password

Select your email provider to view Document

YOU OFTEN ARE DIRECTED TO A WEBPAGE REQUESTING YOU TO LOG IN TO VIEW A DOCUMENT OR MESSAGE.

IF CREDENTIALS ARE ENTERED, THEY'RE STOLEN. THEN YOUR ACCOUNT IS COMPROMISED TOO.

Attempting to Bypass MFA


Sign in to your account
https://login.outl00k.info/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fwww.office.com%2Flandingv2&response_type=code%20id_token&scope=openid%20profi...
Back
Next
Terms of use
Privacy & cookies

Microsoft

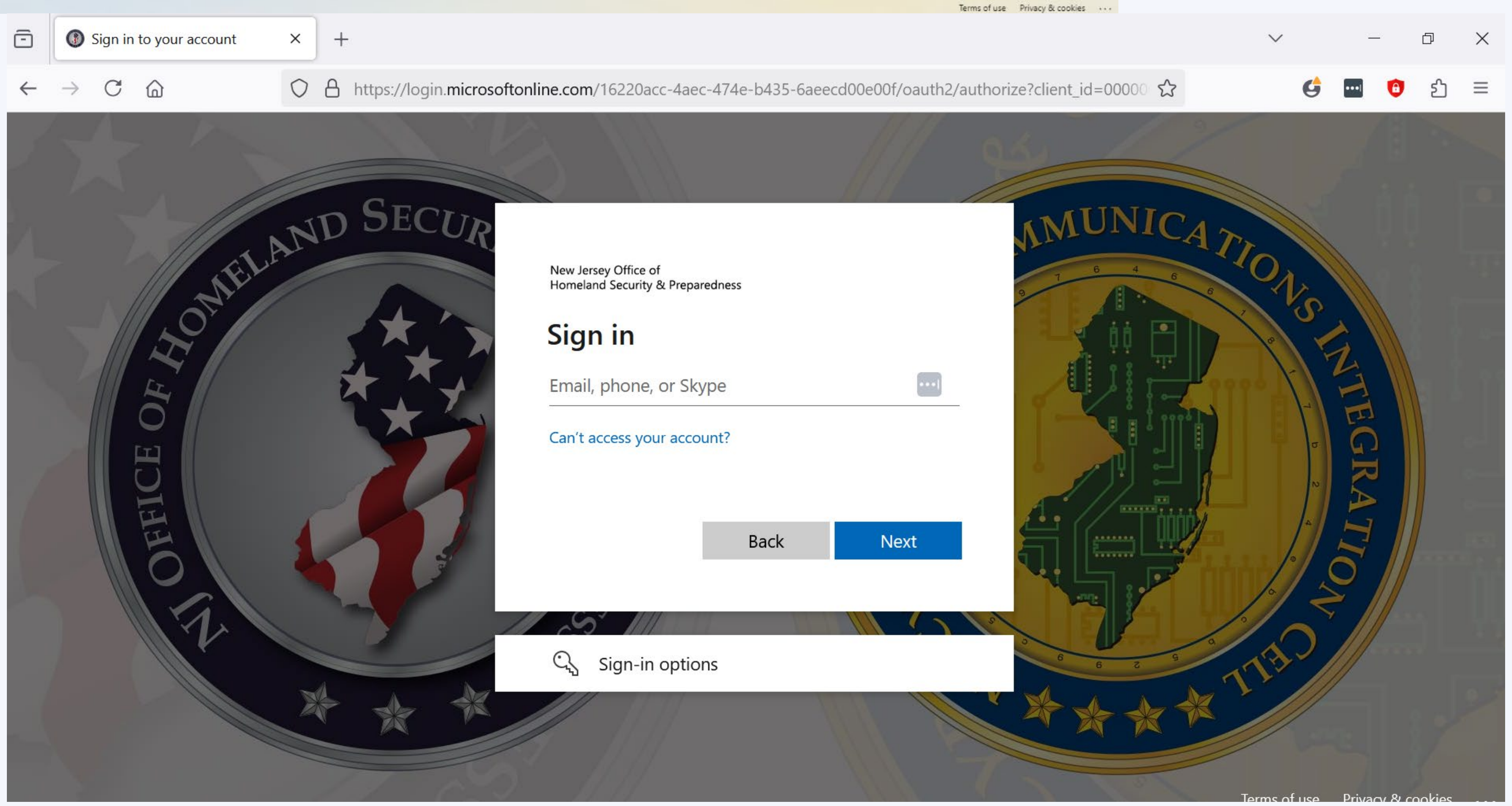
Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Sign-in options


Sign in to your account
https://login.microsoftonline.com/16220acc-4aec-474e-b435-6aeecd00e00f/oauth2/authorize?client_id=0000
Back
Next
Terms of use
Privacy & cookies

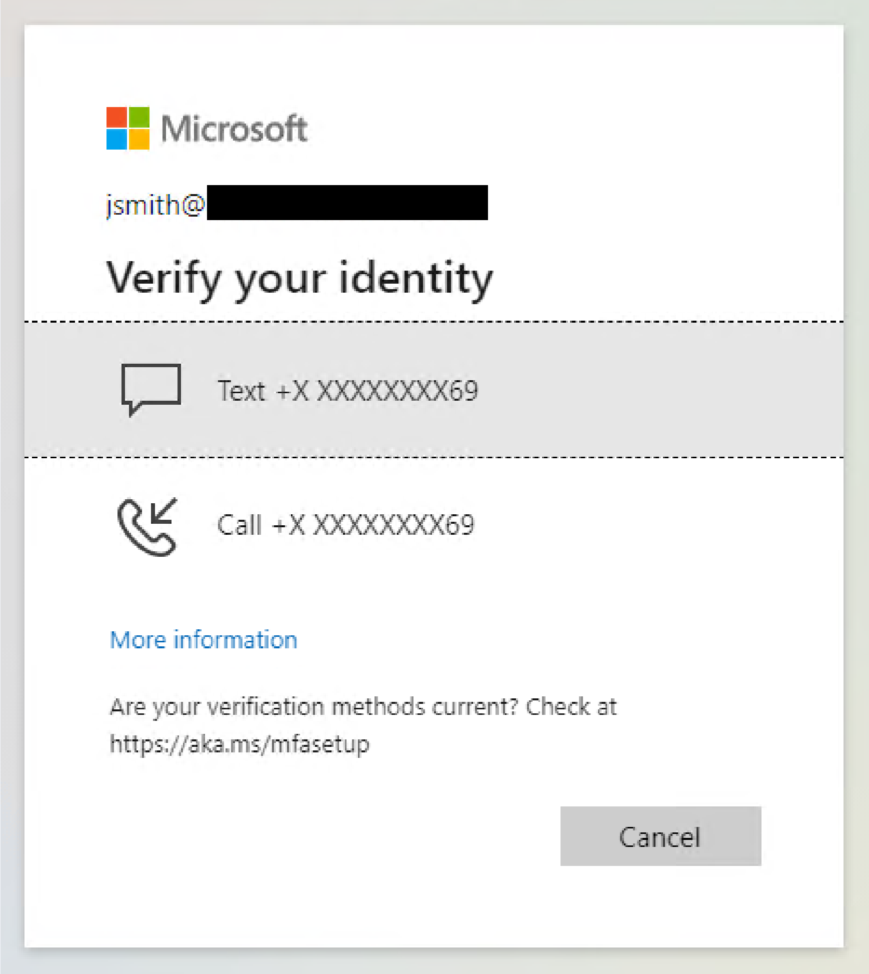
New Jersey Office of
Homeland Security & Preparedness

Sign in

Email, phone, or Skype

Can't access your account?

Sign-in options



Microsoft

jsmith@[redacted]

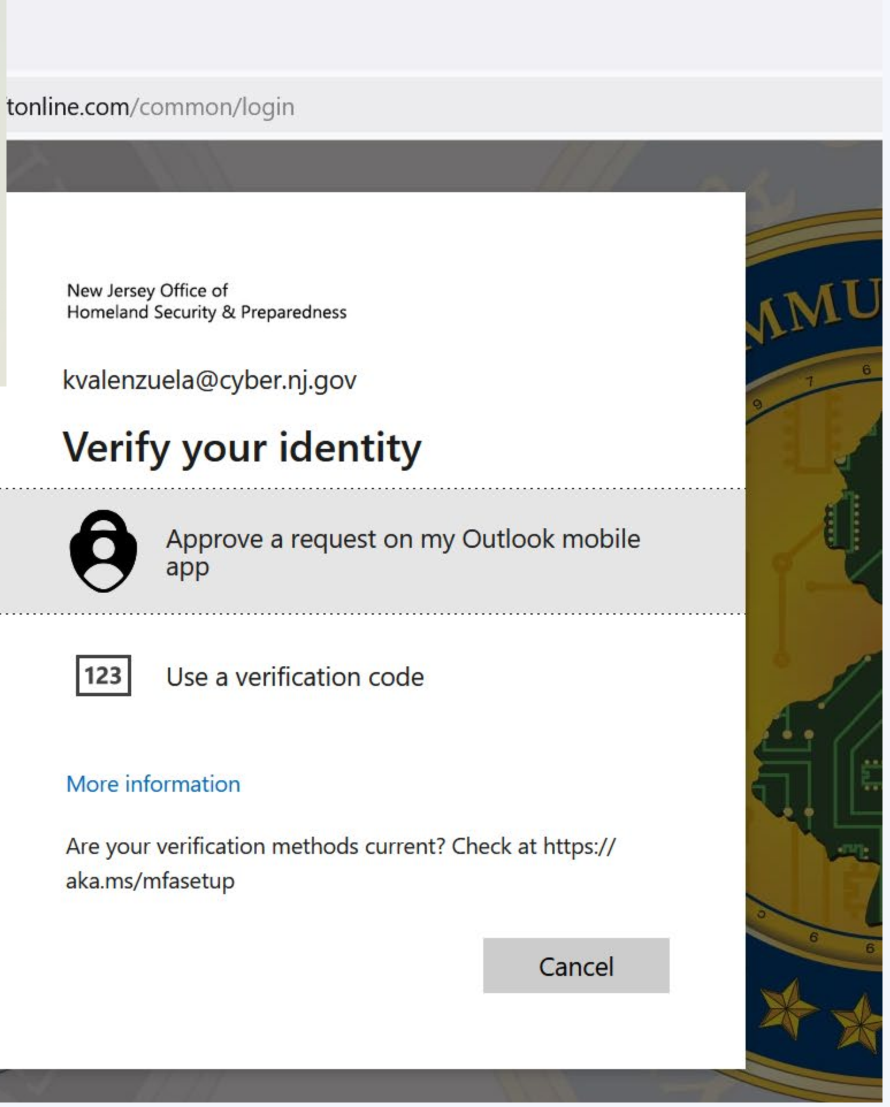
Verify your identity

Text +X XXXXXXXX69

Call +X XXXXXXXX69

More information

Are your verification methods current? Check at https://aka.ms/mfasetup



New Jersey Office of
Homeland Security & Preparedness

kvalenzuela@cyber.nj.gov

Verify your identity

Approve a request on my Outlook mobile app

123 Use a verification code

More information

Are your verification methods current? Check at https://aka.ms/mfasetup

Credential Compromise

GETTING THE KEYS TO THE KINGDOM

How many accounts do you think you have?

Do you ever reuse passwords? 👀

Account compromises often precede ransomware infections.

SO, WHAT SHOULD WE DO?

MULTI-FACTOR AUTHENTICATION

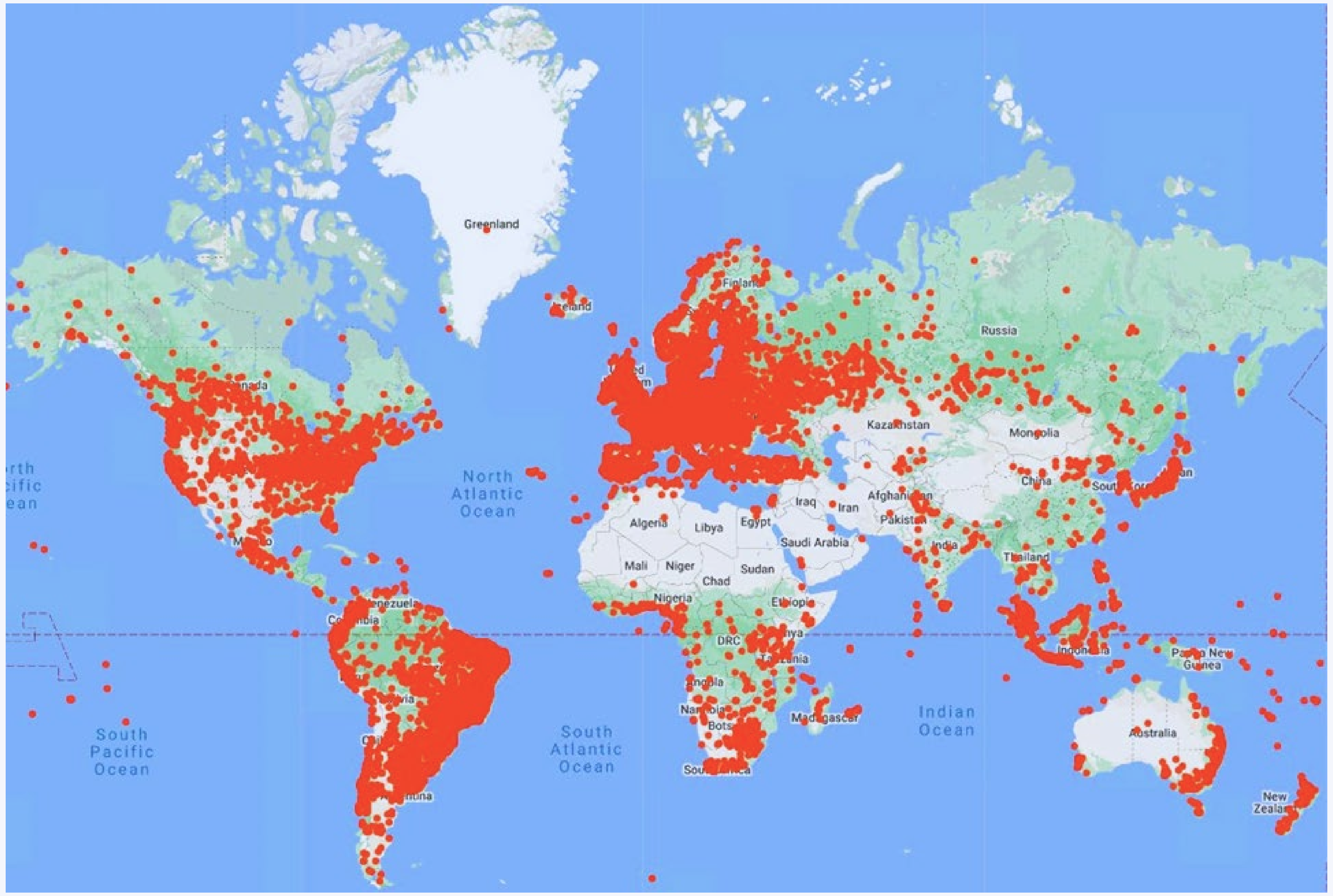
○ Something you know

○ Something you have

○ Something you are

How Are They Compromised?

GETTING THE KEYS TO THE KINGDOM



INFOSTEALERS

DATA BREACHES

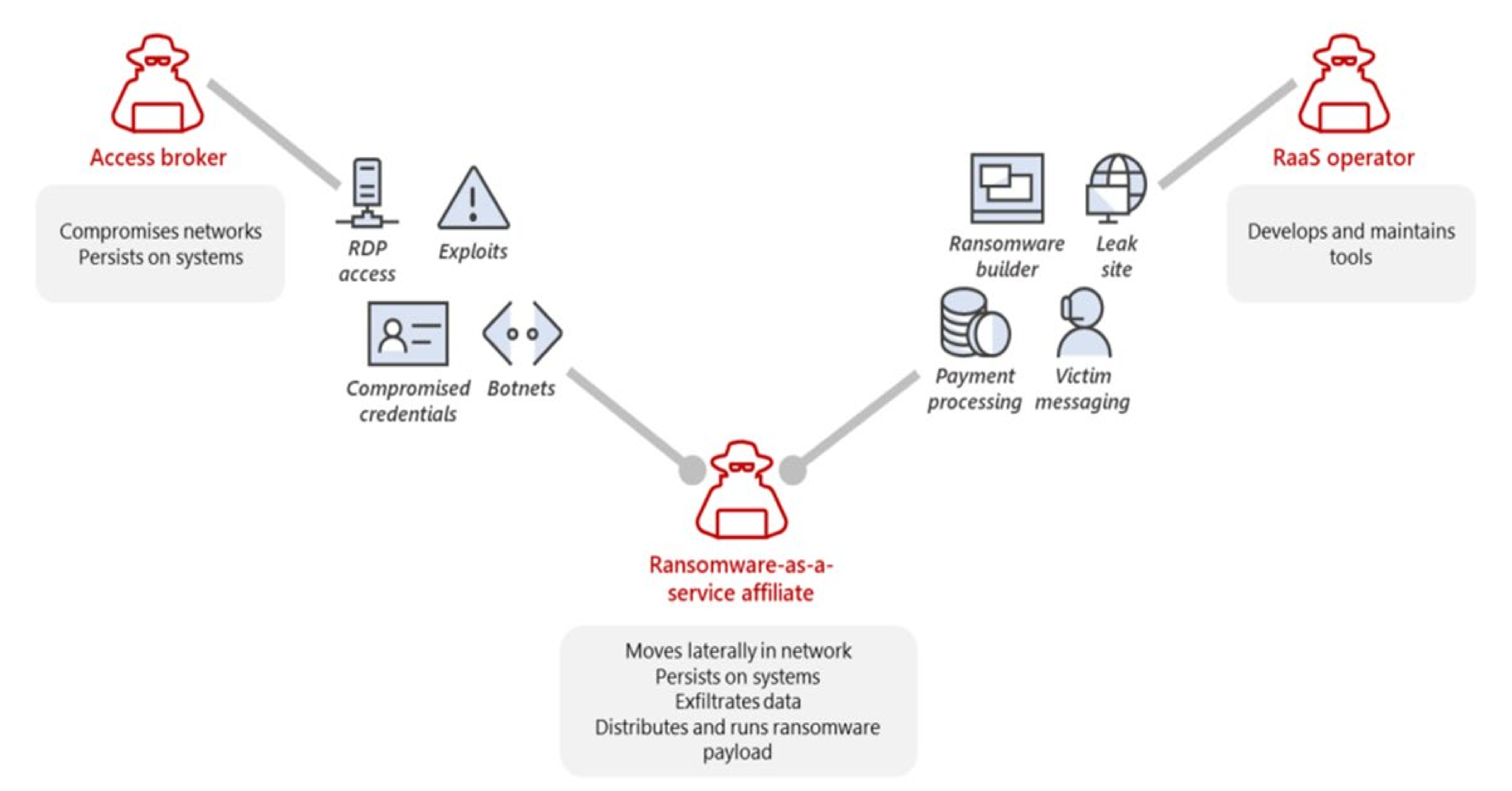
WEAK PASSWORDS

SOCIAL ENGINEERING

Infostealers

Ransomware

Ransomware-as-a-Business

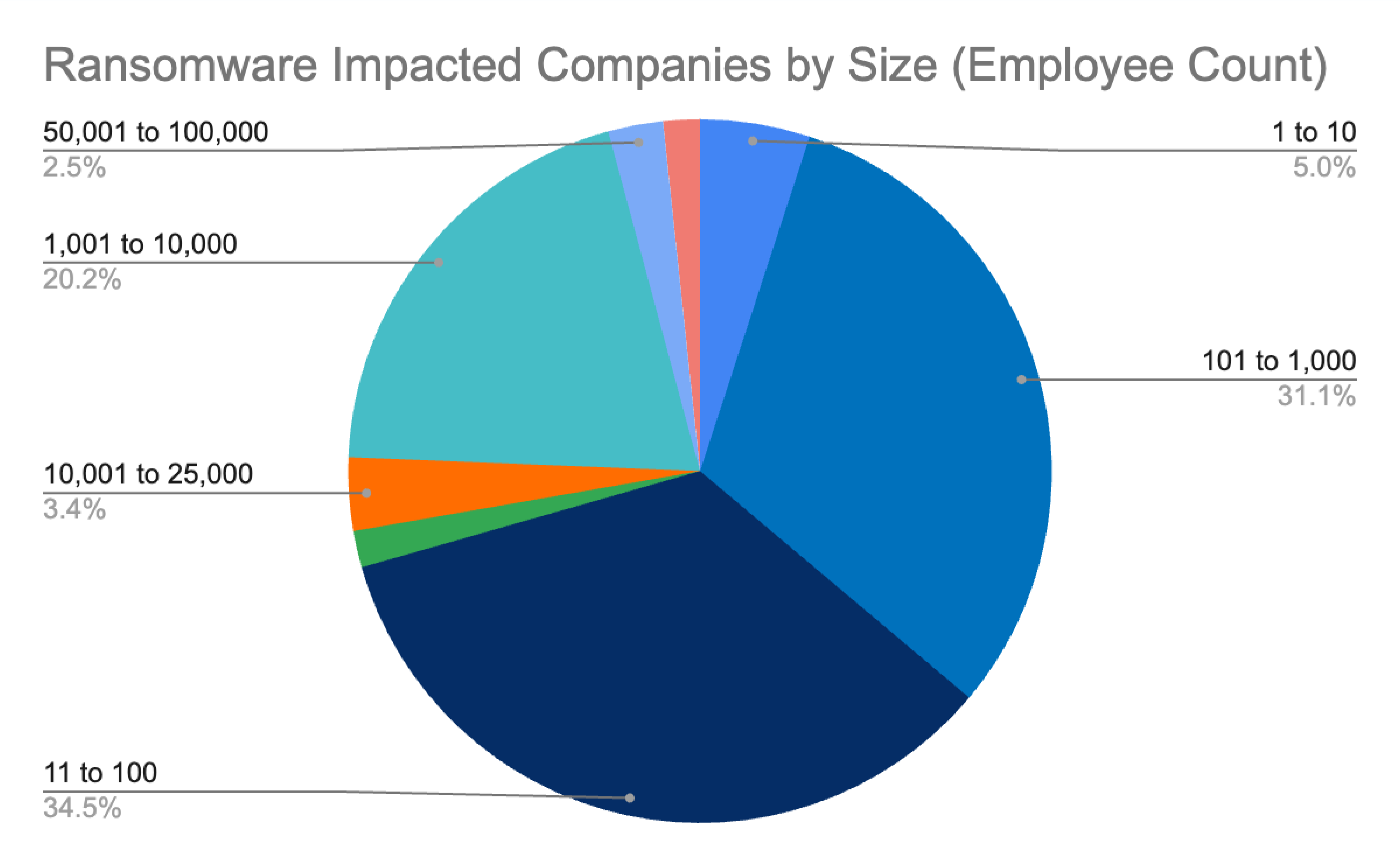


Compromises networks
Persists on systems

Develops and maintains tools

Moves laterally in network
Persists on systems
Exfiltrates data
Distributes and runs ransomware payload

Ransomware



average ransom: $390,000

avg downtime ~24 days

remote access, phishing

data exfiltration in 75% of incidents

target of opportunity

SMBs targeted

No encryption extortion

LIFECYCLE OF A RANSOMWARE INCIDENT

certnz

How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.

INITIAL ACCESS

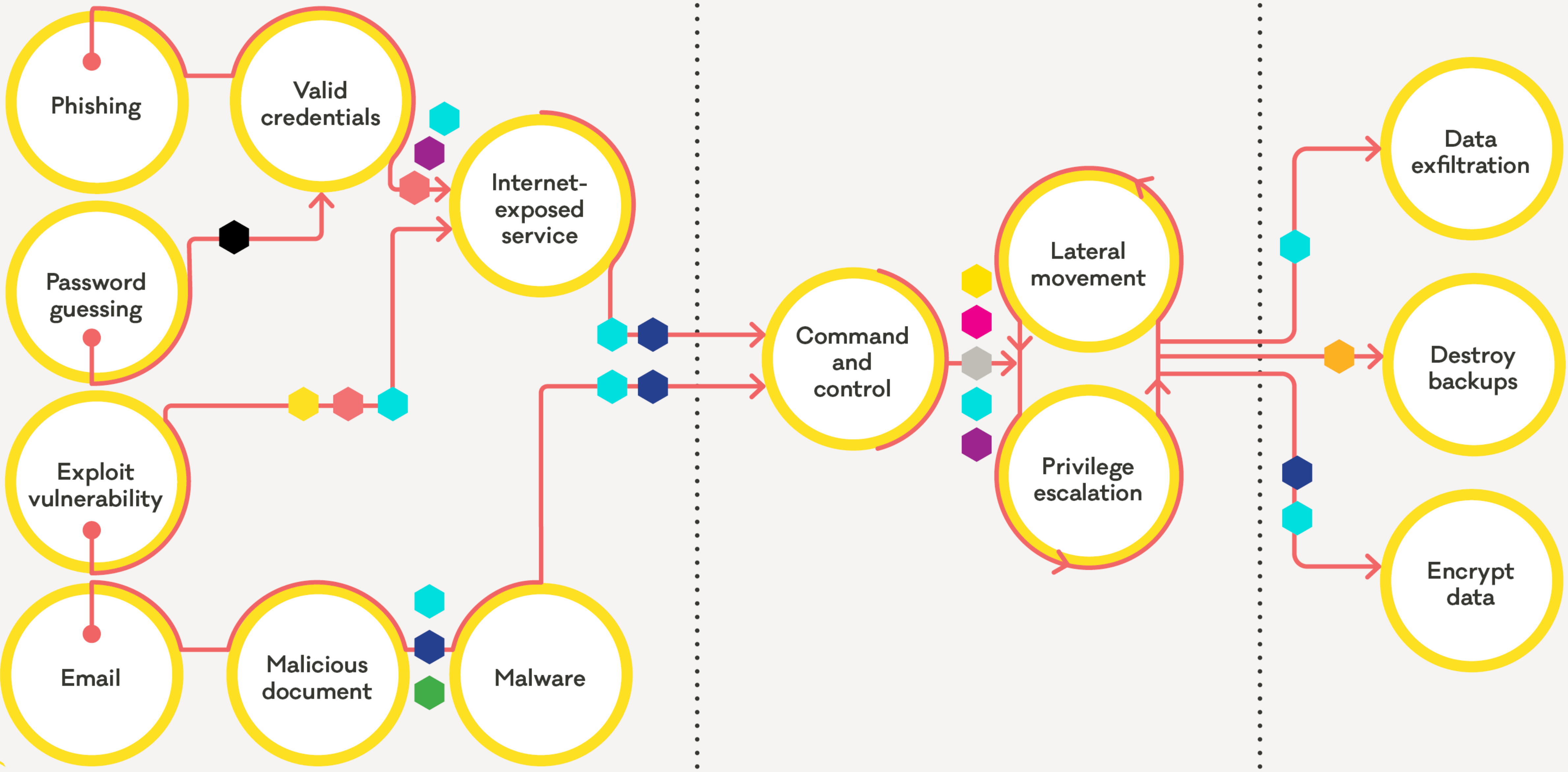
Attacker looks for a way into the network

CONSOLIDATION AND PREPARATION

Attacker attempts to gain access to all devices

IMPACT ON TARGET

Attacker steals and encrypts data, then demands ransom



CRITICAL CONTROLS KEY

- ⬢ Internet-exposed services
- ⬢ Patching
- ⬢ MFA
- ⬢ Network segmentation
- ⬢ Principle of least privilege
- ⬢ Backups
- ⬢ Application allowlisting
- ⬢ Logging and alerting
- ⬢ Disable macros
- ⬢ Password manager

New Zealand Government

Change Healthcare Incident

Change Healthcare is a provider of revenue and payment cycle management for healthcare providers and patients within the United States.

Processes about half of all medical claims in the United States for approximately 900,000 physicians, 33,000 pharmacies, 5,500 hospitals and 600 laboratories.

On **February 21** , a major ransomware attack targeted Change Healthcare.

Service were completely down from February 21 to February 26, **5 days**.

AHA predicted that **94%** of hospitals experienced a **financial** impact.

Some patients were forced to pay **out-of-pocket for prescriptions** .

Approximately **4 terabytes** of Protected Health Information (PHI) was stolen.

The culprit was the **BlackCat** ransomware group.

Who is BlackCat?

BlackCat is a Russian-based ransomware organization.

They are also known as ALPHV.

They offer a **ransomware -as-service** business model.

BlackCat offers their ransomware to third-party affiliates to infect organizations in exchange for a **percentage** of the ransom payment.

Timeline of Events

February 12:

Threat actors first access Change Healthcare network.

February 21:

Ransomware attack initiated.

March 1:

A $22 million payment sent to BlackCat cryptowallet .

March 1:

BlackCat exit Scam began by taking their data leak blog offline

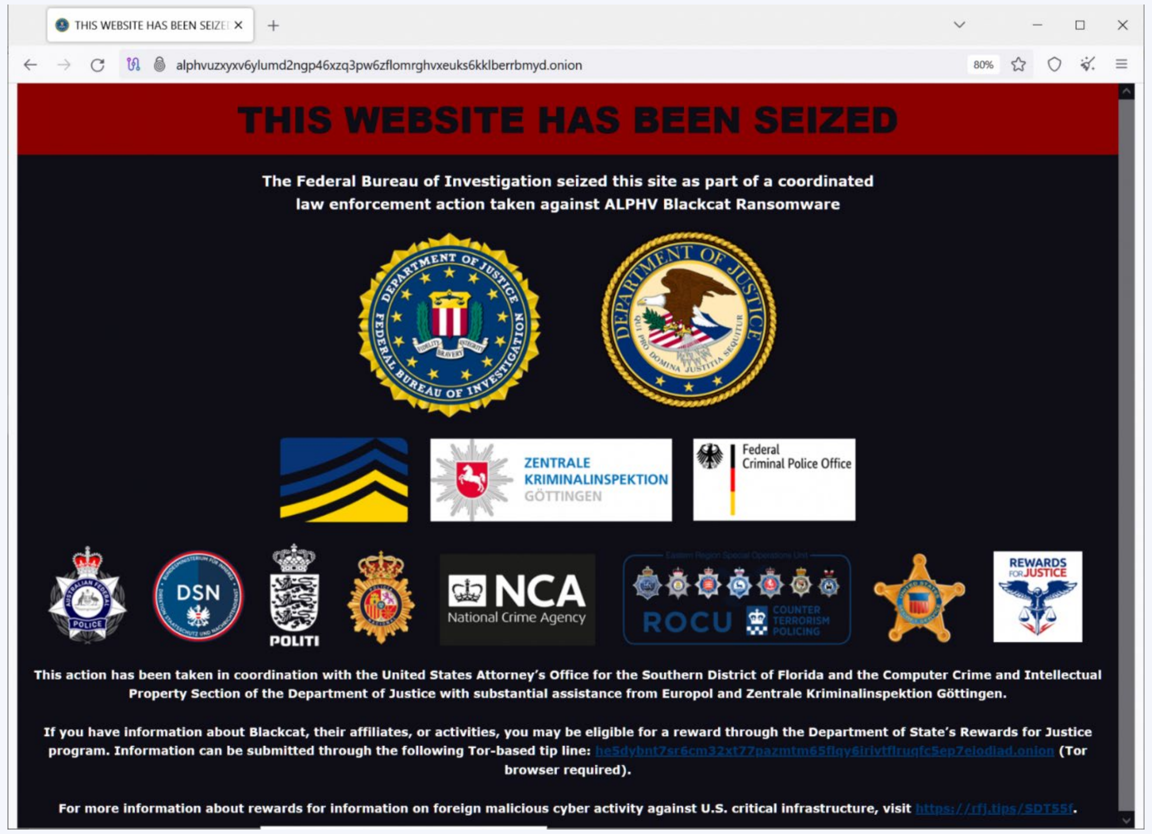
March 3:

An affiliate “Notchy,” claimed responsibility for the incident on a Russian hacking forum.

They claimed BlackCat took the money, did not pay them as an affiliate; therefore, the data would not be deleted.

March 7:

Pharmacy electronic prescribing is fully functional for claim submission and payment transmission.



THIS WEBSITE HAS BEEN SEIZED
alphvuzxyxv6ylumd2ngp46xzq3pw6zflomrghvxeuks6kklberrbmyd.onion
80%
ZENTRALE KRIMINALINSPEKTION GÖTTINGEN
Federal Criminal Police Office
DSN
POLITI
NCA National Crime Agency
ROCU COUNTER TERRORISM POLICING
REWARDS FOR JUSTICE

THIS WEBSITE HAS BEEN SEIZED

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against ALPHV Blackcat Ransomware

This action has been taken in coordination with the United States Attorney’s Office for the Southern District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol and Zentrale Kriminalinspektion Göttingen.

If you have information about Blackcat, their affiliates, or activities, you may be eligible for a reward through the Department of State’s Rewards for Justice program. Information can be submitted through the following Tor-based tip line: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion (Tor browser required).

For more information about rewards for information on foreign malicious cyber activity against U.S. critical infrastructure, visit https://rfj.tips/SDT55f.

Timeline of Events Cont.

March 15:

Forensic investigations identified the original vulnerability that acted as the initial attack vector, though United Health did not disclose the vulnerability. It is believed to be a remote access compromise of an account without MFA enforced.

March 27:

The U.S. Department of State's Rewards for Justice (RFJ) program, is offering a reward of up to $10 million dollars for information leading to the identification of BlackCat members.

April 8:

A new ransomware group known as " RansomHub" allegedly claimed that they obtained Change Healthcare's stolen data and demanded a second ransom to keep them from leaking the data.

April 16:

RansomHub began selling the stolen Change Healthcare data, which includes medical and dental records, payment claims, insurance details, and personal information such as Social Security numbers and email addresses. Post was later removed, causing speculation that a second payment was made.

Impacts

UnitedHealth stated that the ransomware incident caused **$872 million** in losses so far.
UnitedHealth reported **$1.521 billion** in direct response costs and expected **$2.87** billion in total cyberattack impacts for 2024.

The cyberattack affected at least 100 million individuals' protected health information.
Largest known breach of PHI.
Why is this significant?

Healthcare providers:
94% of all US Hospitals were financially impacted by the cyberattack.
~60% of US Hospitals lost at least $1M per day during this incident.
Physician practices (as of April 2024, issues continued after):
80 percent of physician practices lost revenue from unpaid claims
36 percent reported delays in claim repayment
Small practices (10 or fewer physicians) were hit particularly hard.

Ransomware attacks against health care organizations surged following the hack of Change Healthcare.

Artificial Intelligence

The Good and The Bad

CYBERSECURITY

GENERATIVE AI

AUTOMATION

ENHANCED CUSTOMER EXPERIENCE

REDUCTION IN HUMAN ERROR

EFFICIENCY AND EFFECTIVENESS

CYBER THREATS

AUTOMATING ATTACKS

VULNERABILITY DISCOVERY

GENERATIVE AI

VOICE REPLICATION

DISINFORMATION

RELIANCE ON TECH

Cyber Resiliency

- Data Backups
- Patch management
- Multi-Factor Authentication
- Endpoint Detection and Response
- User Awareness Training
- Password Manager
- Cybersecurity Plans
- Tabletop Exercises
- Caution with Email
- Network Segmentation
- Limit sharing of information

NJ CCIC Services

- weekly bulletin
- presentations
- cybersecurity reports
- risk management
- incident reporting
- alerts, advisories
- assessments
- grant management
- training
- cyber range

cyber.nj.gov/members

CONNECT

1-833-4-NJCCIC

KVALENZUELA@CYBER.NJ.GOV

CYBER.NJ.GOV