NJCCIC

PREVENT | DETECT | RESPOND

This presentation is TLP: CLEAR

NJCCIC Mission

To lead and coordinate New Jersey's cybersecurity efforts while building resiliency to cyber threats throughout the State.

Formed in May 2015 by Executive Order 178, (Christie, 2015)

Tasked with strategic development and execution of the State's cybersecurity efforts, which includes:

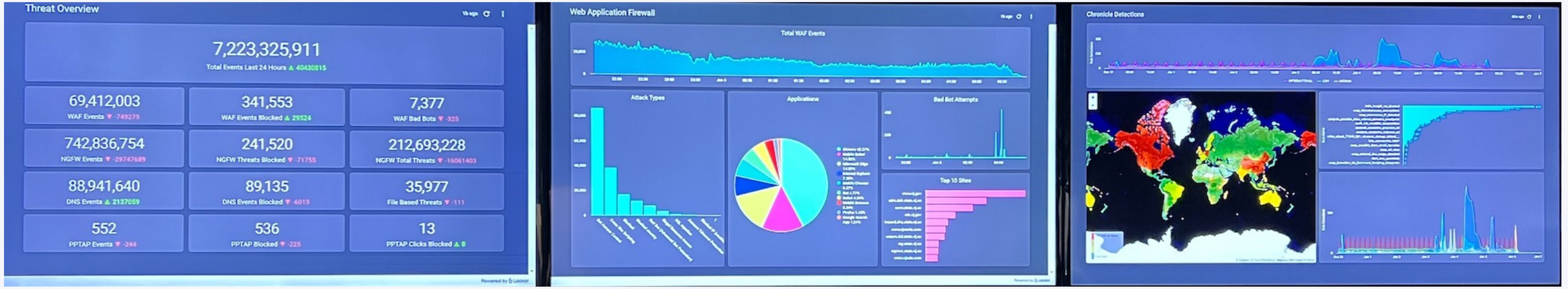
- acting as the State's one-stop shop for cybersecurity information sharing, threat intelligence, best practices, and incident reporting and response; and
- the development, management, and execution of an information security program that ensures the confidentiality, integrity, and availability of the information resources, systems, and services of the State of New Jersey Executive Branch's departments and agencies.

Organization

Governance, Risk, and Compliance

Cyber Threat Outreach and Partnerships

Security Engineering and Cyber Operations

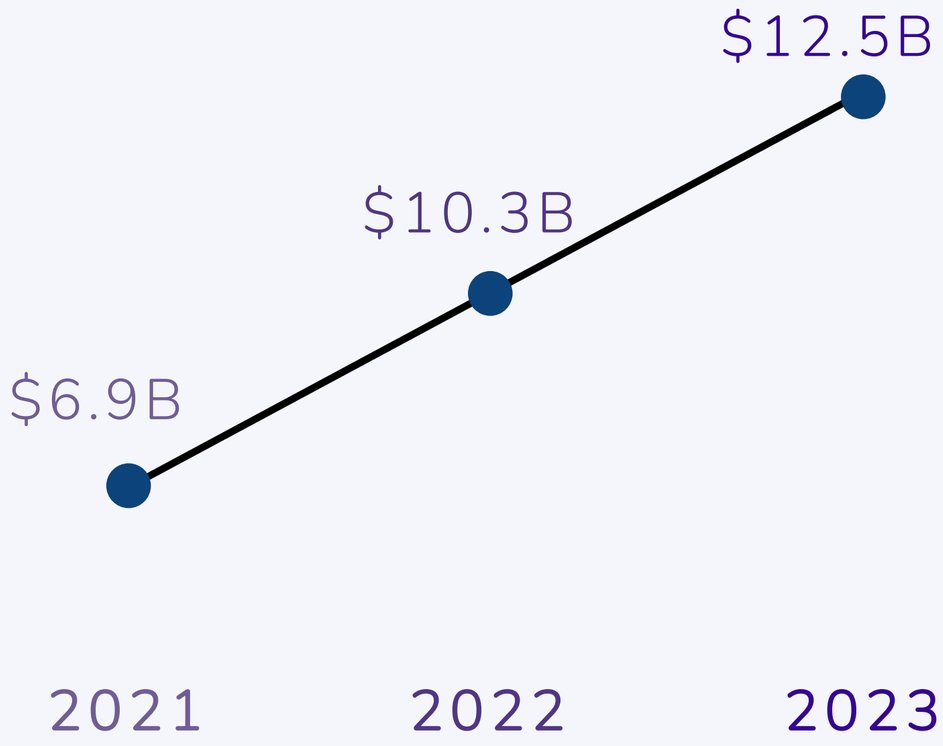


Cyber Threats & Best Practices

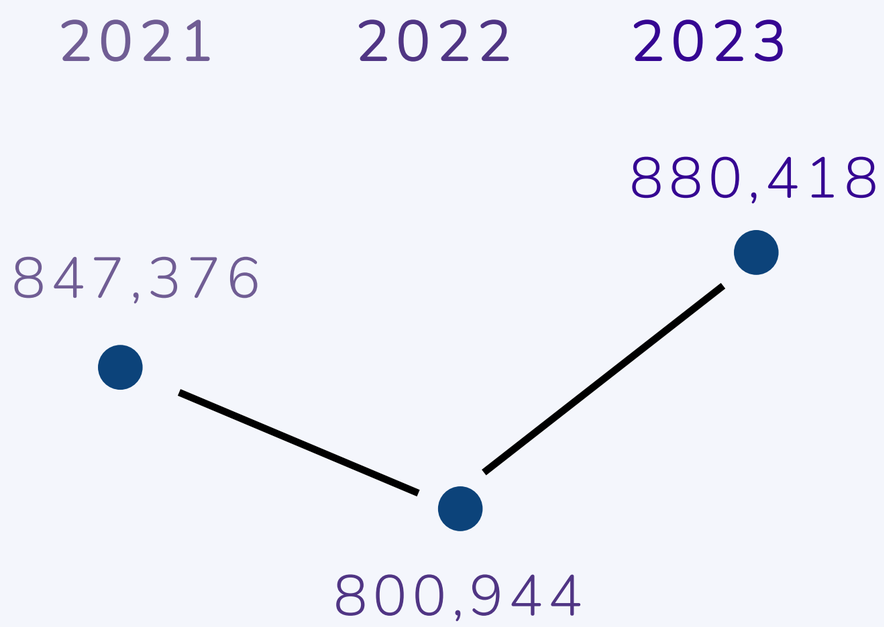
INCREASING RESILIENCY THROUGH KNOWLEDGE AND ACTION

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

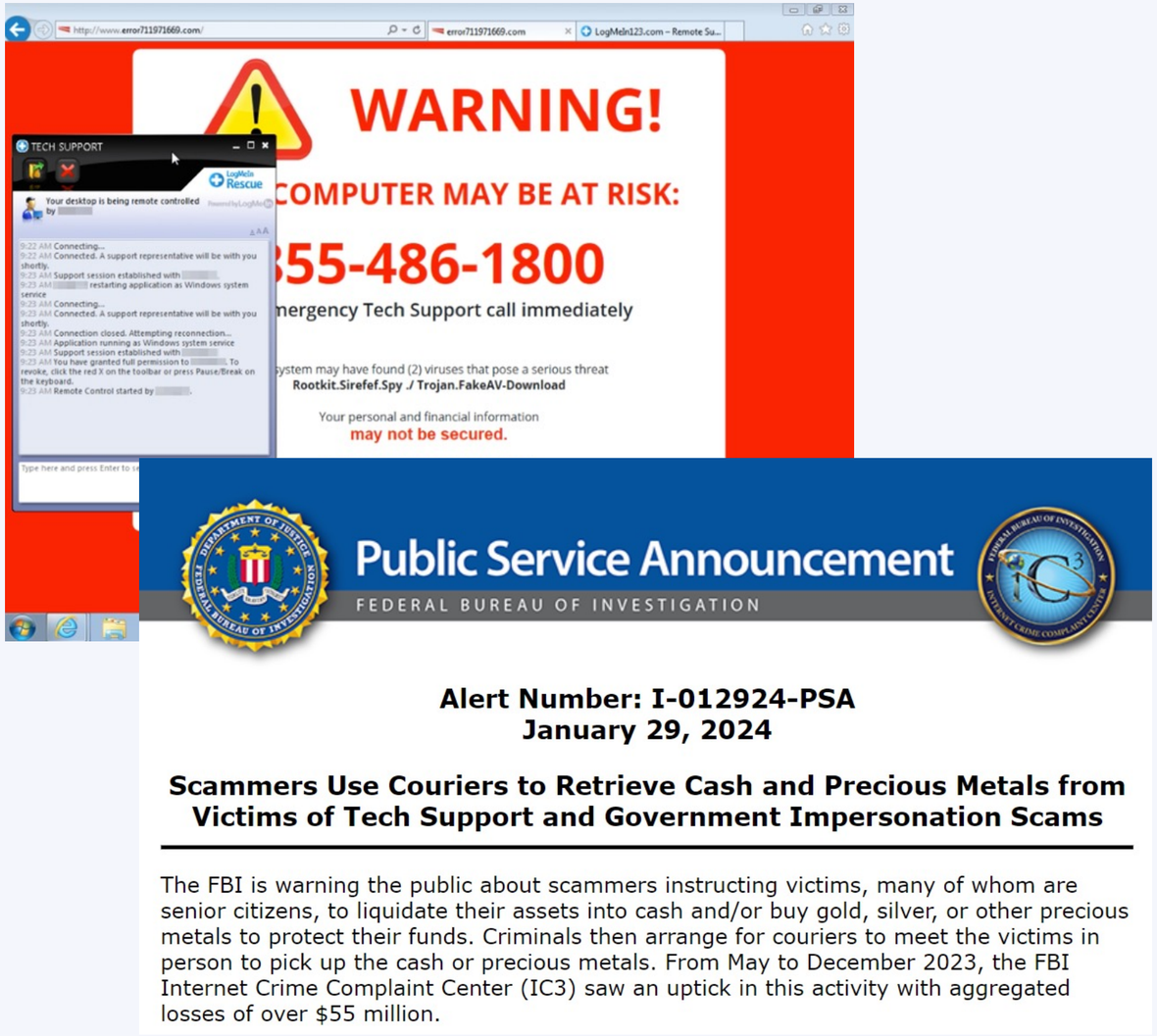
Real Estate Transaction - $145 M

Extortion - $74.8 M

Social Engineering

Tech Support Scam

IMPERSONATING THOSE YOU TRUST



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.

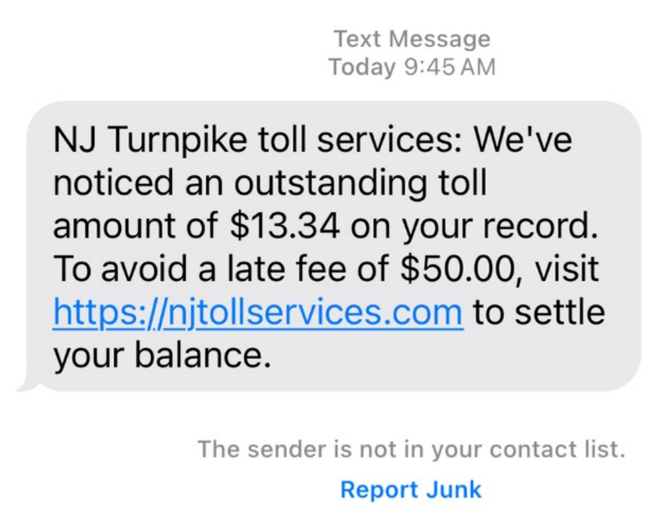
SMS Text Scam

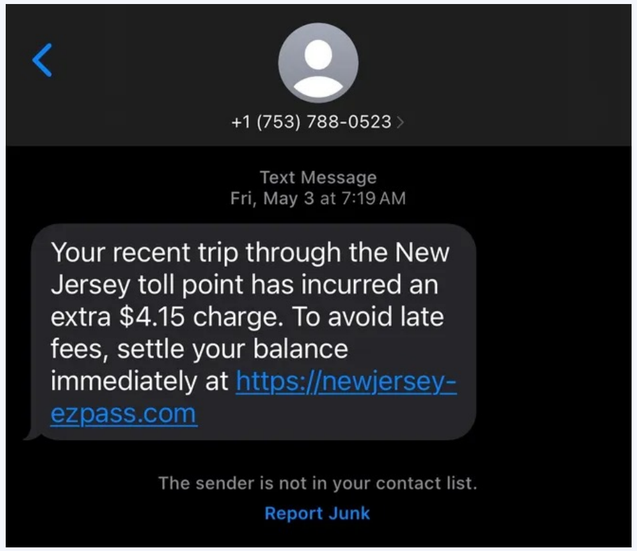
Exploiting Legitimate Comms

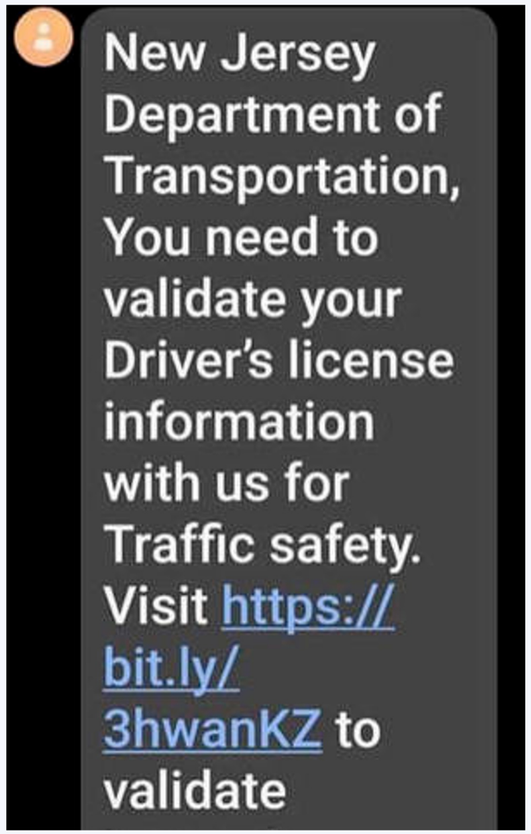
- Missed delivery notifications
- “Is this you?” messages
- Text scams claiming that your bank is closing your account
- Texts claiming that you’ve won a prize
- Texts claiming that your debit or credit card has been locked
- Text messages supposedly from the IRS
- Text messages from your own number
- 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

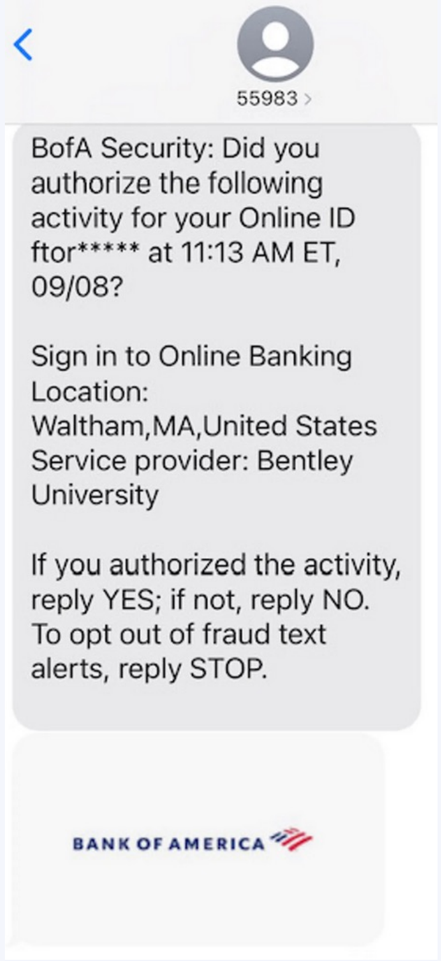
SMS Text Scam

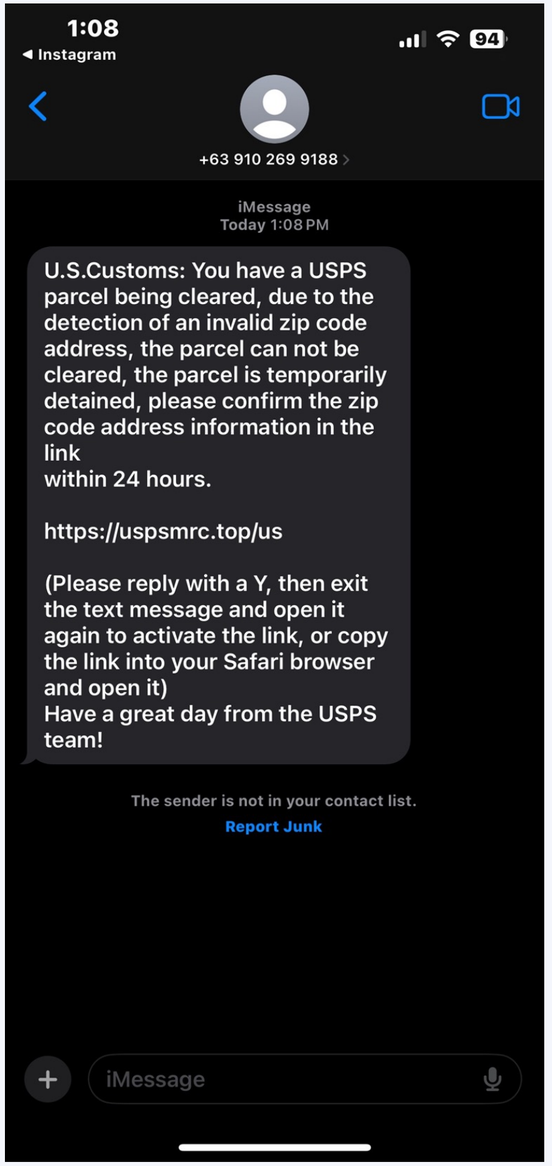
Exploiting Legitimate Comms











Direct Deposit Scams

Sender: Steven [redacted]
Sender IP Address: [redacted]
To reply to this message, use reply email [redacted]@gmail.com

Hi [redacted]

I changed banks and I would like to change my payroll deposit information. Can you please help me?

Regards
Steven [redacted]

This message was sent from the messaging service on your website via [redacted] on 04/29/24 09:01 AM CDT

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]

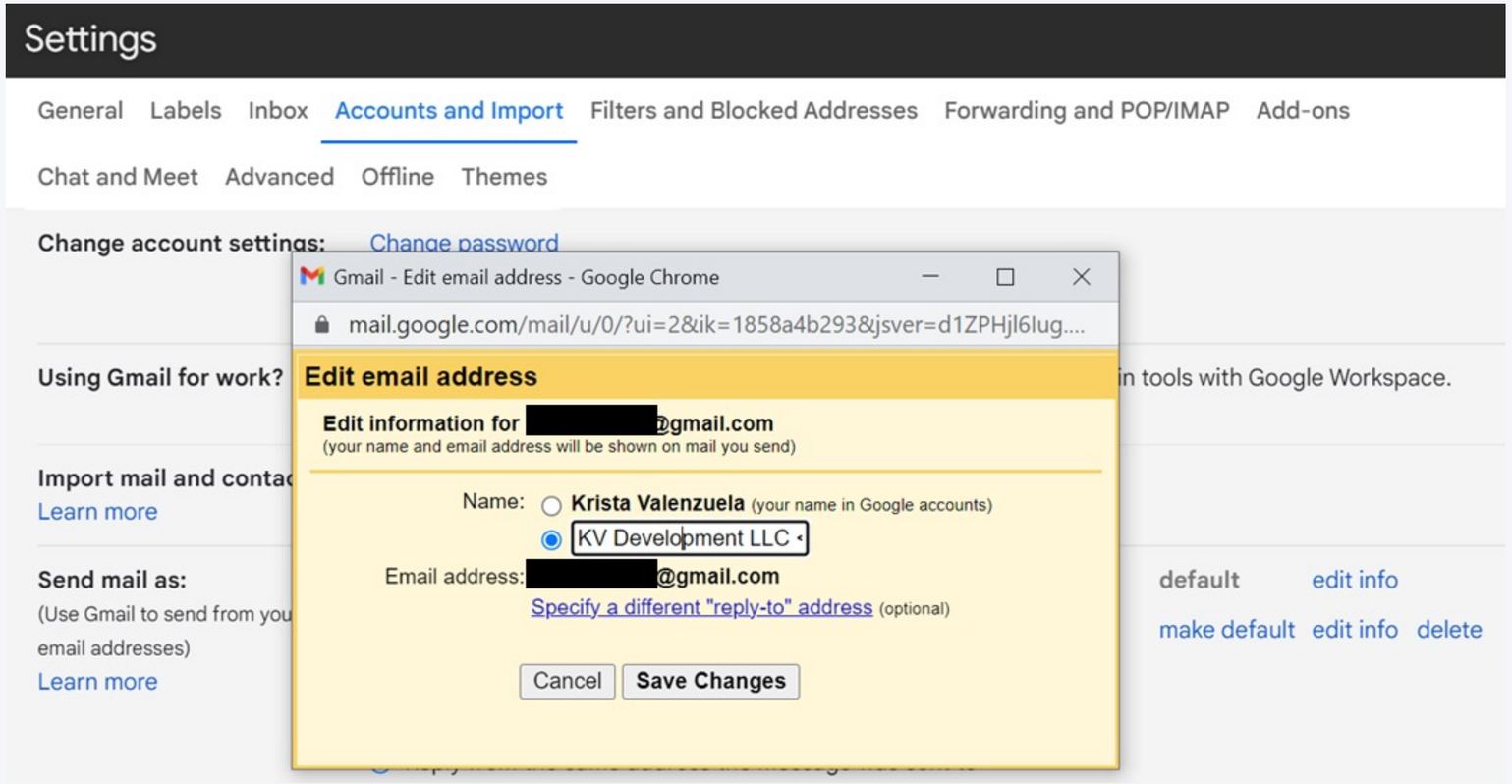
Hello Maria

I would like to change the details of my direct deposit information in our records. Unfortunately, my 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.

Business Email Compromise



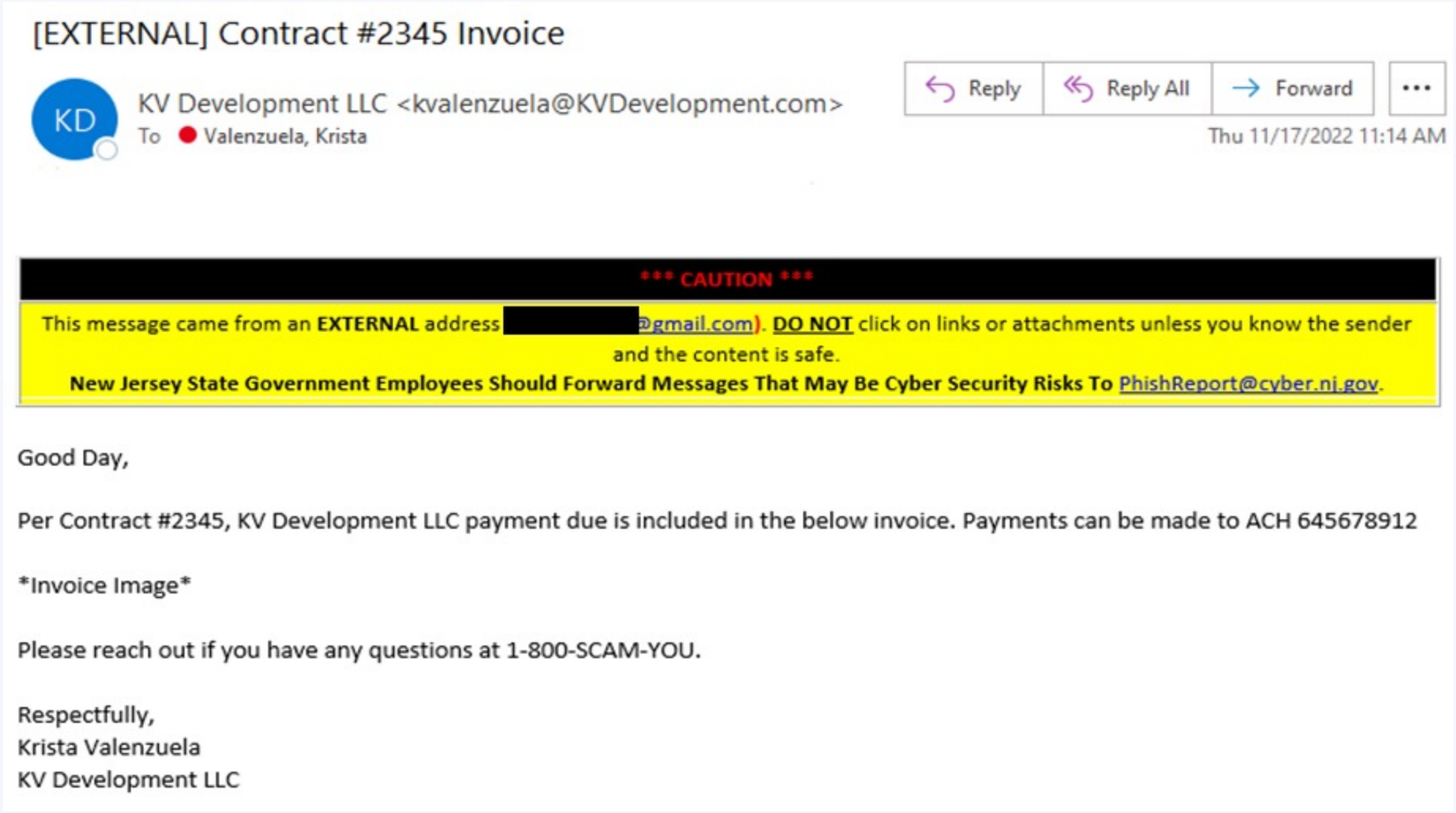
WHY IS IT SO PERVASIVE?
-IT'S EASY.

- Gather information online.
- Research the target and impersonating entities.
- Craft a convincing email.
- Wait.

Business Email Compromise

WHAT RED FLAGS DO YOU SEE?

HOW DID THIS BYPASS EMAIL SECURITY?



[EXTERNAL] Contract #2345 Invoice

KD

KV Development LLC <kvalenzuela@KVDevelopment.com>

To Valenzuela, Krista

Reply | Reply All | Forward | ...

Thu 11/17/2022 11:14 AM

*** CAUTION ***

This message came from an **EXTERNAL** address [redacted]@gmail.com). **DO NOT** click on links or attachments unless you know the sender and the content is safe.

New Jersey State Government Employees Should Forward Messages That May Be Cyber Security Risks To PhishReport@cyber.nj.gov.

Good Day,

Per Contract #2345, KV Development LLC payment due is included in the below invoice. Payments can be made to ACH 645678912

Invoice Image

Please reach out if you have any questions at 1-800-SCAM-YOU.

Respectfully,
Krista Valenzuela
KV Development LLC

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.

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.

Credential Compromise

Tricking Users

From: NJ Division of Pensions and Benefits <donotreply@cclifestyle.net>
Sent on: Friday, February 4, 2022 1:29:30 AM
To: [redacted]
Subject: NJ Division of Pensions and Benefits Reports
Urgent: High

Attachments: NJDPB _4452.pdf (25.33 KB)

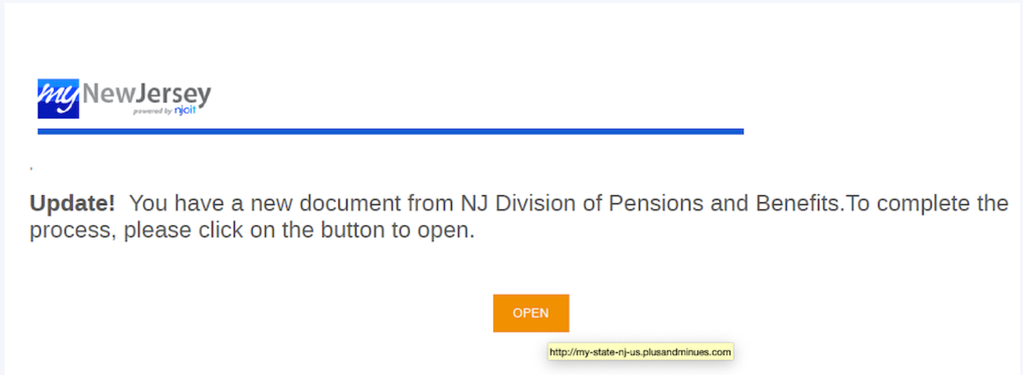
WARNING: This email originated from outside your organization. Please use extreme caution before opening any links or attachments.

NJ Division of Pensions and Benefits

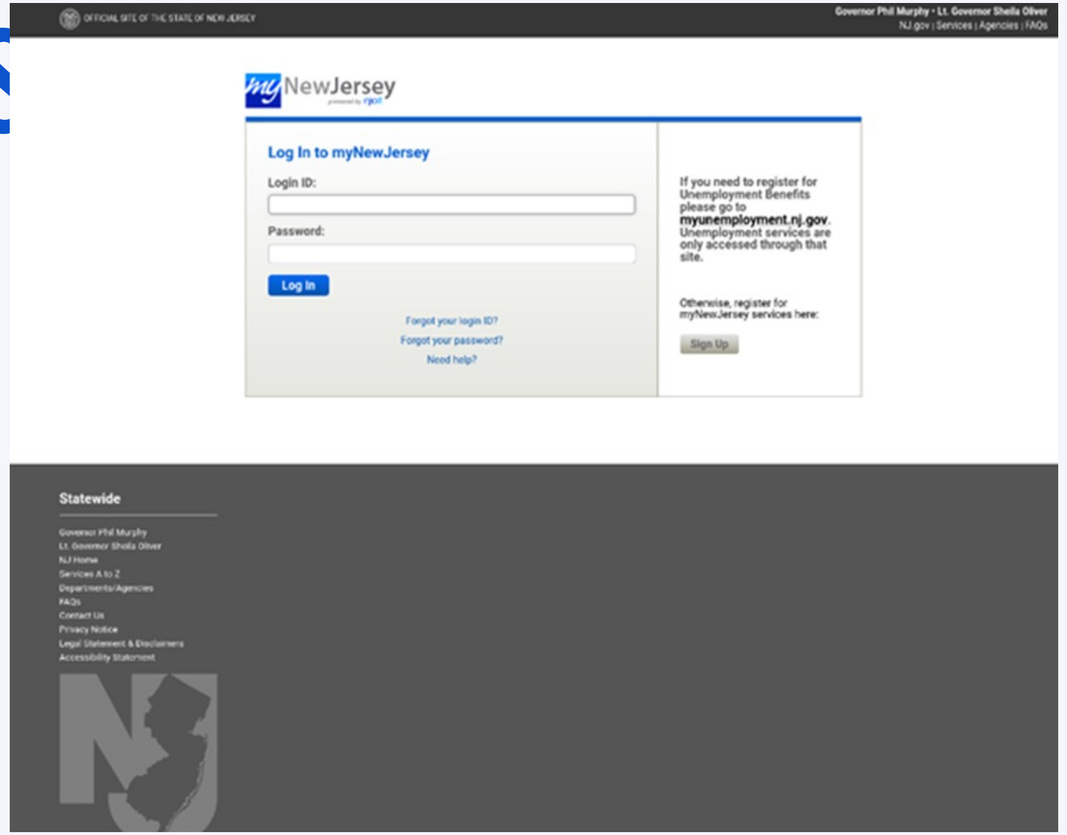
Dear : [redacted]

You have a new document from NJ Division of Pensions and Benefits : Thursday, February 3, 2022 _ 8:29:22 PM

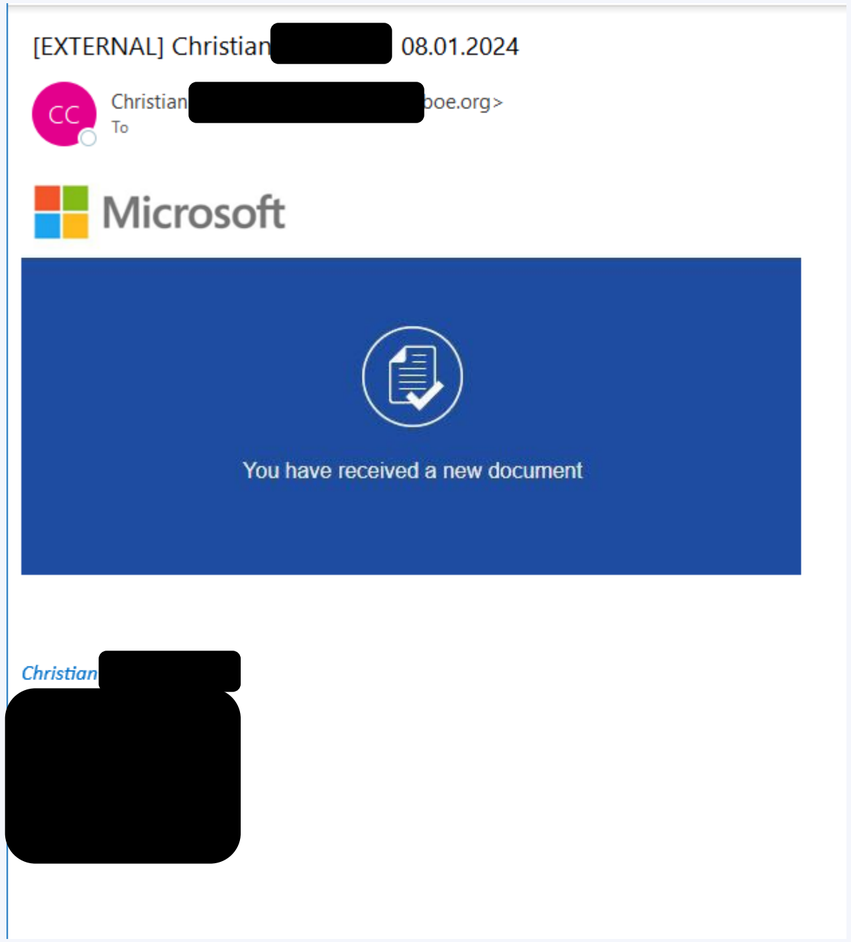
Notice: This e-mail message and any attachments to this e-mail message contain information that may be legally privileged and confidential from the State of New Jersey, Department of the Treasury, Pensions & Benefits. If you are not the intended recipient, you must not review, transmit, convert to hard copy, copy, use or disseminate this e-mail or any attachments to it. If you have received this e-mail in error, please immediately notify us by return e-mail and delete this message. If this e-mail contains a forwarded message or is a reply to a prior message, some or all of its contents or attachments may not have been produced by the State of New Jersey, Department of the Treasury.

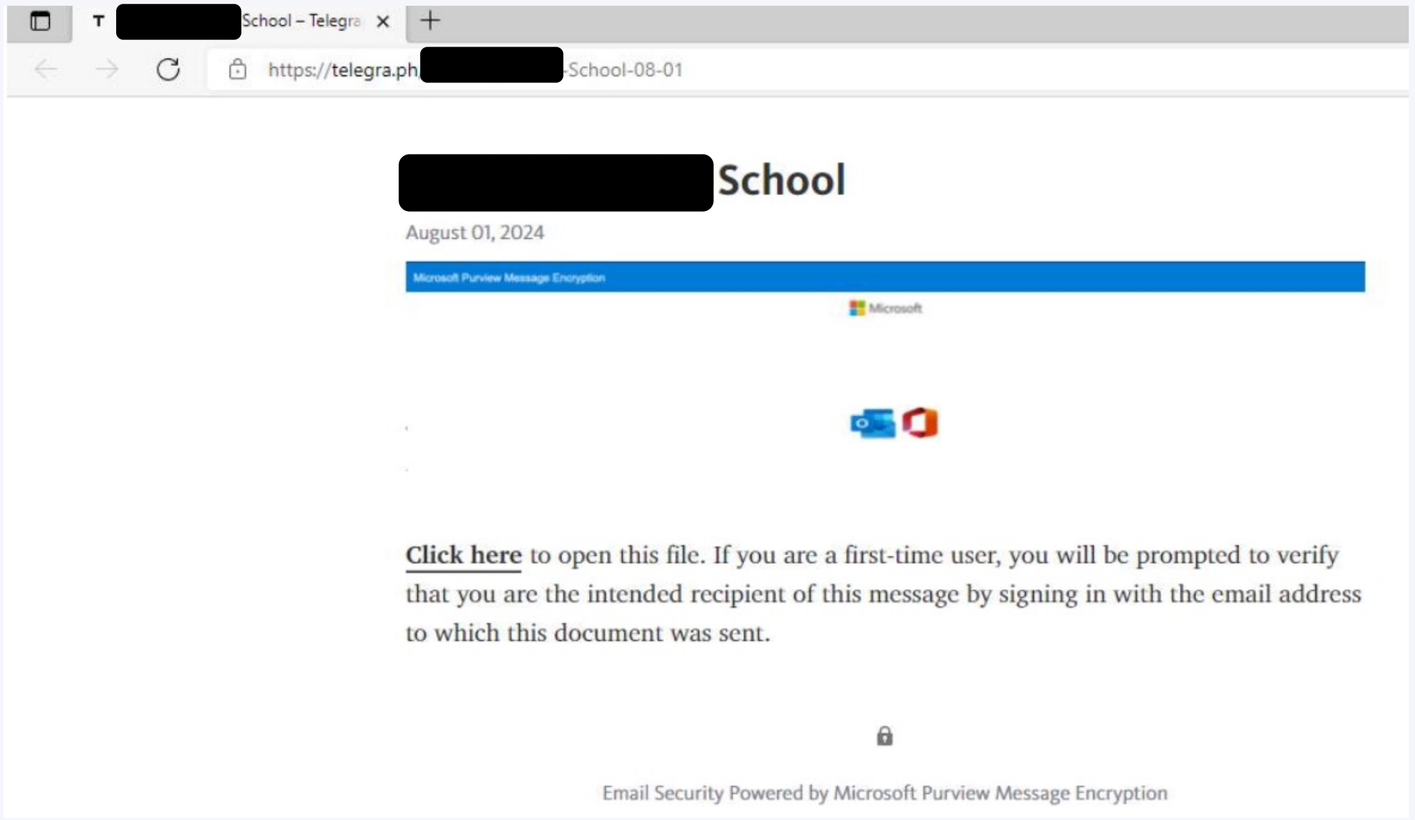


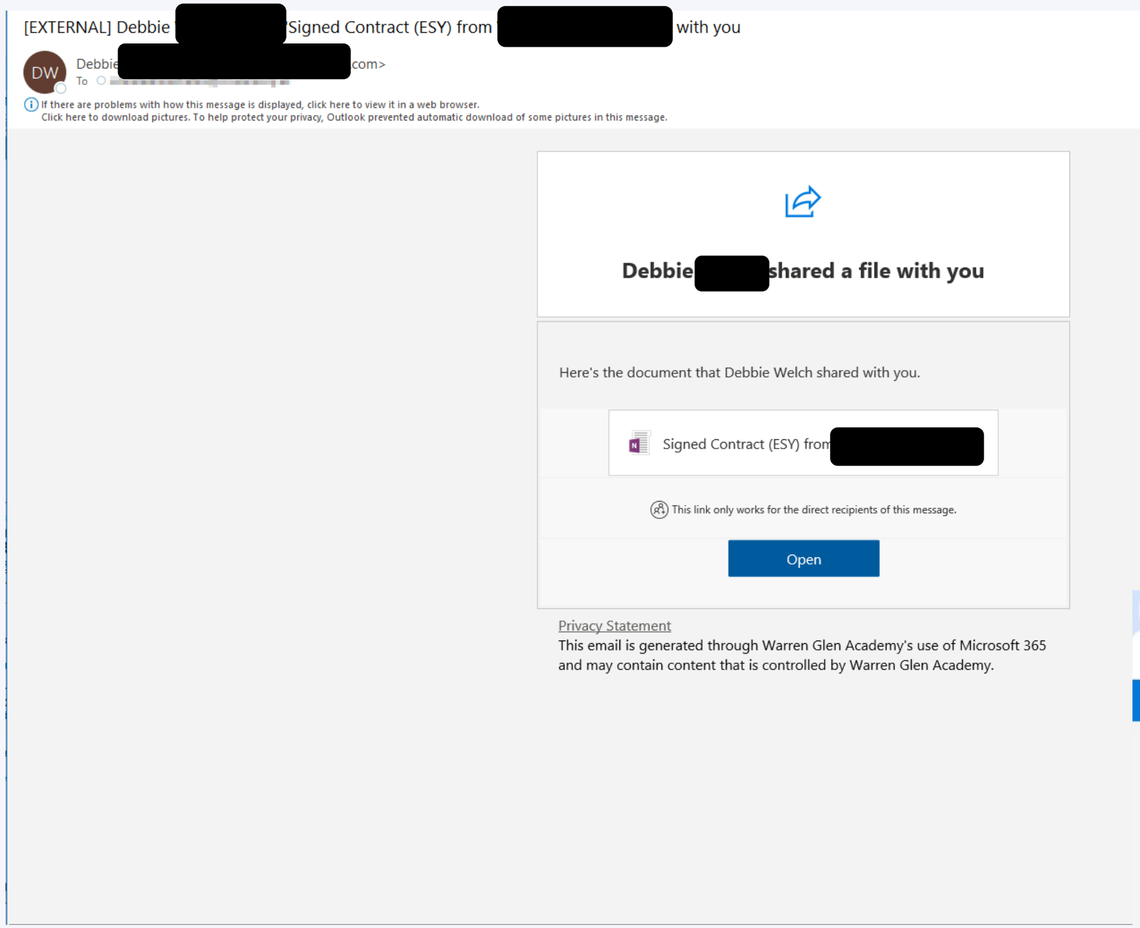
http://my-state-nj-us.plusandminues.com

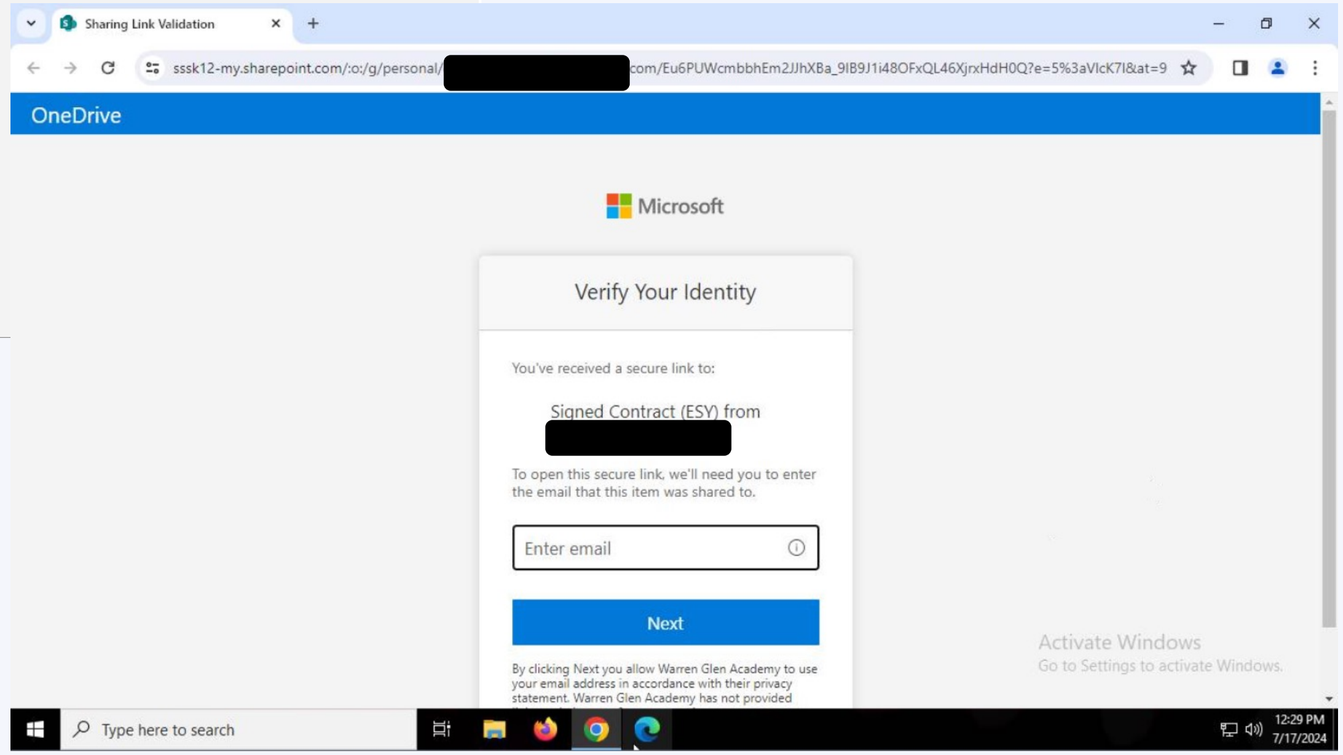


Compromised Accounts






[EXTERNAL] Debbie [redacted] Signed Contract (ESY) from [redacted] with you
Debbie [redacted] com>
To [redacted]
Reply
Reply All
Forward
Tue 7/16/2024 10:51 AM
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.
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.
Open
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.


Sharing Link Validation
sssk12-my.sharepoint.com/:o:/g/personal/[redacted]com/Eu6PUWcmbbhEm2JJhXBa_9IB9J1i48OFxQL46XjrxHdH0Q?e=5%3aVIcK7I&at=9
OneDrive
Microsoft
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
Next
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
Activate Windows
Go to Settings to activate Windows.
Type here to search
12:29 PM
7/17/2024

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

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

Reply | Reply All | Forward

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;

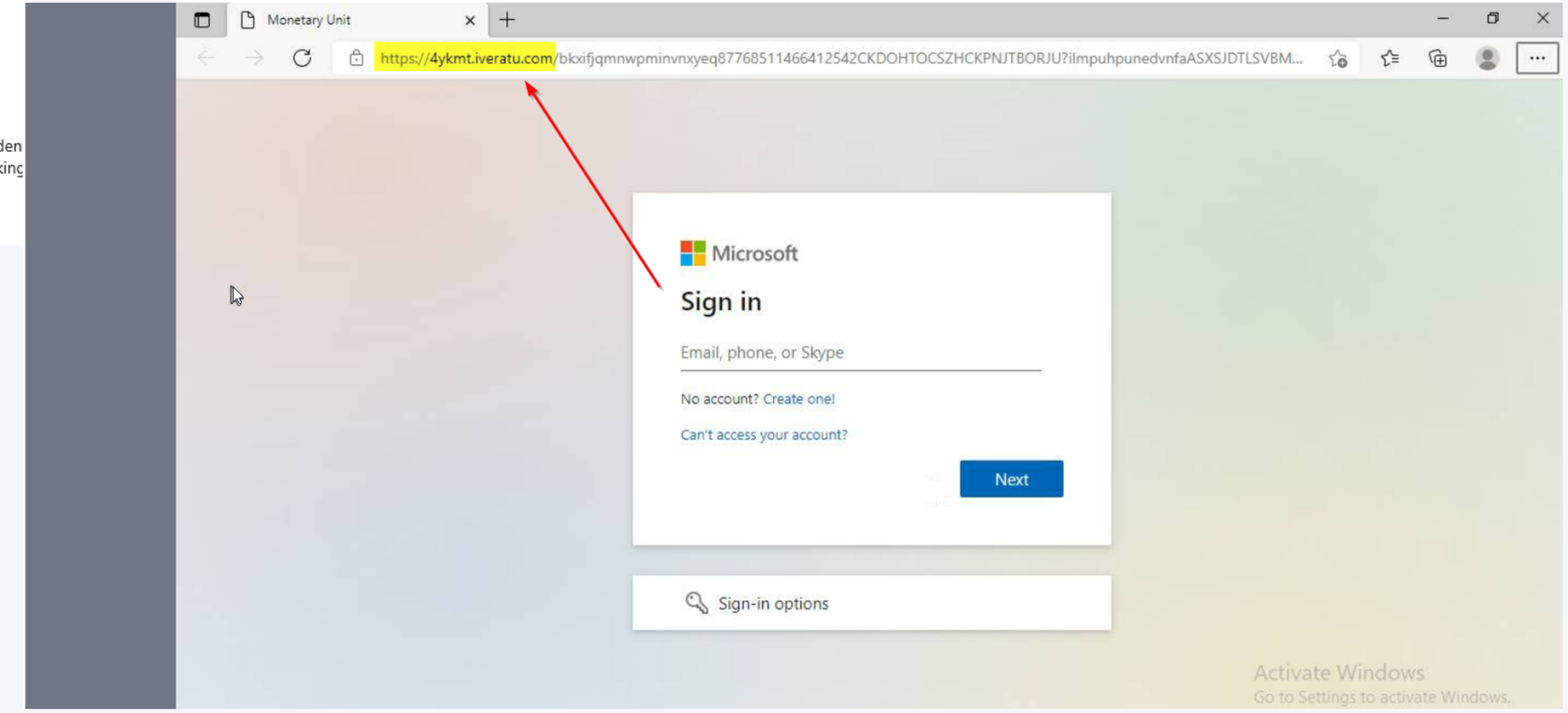
Online document and deal tracker url: fondexgruppen-online-deal-tracker-url-update-fondexgruppen.esdebutik.com

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



Using Compromised Accounts

[EXTERNAL] YOU HAVE RECEIVED A NEW DOCUMENT

NB

To .k12.nj.us>

Reply | Reply All | Forward

Mon 7/31/2023 8:50 AM

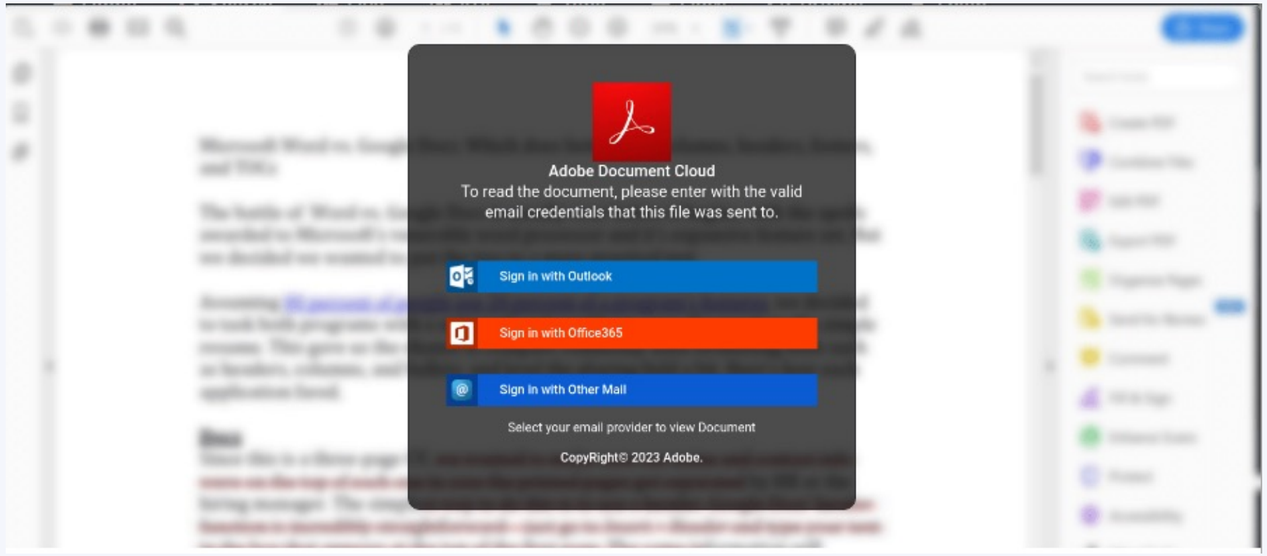
Hello,

Find attached the updated statement for your =eview

ACCESS DOCUMENT

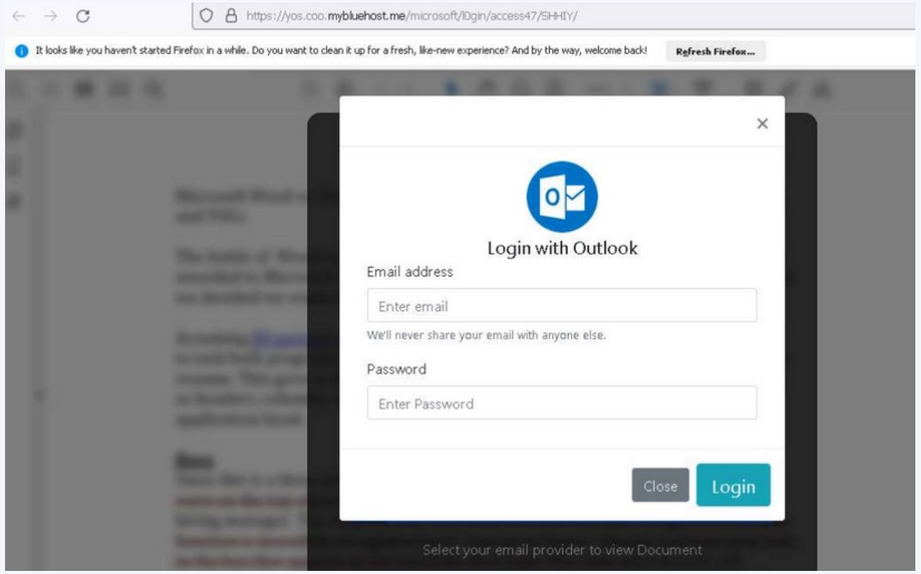
Document expires in 24 hours

Let me know if you have any questions



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.



Using Compromised Accounts

SENT FROM A KNOWN, TRUSTED ACCOUNT, WHICH INCREASES THE LIKELIHOOD OF SUCCESS.

SENDER IS OFTEN 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.

INCREASED EFFORT TO BYPASS MULTI-FACTOR AUTHENTICATION.

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.

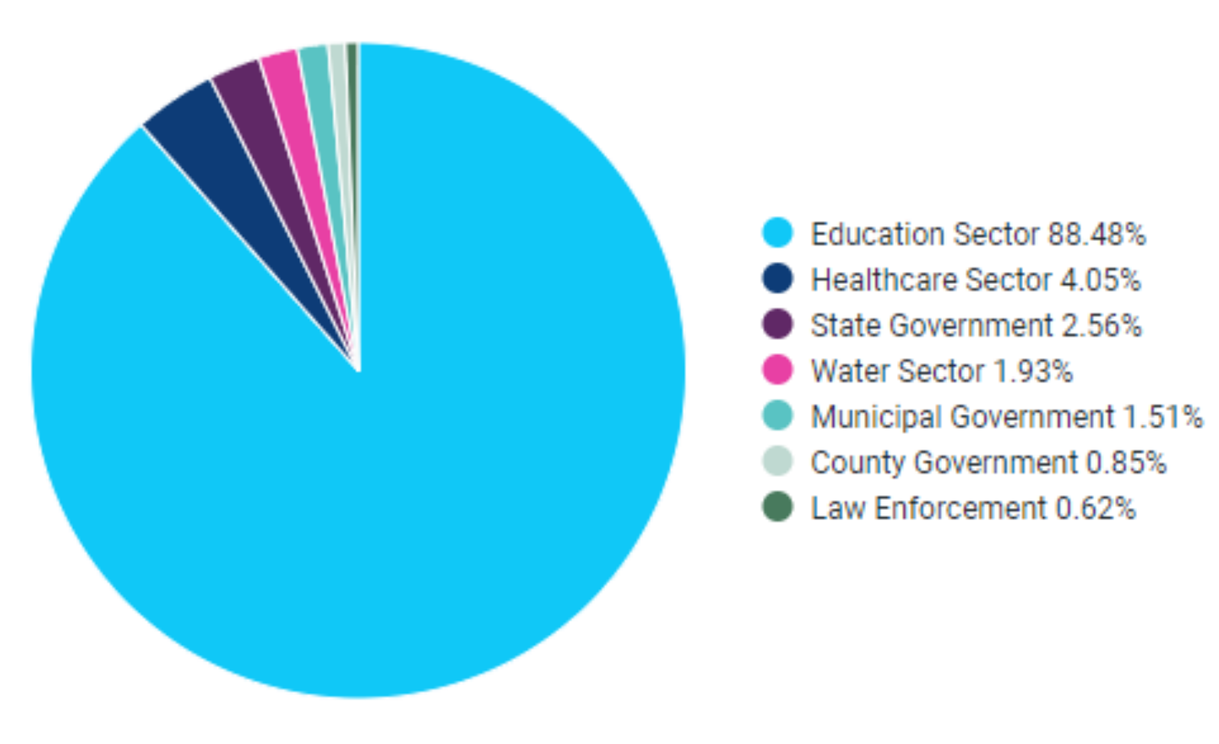
SO, WHAT SHOULD WE DO?

MULTI-FACTOR AUTHENTICATION

- Something you know
- Something you have
- Something you are

Credential Compromise

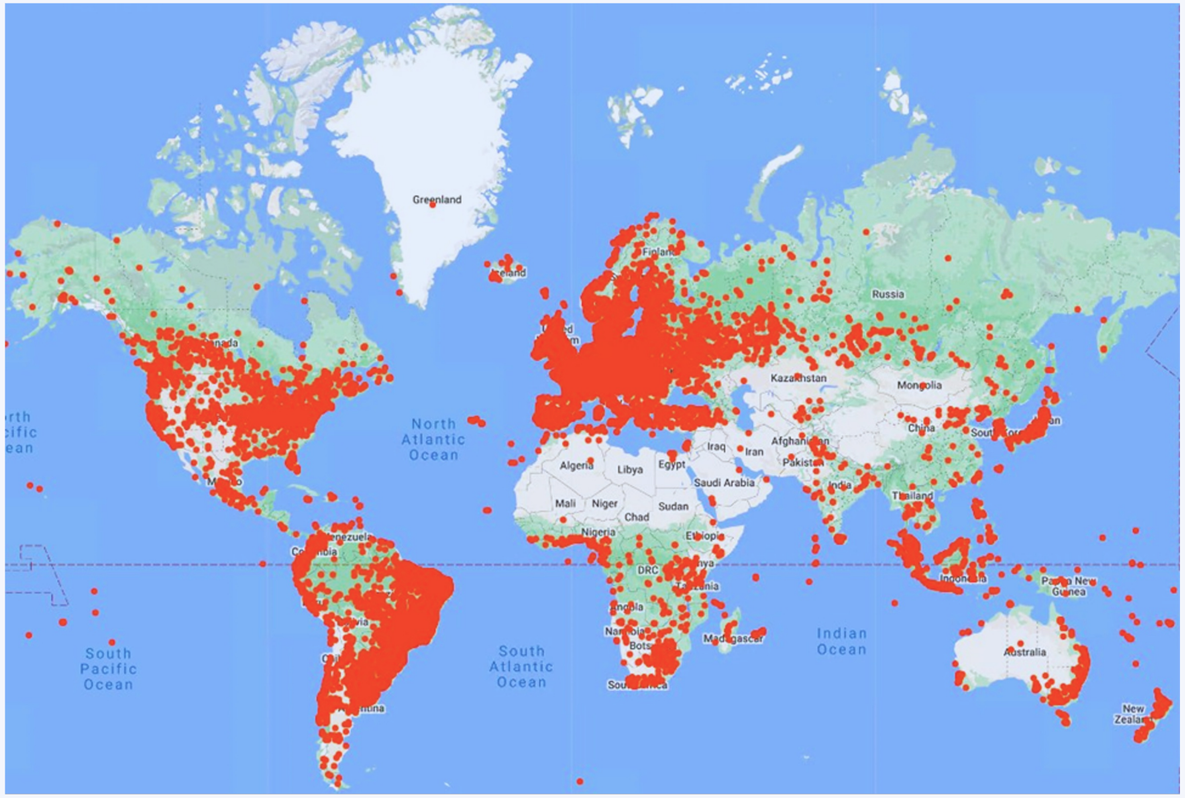
GETTING THE KEYS TO THE KINGDOM



Sector	Notifications
Education	66,551
Healthcare	3,045
State Government	1,927
Water	1,453
Municipal Government	1,135
County Government	640
Law Enforcement	468

How Are They Compromised?

GETTING THE KEYS TO THE KINGDOM



INFOSTEALERS

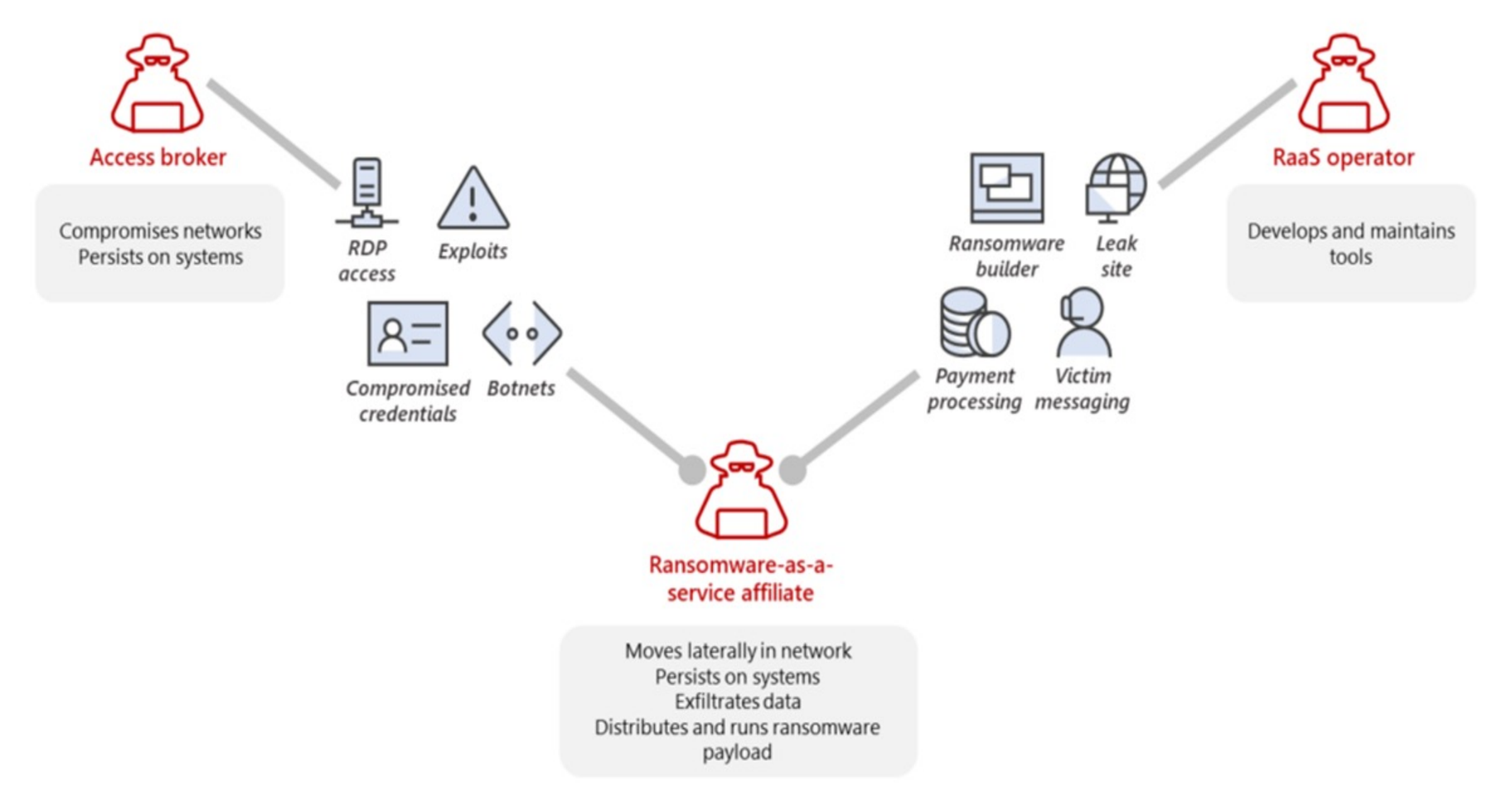
DATA BREACHES

WEAK PASSWORDS

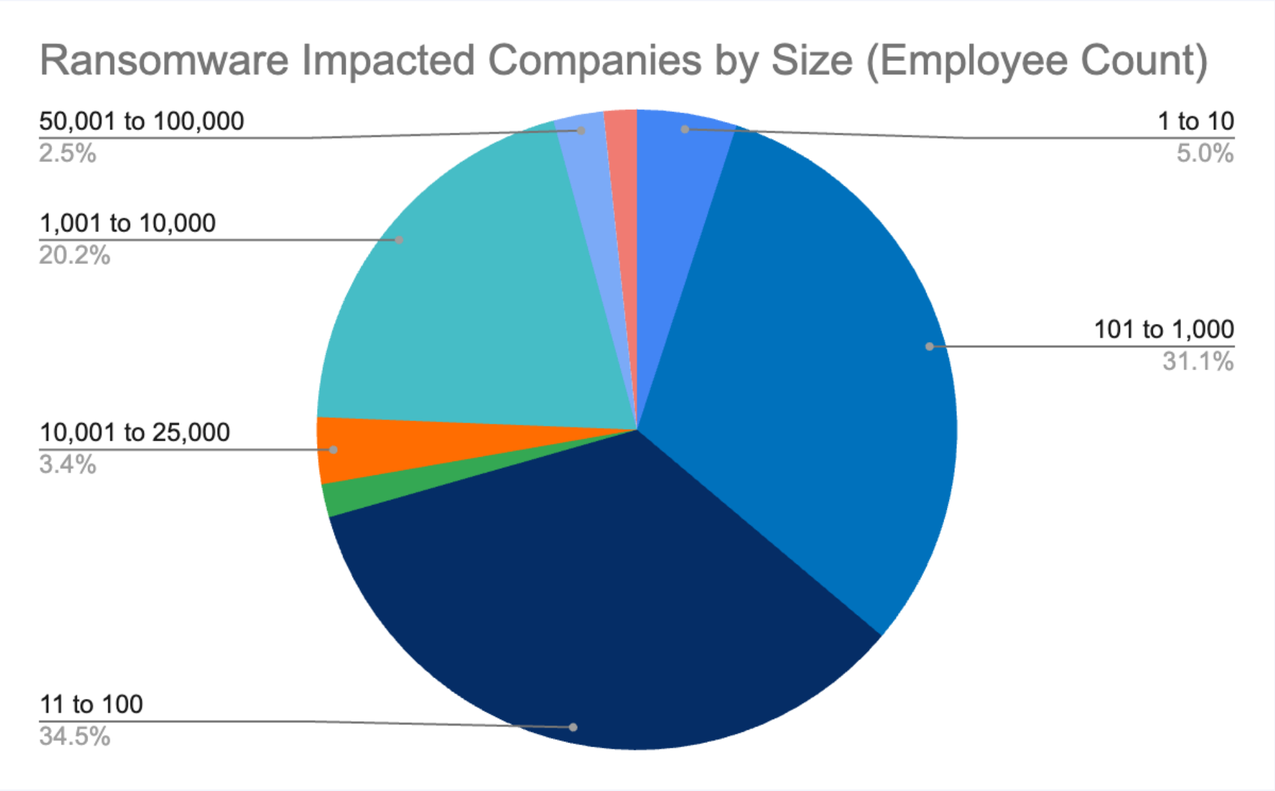
SOCIAL ENGINEERING

Ransomware

Ransomware-as-a-Business



Ransomware



average ransom: $390,000

avg downtime ~24 days

remote access, phishing, unknown

data exfiltration in 75% of incidents

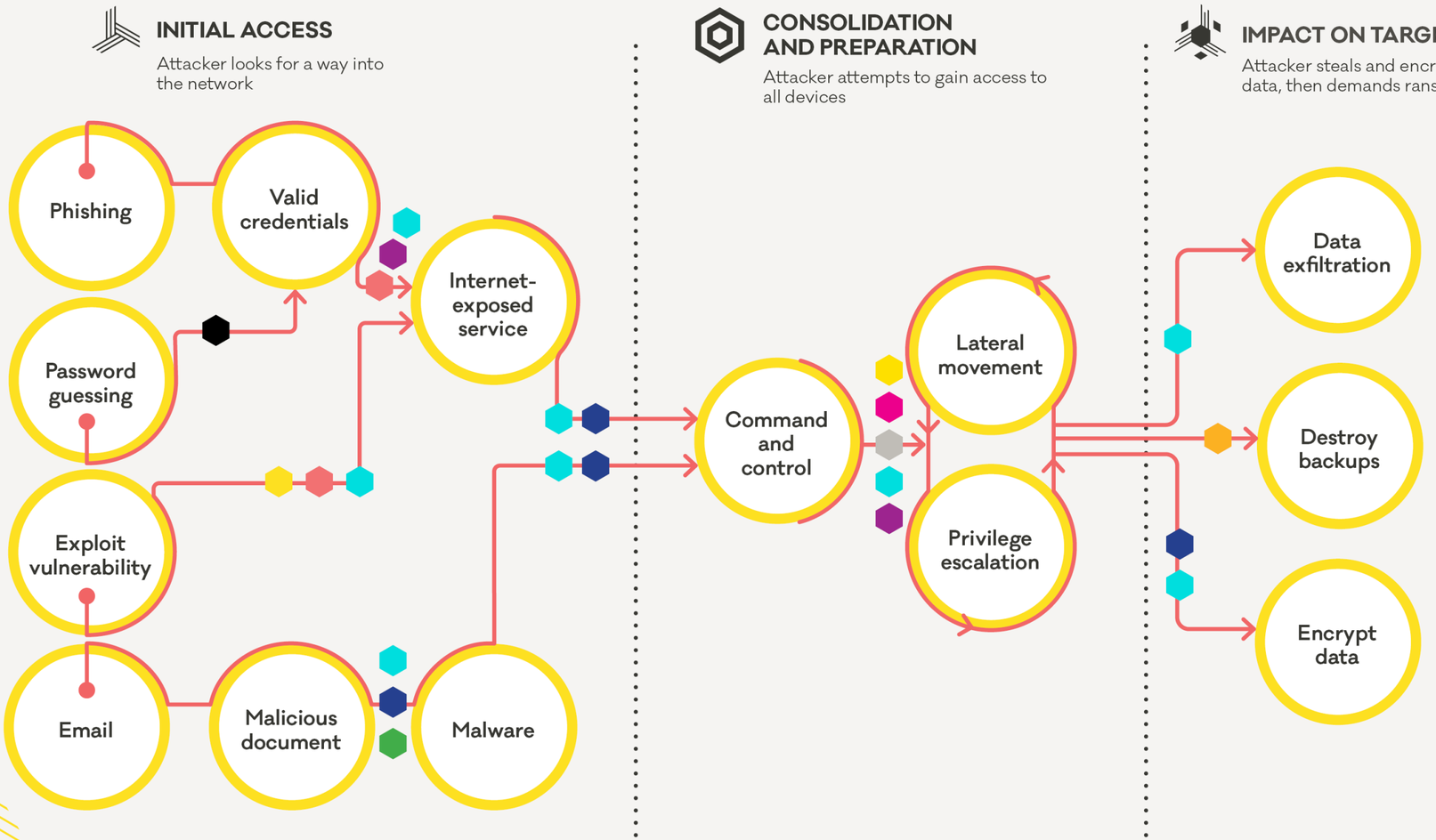
target of opportunity

SMBs targeted

o encryption extortion

LIFECYCLE OF A RANSOMWARE INCIDENT

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



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, and **60%** of affected hospitals **lost over $1 million daily**.

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.

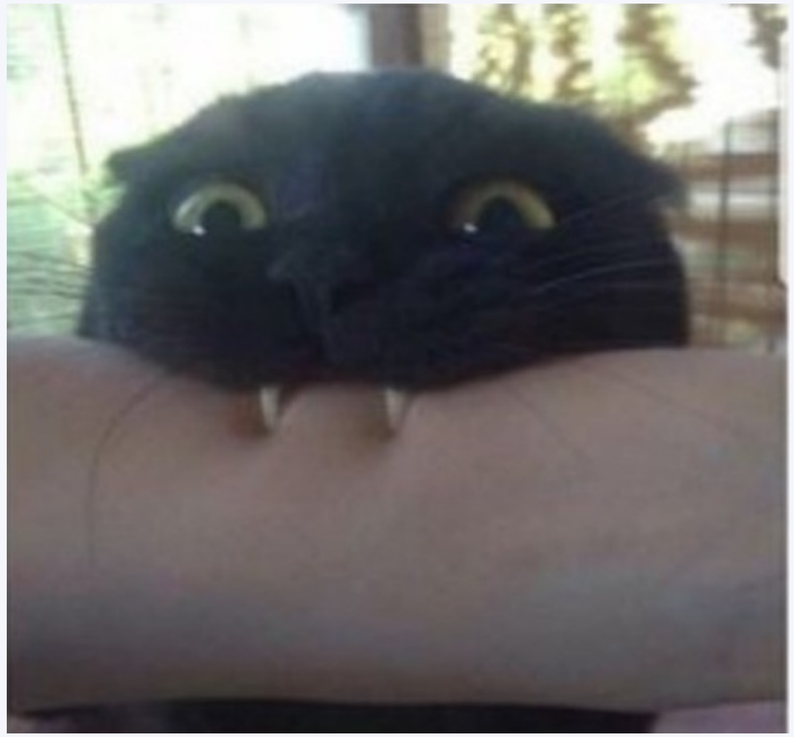
Who is BlackCat?

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 was sent to a cryptocurrency wallet mapped to BlackCat.

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, then announced they were shutting down.

Because a BlackCat failed to pay them, Notchy stated the data wouldn’t be deleted.

March 7:

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

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.

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 expects the **total cost for 2024 to increase to between $1.35 billion and $1.6 billion**.

Healthcare providers:
94% of all US Hospitals were financially impacted by the cyberattack.
~60% of US Hospitals noted they had significant or serious financial damage.
Physician practices (as of April 2024, issues continued after):
80 percent of physician practices lost revenue from unpaid claims
85 percent have committed additional staff time and resources to finish revenue cycle tasks
78 percent have lost revenue from claims that they have been unable to submit
36 percent reported delays in claim repayment
32 percent reported inability to submit claims
22 percent reported being unable to check eligibility for benefits
Small practices (10 or fewer physicians) were hit particularly hard.

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

Key Takeaways

This incident highlights why **making ransom payments are a bad idea**. If a ransom is paid, there is no guarantee that criminals will keep their word.

Instead, organizations should focus on **preventative security**.

Update systems and software.

Implement robust **backup** policies.

Implement strong passwords and **MFA**.

Encrypt sensitive data-at-rest.

Source: twitter.com

Artificial Intelligence

The Good and The Bad

CYBERSECURITY

GENERATIVE AI

AUTOMATION

ENHANCED CUSTOMER EXPERIENCE

REDUCED HUMAN ERROR

EFFICIENCY

CYBER THREATS

AUTOMATING ATTACKS

VULNERABILITY DISCOVERY

SOCIAL ENGINEERING

VOICE REPLICATION

DISINFORMATION

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

NJCCIC 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