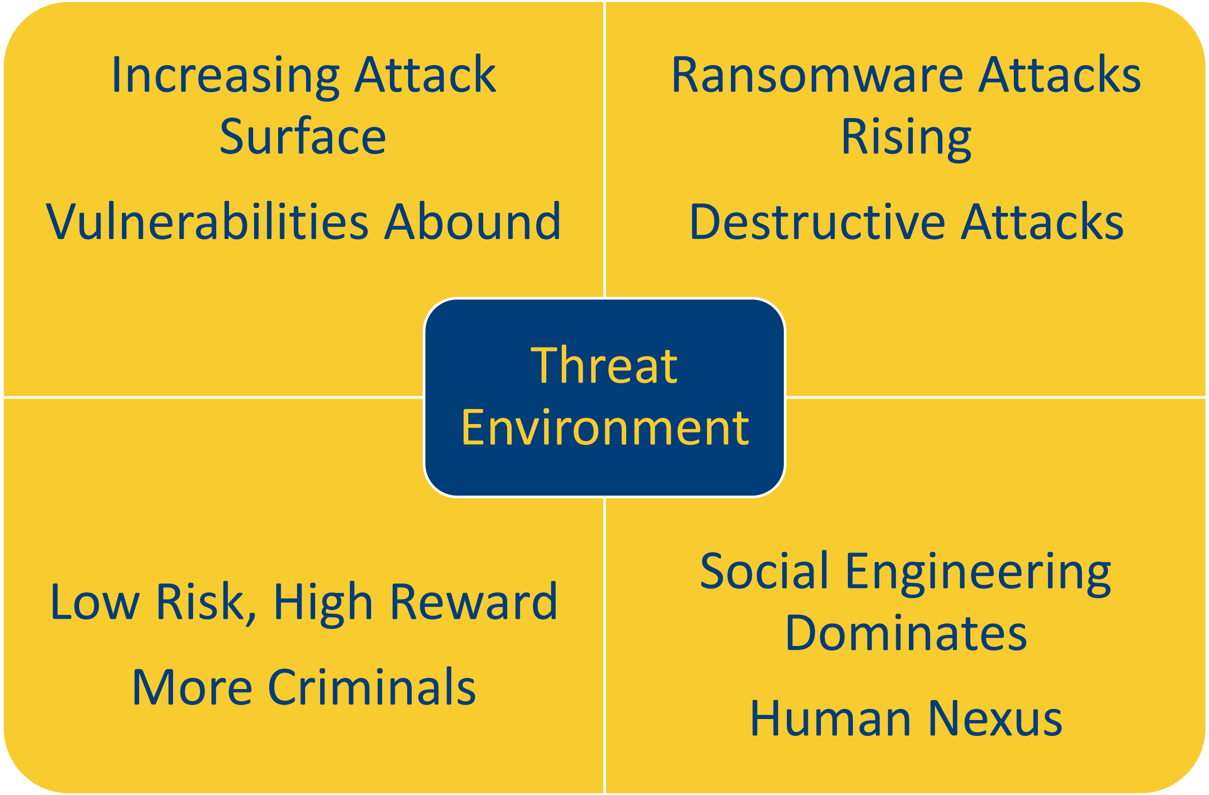
NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

Prevent, Detect, Respond

TLP: White

Threat Environment



Increasing Attack Surface

Vulnerabilities Abound

Ransomware Attacks Rising

Destructive Attacks

Threat Environment

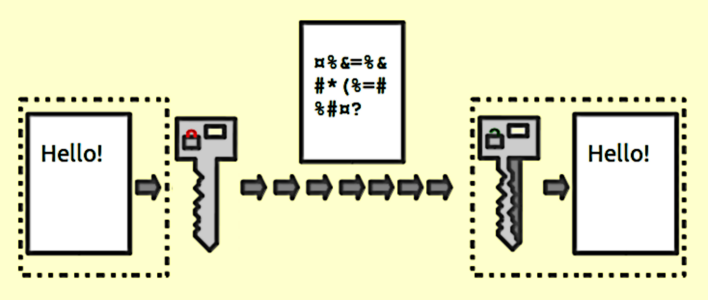
Low Risk, High Reward

More Criminals

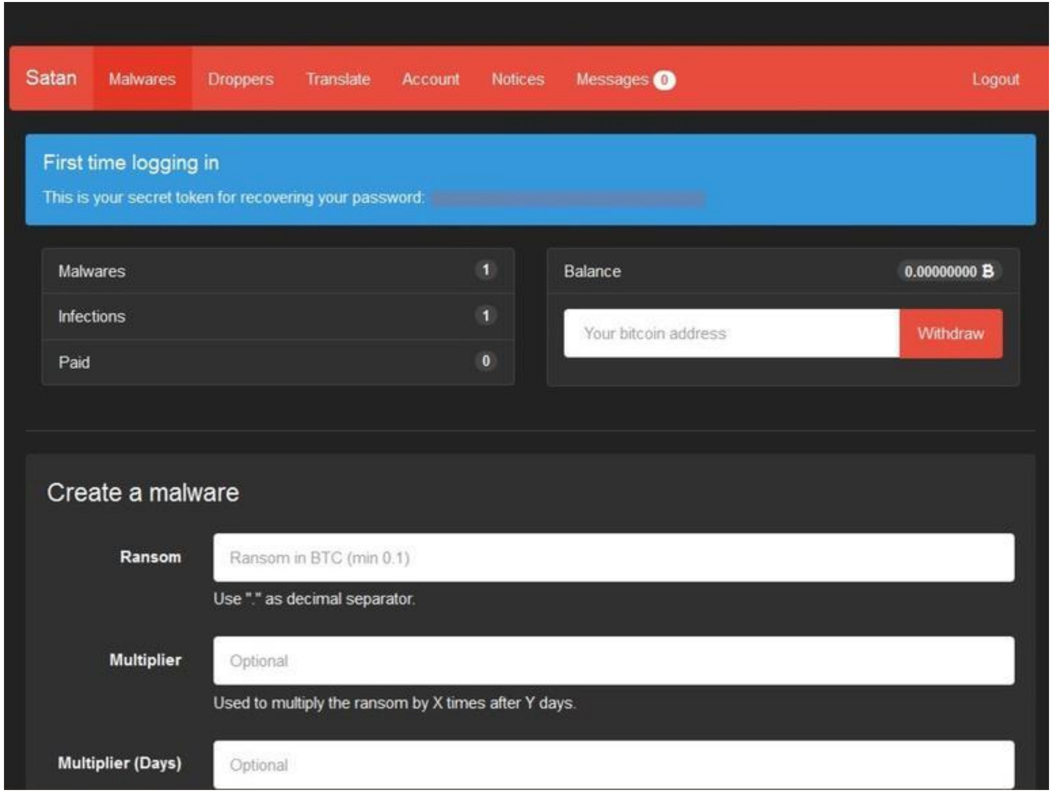
Social Engineering Dominates

Human Nexus

Ransomware



Ransomware-as-a-Service



First time logging in

This is your secret token for recovering your password: [redacted]

Malwares	1
Infections	1
Paid	0

Balance 0.00000000 Ƀ

Create a malware

Ransom Ransom in BTC (min 0.1)

Use "." as decimal separator.

Multiplier Optional

Used to multiply the ransom by X times after Y days.

Multiplier (Days) Optional

Q4 2021 Ransomware Stats

Average ransom amount $322,168

Average downtime is 20 days

Top attack vectors:

Phishing
Remote Access

Selective targeting is more common

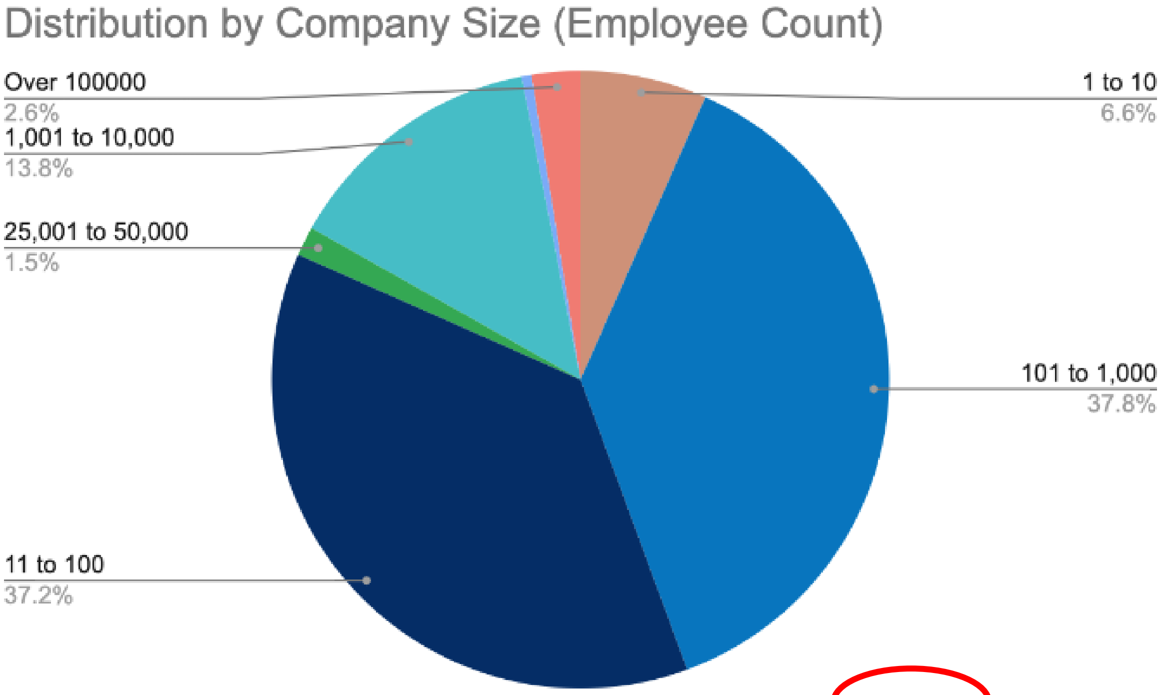
84% of cases include data exfiltration

Top Target:

Professional Services

Over 3,100 Ransomware attacks in 2021

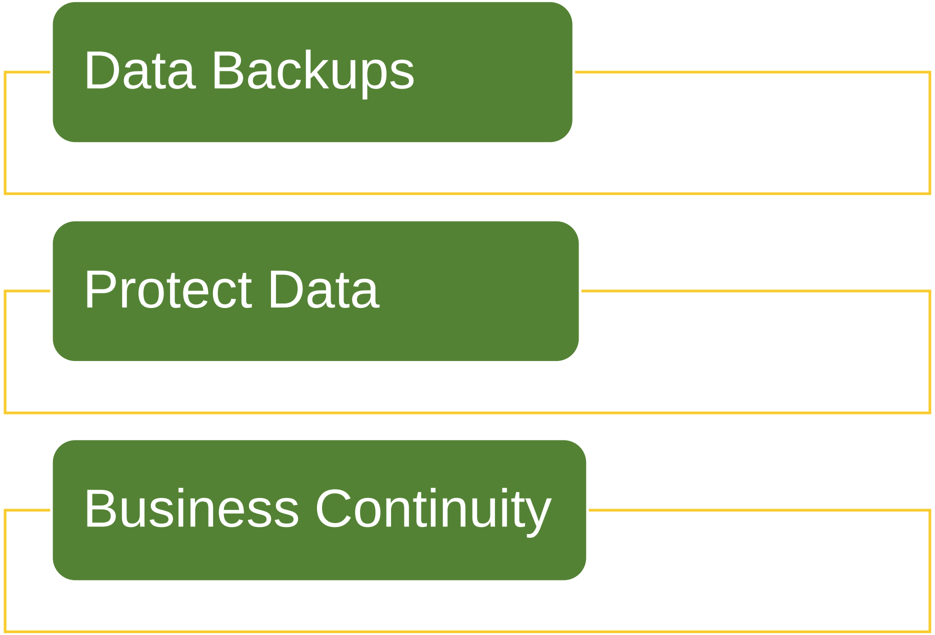
Ransomware Targets



COVEWARE

Over 75% of attacks impact companies with less than 1,000 employees.

Increase Resiliency



Data Backups

Protect Data

Business Continuity

What if you are a victim of ransomware?

Credential Compromise

Colonial Pipeline Incident

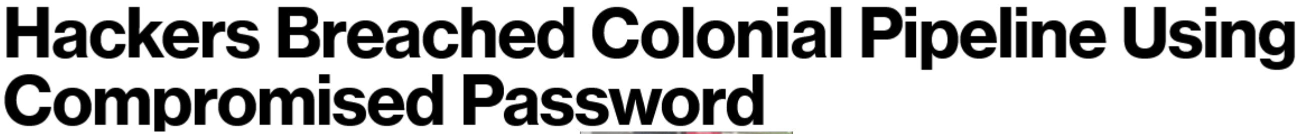
IT and OT not separate

Panic buying

Gas stations closed

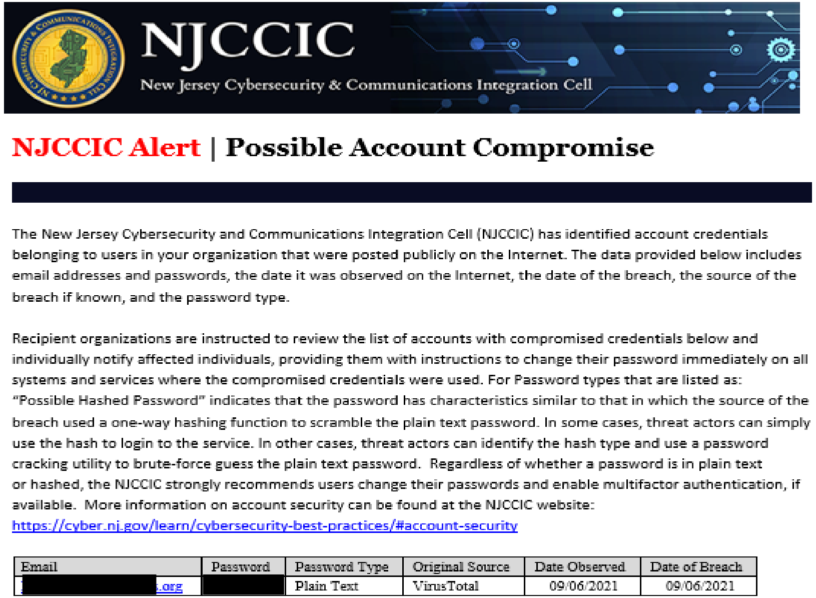
Paid $4.4M in ransom

Password reuse



Hackers Breached Colonial Pipeline Using Compromised Password

U Have Been Pwned Project



NJCCIC

New Jersey Cybersecurity & Communications Integration Cell

NJCCIC Alert | Possible Account Compromise

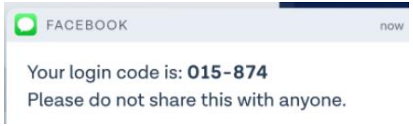
The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) has identified account credentials belonging to users in your organization that were posted publicly on the Internet. The data provided below includes email addresses and passwords, the date it was observed on the Internet, the date of the breach, the source of the breach if known, and the password type.

Recipient organizations are instructed to review the list of accounts with compromised credentials below and individually notify affected individuals, providing them with instructions to change their password immediately on all systems and services where the compromised credentials were used. For Password types that are listed as: "Possible Hashed Password" indicates that the password has characteristics similar to that in which the source of the breach used a one-way hashing function to scramble the plain text password. In some cases, threat actors can simply use the hash to login to the service. In other cases, threat actors can identify the hash type and use a password cracking utility to brute-force guess the plain text password. Regardless of whether a password is in plain text or hashed, the NJCCIC strongly recommends users change their passwords and enable multifactor authentication, if available. More information on account security can be found at the NJCCIC website: https://cyber.nj.gov/learn/cybersecurity-best-practices/#account-security

Email	Password	Password Type	Original Source	Date Observed	Date of Breach
[redacted].org	[redacted]	Plain Text	VirusTotal	09/06/2021	09/06/2021

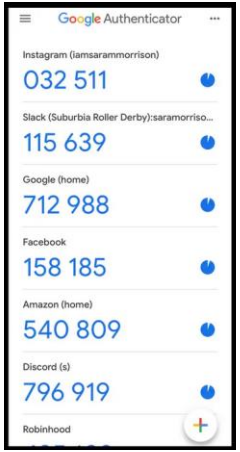
To check your personal email address, visit haveibeenpwned.com

Credential Compromise

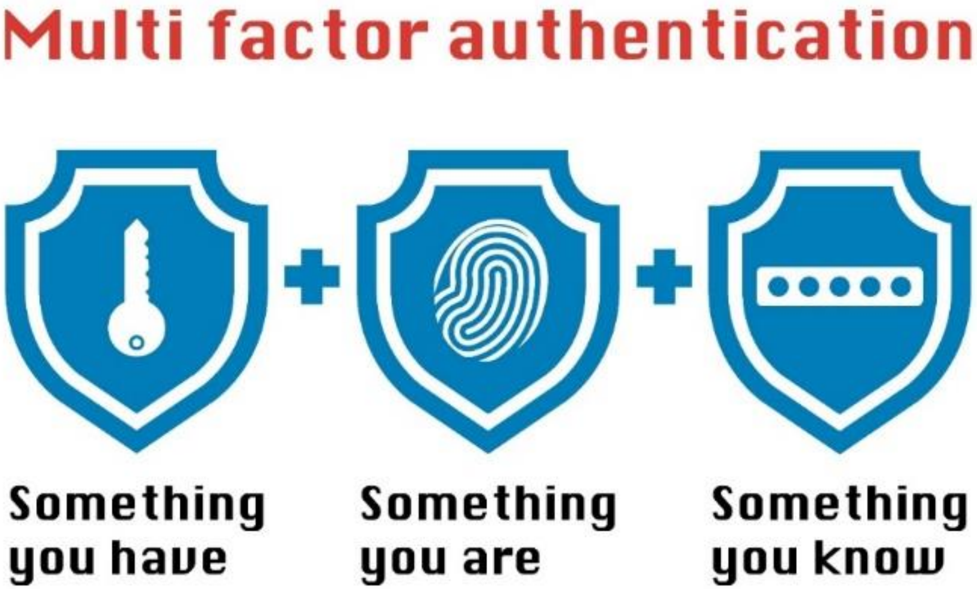


FACEBOOK now

Your login code is: **015-874**
Please do not share this with anyone.



Instagram (iamsarammorrison)	032 511
Slack (Suburbia Roller Derby):saramorriso...	115 639
Google (home)	712 988
Facebook	158 185
Amazon (home)	540 809
Discord (s)	796 919
Robinhood	



Multi factor authentication

Something you have + Something you are + Something you know

Social Engineering

Social Engineering Losses

2021 Losses

$6.9B in total (up from $4.2B in 2019)

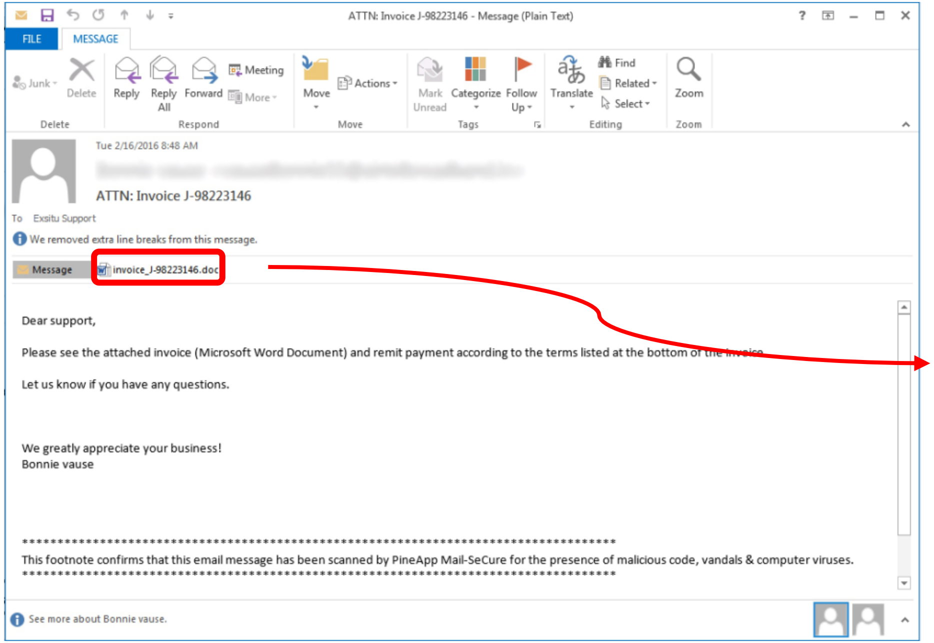
Ransomware: $49M in losses

Business Email Compromise: $2.4B (**35% of all losses related to cybercrime**)

Tech support scam losses up over 137% to over $347.5M

Complaints only increased ~8%, yet losses increased ~60%

Business Email Compromise



ATTN: Invoice J-98223146 - Message (Plain Text)

Tue 2/16/2016 8:48 AM

[redacted]

ATTN: Invoice J-98223146

To Exsitu Support

We removed extra line breaks from this message.

invoice_J-98223146.doc

Dear support,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

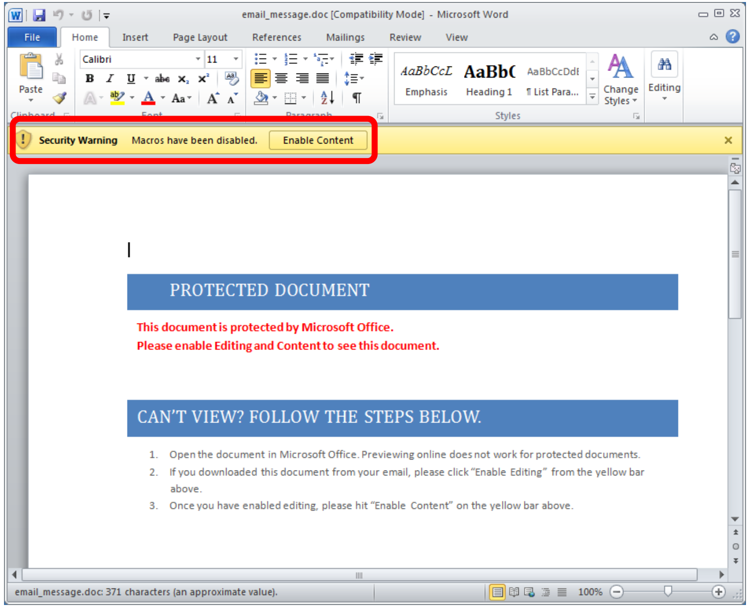
We greatly appreciate your business!
Bonnie vause

****

This footnote confirms that this email message has been scanned by PineApp Mail-SeCure for the presence of malicious code, vandals & computer viruses.

****

See more about Bonnie vause.



email_message.doc [Compatibility Mode] - Microsoft Word

Security Warning Macros have been disabled. Enable Content

PROTECTED DOCUMENT

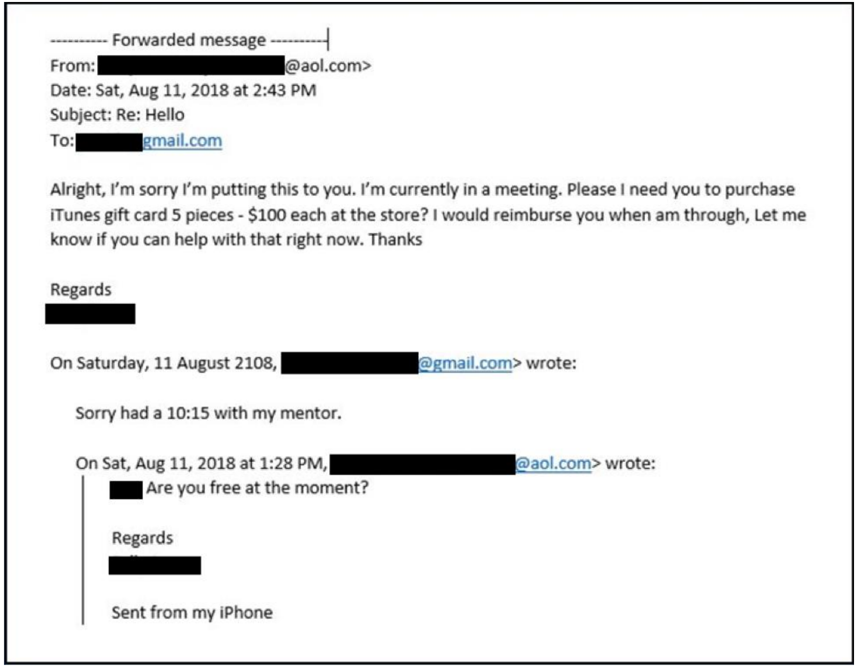
This document is protected by Microsoft Office.
Please enable Editing and Content to see this document.

CAN'T VIEW? FOLLOW THE STEPS BELOW.

1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enabled editing, please hit "Enable Content" on the yellow bar above.

email_message.doc: 371 characters (an approximate value).

Gift Card Scams



---------- Forwarded message ---------
From: [redacted]@aol.com>
Date: Sat, Aug 11, 2018 at 2:43 PM
Subject: Re: Hello
To: [redacted]gmail.com

Alright, I'm sorry I'm putting this to you. I'm currently in a meeting. Please I need you to purchase iTunes gift card 5 pieces - $100 each at the store? I would reimburse you when am through, Let me know if you can help with that right now. Thanks

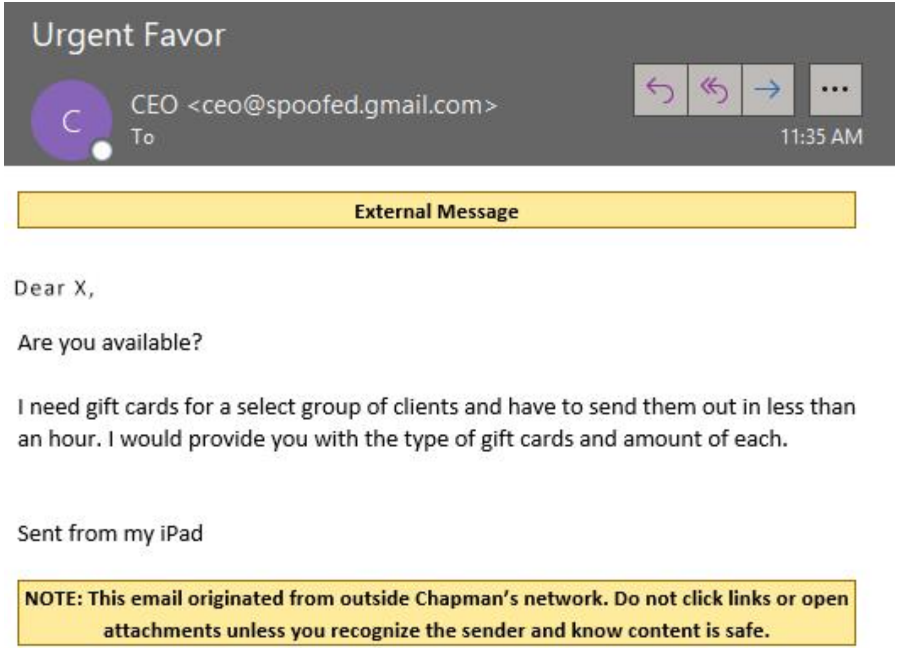
Regards
[redacted]

On Saturday, 11 August 2108, [redacted]@gmail.com> wrote:

Sorry had a 10:15 with my mentor.

On Sat, Aug 11, 2018 at 1:28 PM, [redacted]@aol.com> wrote:

> [redacted] Are you free at the moment?
>
> Regards
> [redacted]
>
> Sent from my iPhone



Urgent Favor

CEO <ceo@spoofed.gmail.com>
To
11:35 AM

External Message

Dear X,

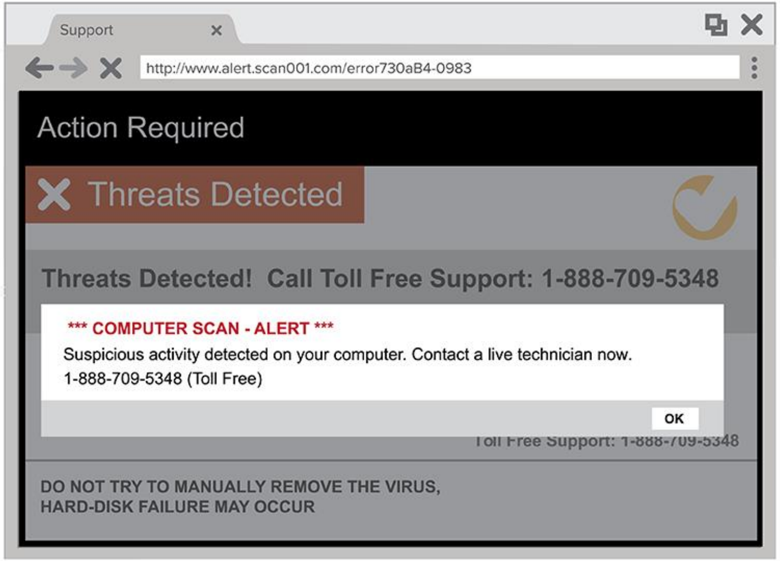
Are you available?

I need gift cards for a select group of clients and have to send them out in less than an hour. I would provide you with the type of gift cards and amount of each.

Sent from my iPad

NOTE: This email originated from outside Chapman's network. Do not click links or open attachments unless you recognize the sender and know content is safe.

Tech Support Scams



http://www.alert.scan001.com/error730aB4-0983

Action Required

☒ Threats Detected

Threats Detected! Call Toll Free Support: 1-888-709-5348

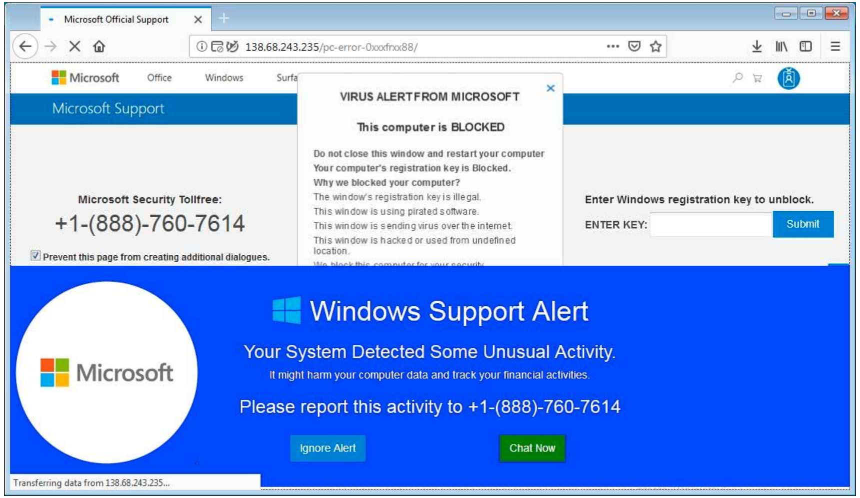
*** COMPUTER SCAN - ALERT ***

Suspicious activity detected on your computer. Contact a live technician now.
1-888-709-5348 (Toll Free)

Toll Free Support: 1-888-709-5348

DO NOT TRY TO MANUALLY REMOVE THE VIRUS,
HARD-DISK FAILURE MAY OCCUR

Incident report submitted to NJCCIC:
Amount stolen was more than $838,200.00.



138.68.243.235/pc-error-0xxxfrxx88/

Microsoft Support

Microsoft Security Tollfree:
+1-(888)-760-7614

☑ Prevent this page from creating additional dialogues.

VIRUS ALERTFROM MICROSOFT

This computer is BLOCKED

Do not close this window and restart your computer
Your computer's registration key is Blocked.
Why we blocked your computer?
The window's registration key is illegal.
This window is using pirated software.
This window is sending virus over the internet.
This window is hacked or used from undefined location.
We block this computer for your security.

Enter Windows registration key to unblock.

ENTER KEY:

Windows Support Alert

Your System Detected Some Unusual Activity.

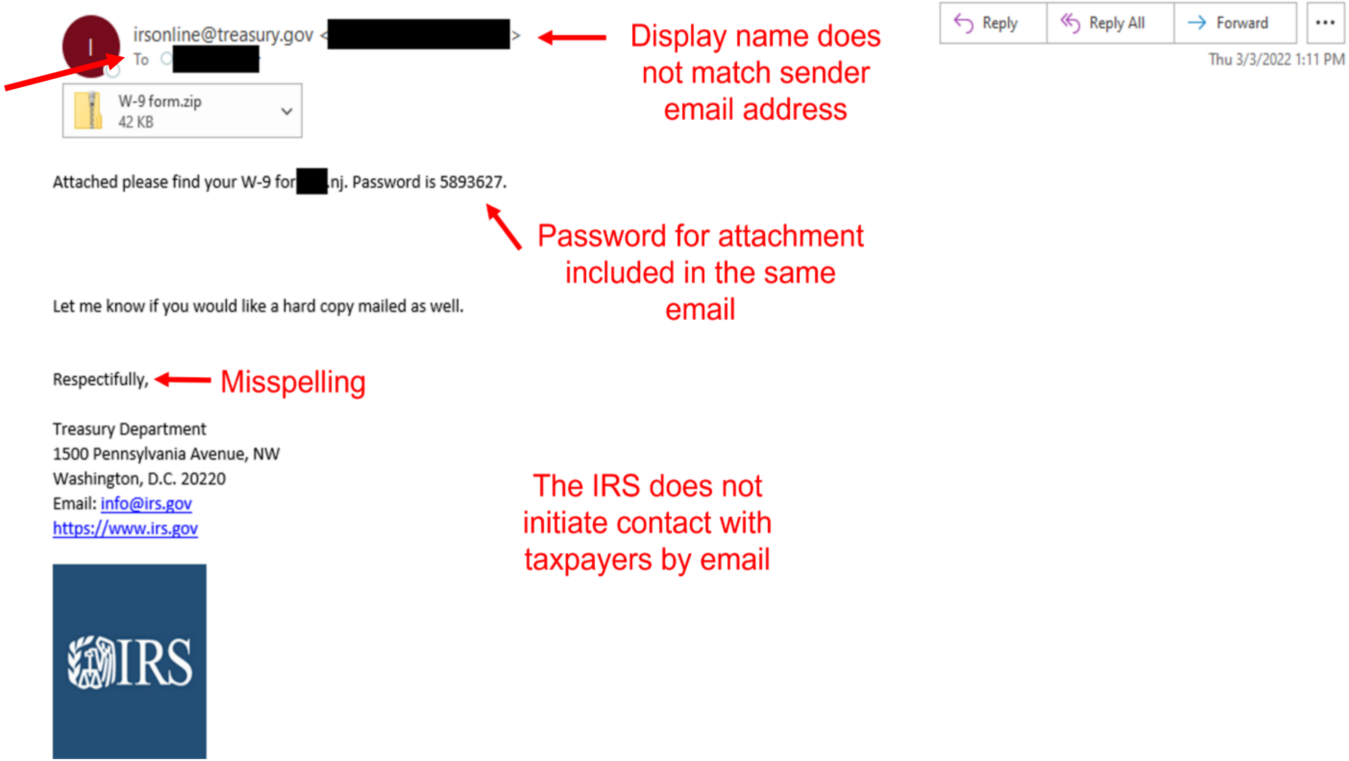
It might harm your computer data and track your financial activities.

Please report this activity to +1-(888)-760-7614

Transferring data from 138.68.243.235...

Email-Based Threats

Government Impersonation



irsonline@treasury.gov <[redacted]>

To [redacted]

Thu 3/3/2022 1:11 PM

Attached please find your W-9 for[redacted]nj. Password is 5893627.

Let me know if you would like a hard copy mailed as well.

Respectifully,

Treasury Department
1500 Pennsylvania Avenue, NW
Washington, D.C. 20220
Email: info@irs.gov
https://www.irs.gov

IRS

Almost always see display name spoofing

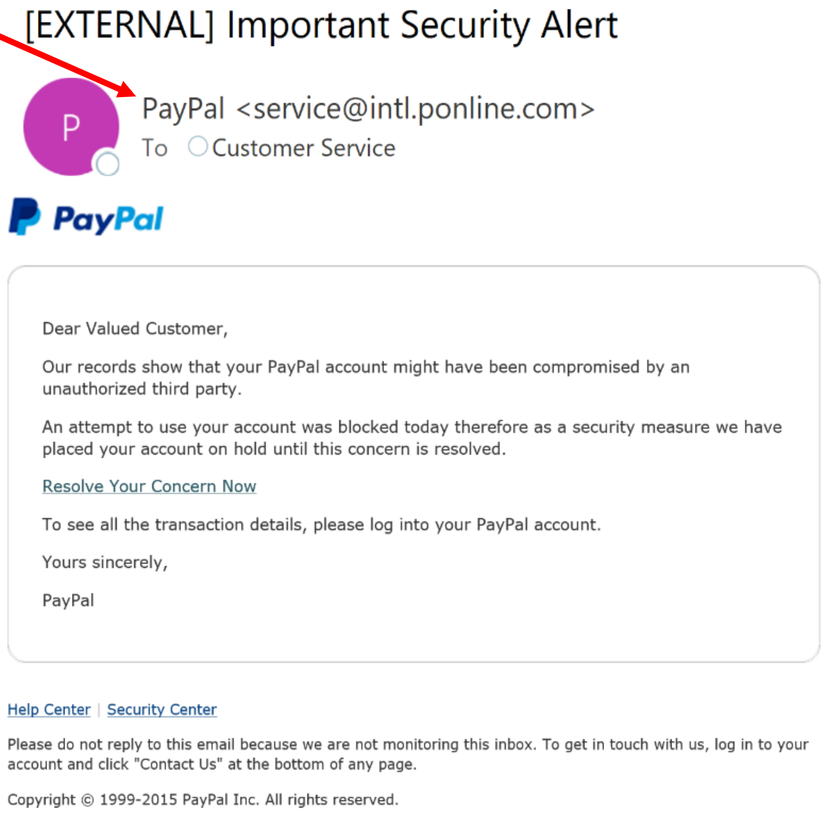
Display name does not match sender email address

Password for attachment included in the same email

Misspelling

The IRS does not initiate contact with taxpayers by email

Impersonation/Branding



Display name spoofing

Branding

[EXTERNAL] Important Security Alert

P

PayPal <service@intl.ponline.com>

To ○Customer Service

PayPal

Dear Valued Customer,

Our records show that your PayPal account might have been compromised by an unauthorized third party.

An attempt to use your account was blocked today therefore as a security measure we have placed your account on hold until this concern is resolved.

Resolve Your Concern Now

To see all the transaction details, please log into your PayPal account.

Yours sincerely,

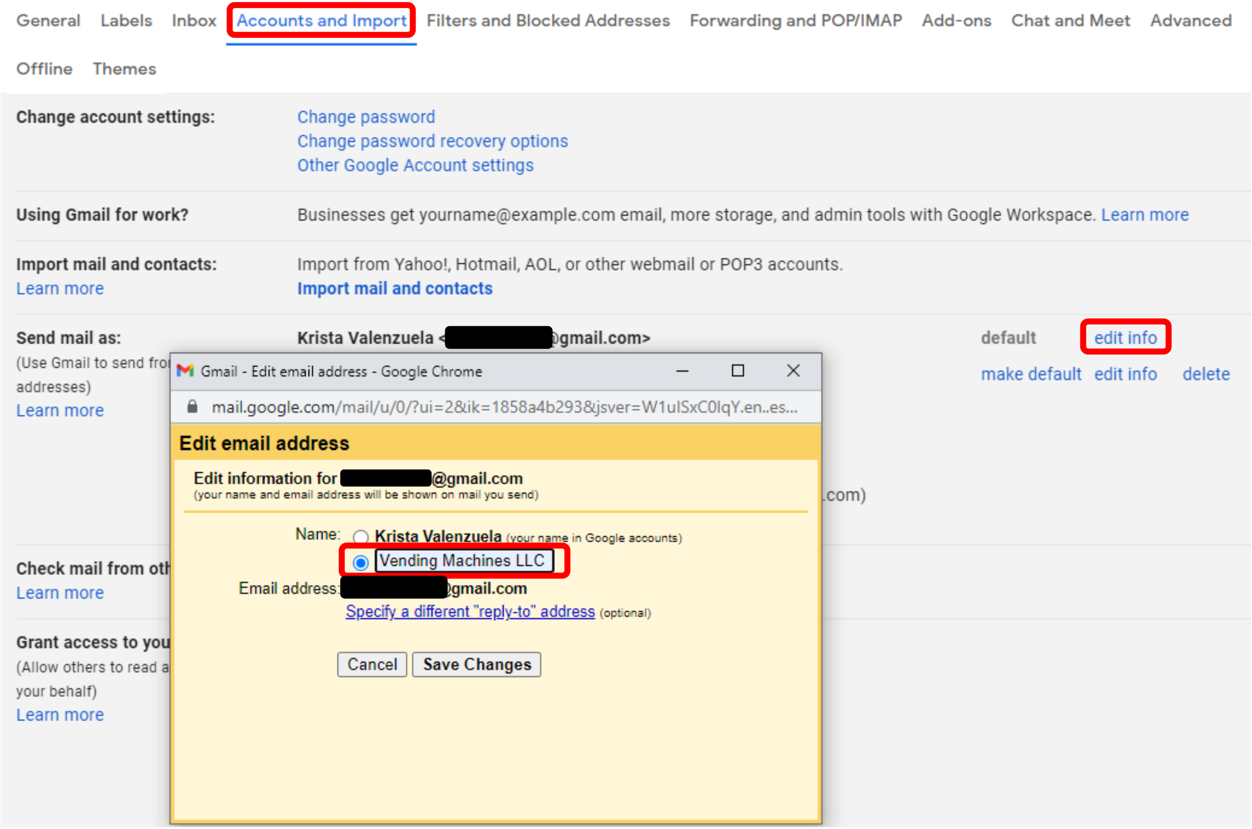
PayPal

Help Center | Security Center

Please do not reply to this email because we are not monitoring this inbox. To get in touch with us, log in to your account and click "Contact Us" at the bottom of any page.

Copyright © 1999-2015 PayPal Inc. All rights reserved.

Display Name Spoofing



Change account settings: Change password
Change password recovery options
Other Google Account settings

Using Gmail for work? Businesses get yourname@example.com email, more storage, and admin tools with Google Workspace. Learn more

Import mail and contacts: Import from Yahoo!, Hotmail, AOL, or other webmail or POP3 accounts.
Learn more
Import mail and contacts

Send mail as: **Krista Valenzuela <[redacted]@gmail.com>** default edit info
(Use Gmail to send fro
addresses)
Learn more
make default edit info delete
.com)

Check mail from oth
Learn more

Grant access to you
(Allow others to read a
your behalf)
Learn more

Gmail - Edit email address - Google Chrome

mail.google.com/mail/u/0/?ui=2&ik=1858a4b293&jsver=W1uISxC0lqY.en..es...

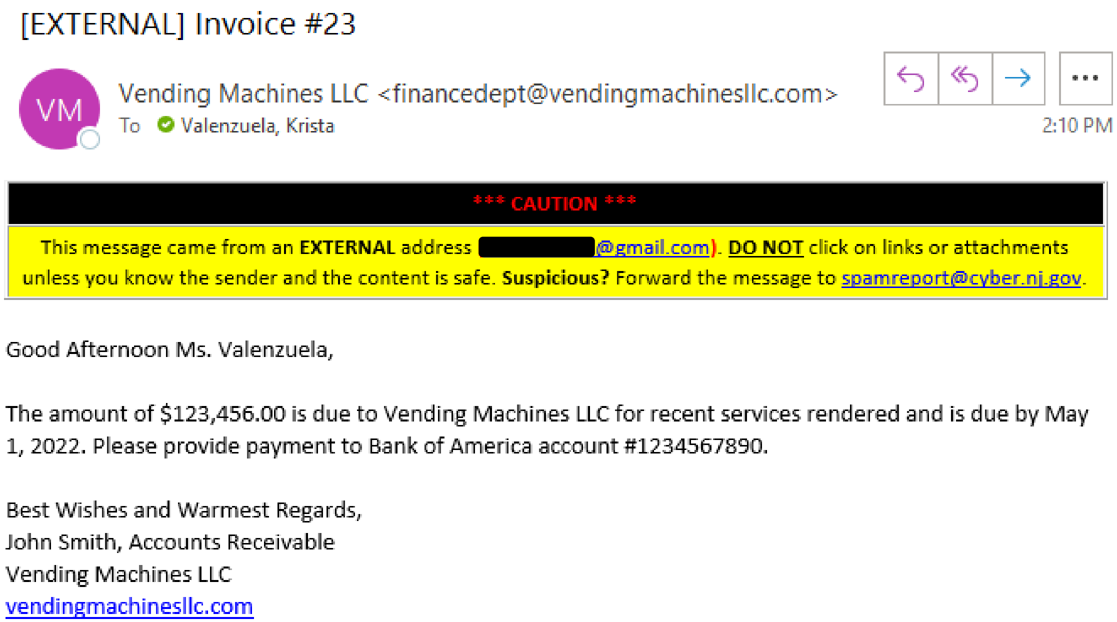
Edit email address

Edit information for [redacted]@gmail.com
(your name and email address will be shown on mail you send)

Name: ○ **Krista Valenzuela** (your name in Google accounts)
● Vending Machines LLC

Email address: [redacted]@gmail.com
Specify a different "reply-to" address (optional)

Spoofed Malicious Email



[EXTERNAL] Invoice #23

Vending Machines LLC <financedept@vendingmachinesllc.com>

To Valenzuela, Krista

2:10 PM

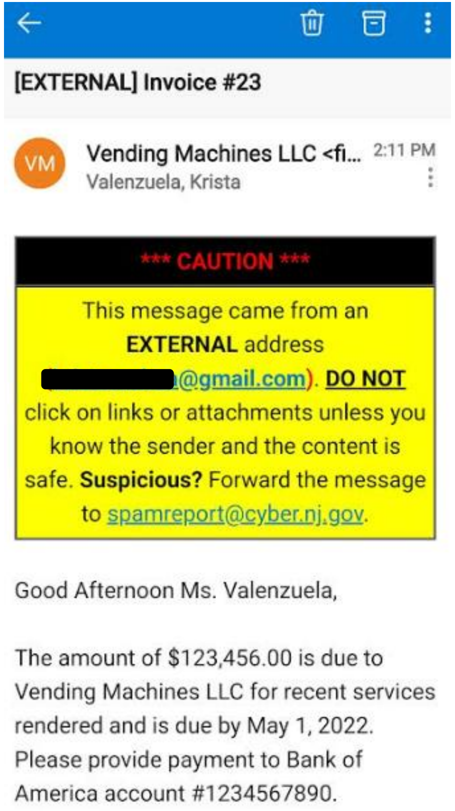
*** CAUTION ***

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. **Suspicious?** Forward the message to spamreport@cyber.nj.gov.

Good Afternoon Ms. Valenzuela,

The amount of $123,456.00 is due to Vending Machines LLC for recent services rendered and is due by May 1, 2022. Please provide payment to Bank of America account #1234567890.

Best Wishes and Warmest Regards,
John Smith, Accounts Receivable
Vending Machines LLC
vendingmachinesllc.com



[EXTERNAL] Invoice #23

Vending Machines LLC <fi...

Valenzuela, Krista

2:11 PM

*** 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. **Suspicious?** Forward the message to spamreport@cyber.nj.gov.

Good Afternoon Ms. Valenzuela,

The amount of $123,456.00 is due to Vending Machines LLC for recent services rendered and is due by May 1, 2022. Please provide payment to Bank of America account #1234567890.

Compromised Accounts

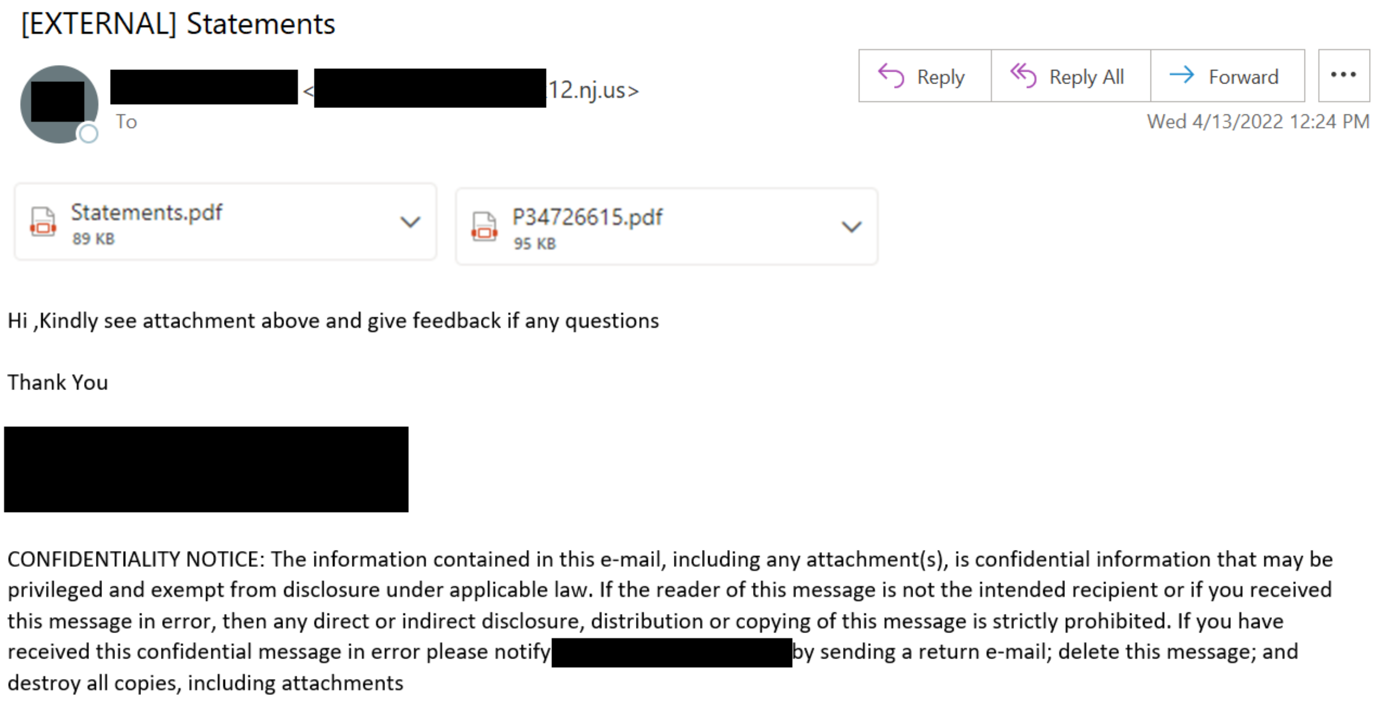
- Attack vectors include **email-based** threats or the use of brute force/**credential stuffing** attacks.
- A threat actor may target a user in order to gain **access to their email account**.
- This allows them to conduct **further attacks** from a **legitimate** account.

What if your account is compromised?

- Change password (for this and other accounts), enable MFA.
- Check for auto-forward or reply-to rules.

Compromised Accounts – BEC

Links, not files.



[EXTERNAL] Statements

[redacted] [redacted] [redacted] <[redacted]12.nj.us>

To

Wed 4/13/2022 12:24 PM

Statements.pdf
89 KB

P34726615.pdf
95 KB

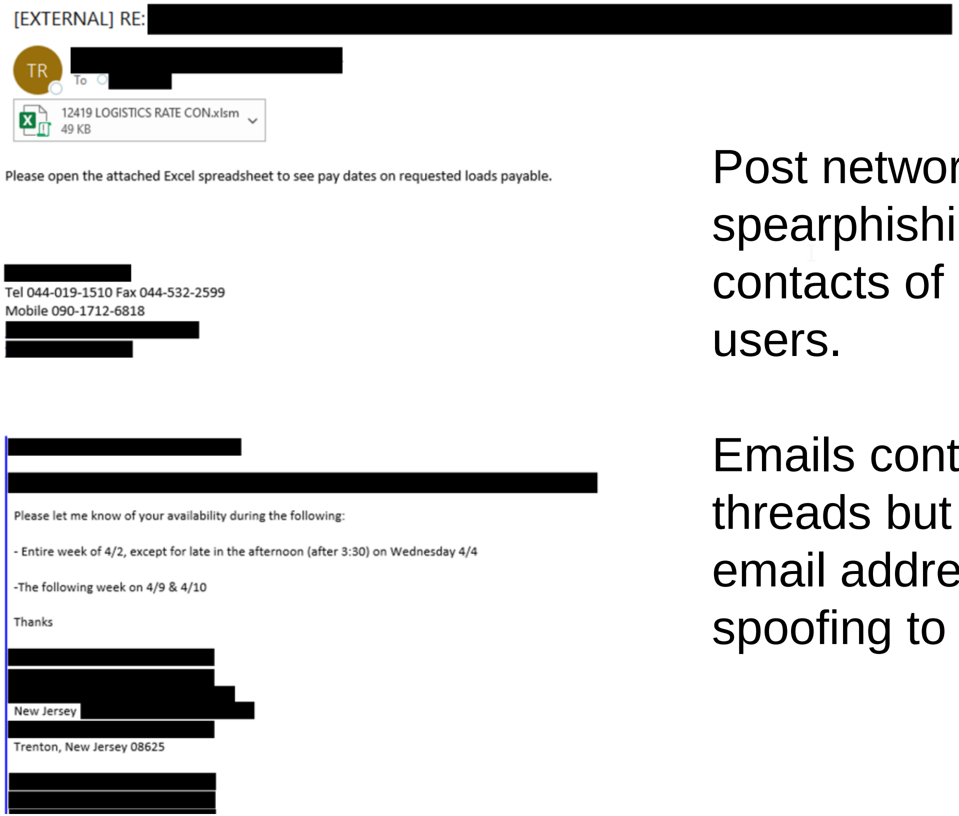
Hi ,Kindly see attachment above and give feedback if any questions

Thank You

[redacted]

CONFIDENTIALITY NOTICE: The information contained in this e-mail, including any attachment(s), is confidential information that may be privileged and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient or if you received this message in error, then any direct or indirect disclosure, distribution or copying of this message is strictly prohibited. If you have received this confidential message in error please notify [redacted] by sending a return e-mail; delete this message; and destroy all copies, including attachments

Thread Hijacking



[EXTERNAL] RE: [redacted]

[redacted]

To [redacted]

12419 LOGISTICS RATE CON.xlsm
49 KB

Please open the attached Excel spreadsheet to see pay dates on requested loads payable.

[redacted]
Tel 044-019-1510 Fax 044-532-2599
Mobile 090-1712-6818
[redacted]

[redacted]

Please let me know of your availability during the following:

- Entire week of 4/2, except for late in the afternoon (after 3:30) on Wednesday 4/4

-The following week on 4/9 & 4/10

Thanks

[redacted]
New Jersey [redacted]
[redacted]
Trenton, New Jersey 08625

[redacted]

Post network compromise spearphishing campaigns targeting contacts of compromised network users.

Emails contain legitimate conversation threads but often come from external email addresses, using display name spoofing to appear authentic.

Cyber Resiliency

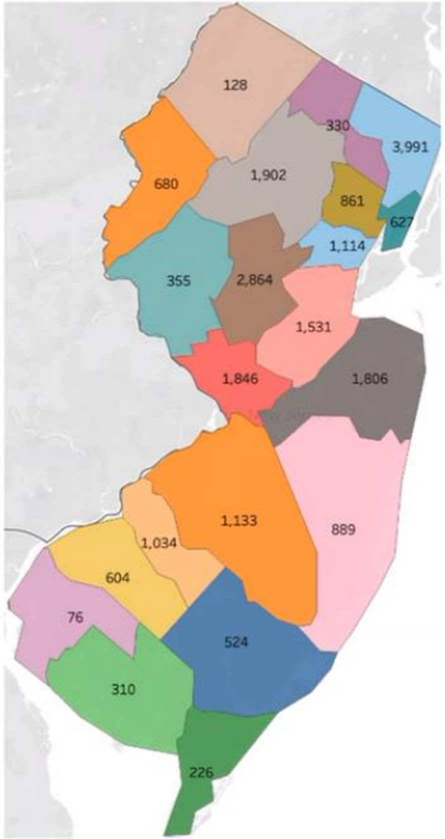
Increase Resiliency

- Segment Networks
- [✓ Enable MFA for ALL Accounts & Users]
- [✓ Keep Systems/Apps Updated]
- Endpoint Detection & Response
- [✓ Delete Unused Programs & Applications]
- [✓ Maintain awareness]
- Establish & Update Inventory
- Reduce External Exposure
- Application Allowlists
- Limit Acceptable File Types
- [✓ COOP/DRP TTX]

NJCCIC Services to Public Sector Organizations

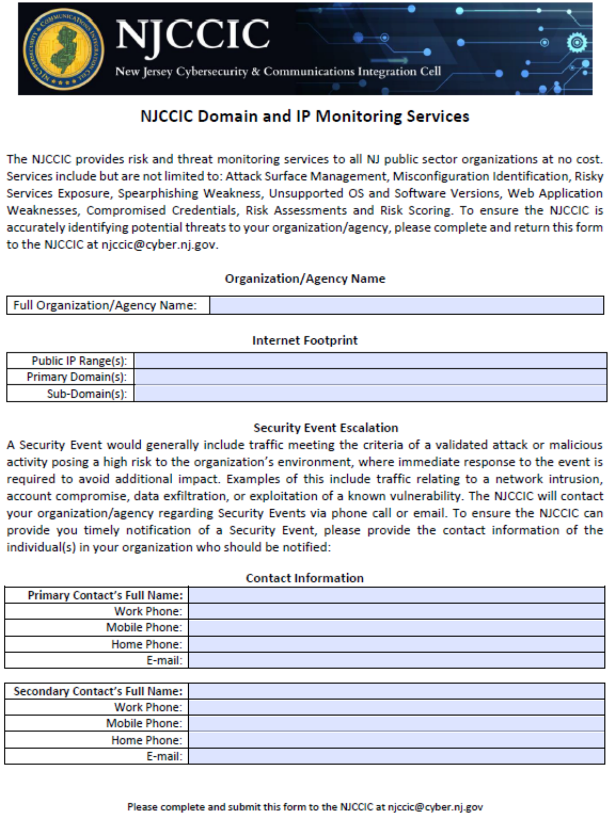
Collective Defense:

- Bulletins, Alerts, Advisories
- Threat Briefings
- Website, Portal, Social Media
- Risk Management Services
  - Attack Surface Management
  - Security Scorecard
  - Risk Assessments
- Incident Reporting
- Limited Incident Response
- Statewide Threat Grid (Albert Sensors)
- Training
  - Instructor-led
  - Self-paced
  - Cyber Range
- Notifications – UHBP, Vulnerabilities, Risky Services



Domain and IP Monitoring Services

Provide domains, IPs/ranges, and contacts in order to begin receiving services (such as that on the next slide) and ensure you receive accurate information.



NJCCIC
New Jersey Cybersecurity & Communications Integration Cell

NJCCIC Domain and IP Monitoring Services

The NJCCIC provides risk and threat monitoring services to all NJ public sector organizations at no cost. Services include but are not limited to: Attack Surface Management, Misconfiguration Identification, Risky Services Exposure, Spearphishing Weakness, Unsupported OS and Software Versions, Web Application Weaknesses, Compromised Credentials, Risk Assessments and Risk Scoring. To ensure the NJCCIC is accurately identifying potential threats to your organization/agency, please complete and return this form to the NJCCIC at njccic@cyber.nj.gov.

Organization/Agency Name

Full Organization/Agency Name:	

Internet Footprint

Public IP Range(s):	
Primary Domain(s):	
Sub-Domain(s):	

Security Event Escalation

A Security Event would generally include traffic meeting the criteria of a validated attack or malicious activity posing a high risk to the organization's environment, where immediate response to the event is required to avoid additional impact. Examples of this include traffic relating to a network intrusion, account compromise, data exfiltration, or exploitation of a known vulnerability. The NJCCIC will contact your organization/agency regarding Security Events via phone call or email. To ensure the NJCCIC can provide you timely notification of a Security Event, please provide the contact information of the individual(s) in your organization who should be notified:

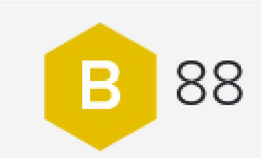
Contact Information

Primary Contact's Full Name:	
Work Phone:	
Mobile Phone:	
Home Phone:	
E-mail:	

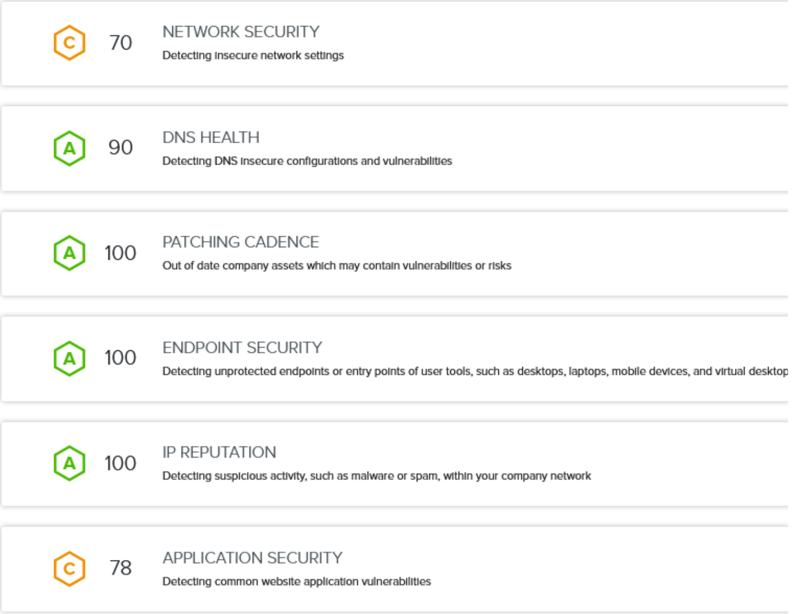
Secondary Contact's Full Name:	
Work Phone:	
Mobile Phone:	
Home Phone:	
E-mail:	

Please complete and submit this form to the NJCCIC at njccic@cyber.nj.gov

NJCCIC Services



B 88



C 70 NETWORK SECURITY
Detecting insecure network settings

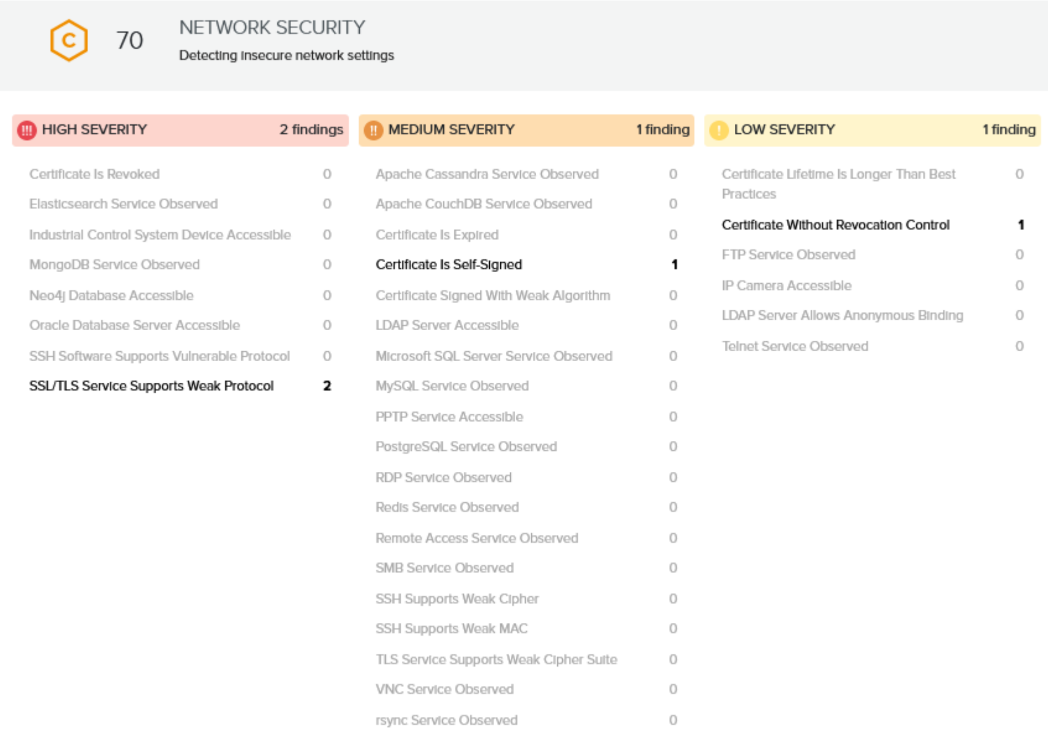
A 90 DNS HEALTH
Detecting DNS insecure configurations and vulnerabilities

A 100 PATCHING CADENCE
Out of date company assets which may contain vulnerabilities or risks

A 100 ENDPOINT SECURITY
Detecting unprotected endpoints or entry points of user tools, such as desktops, laptops, mobile devices, and virtual desktop

A 100 IP REPUTATION
Detecting suspicious activity, such as malware or spam, within your company network

C 78 APPLICATION SECURITY
Detecting common website application vulnerabilities



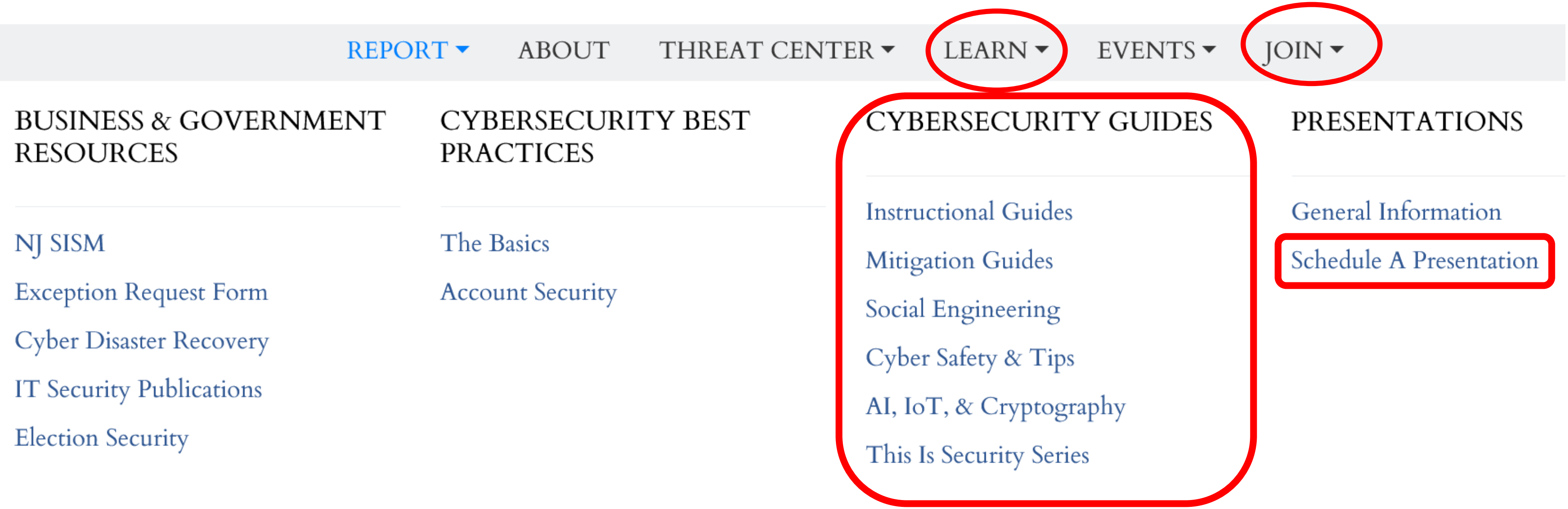
C 70 NETWORK SECURITY
Detecting insecure network settings

HIGH SEVERITY	2 findings
Certificate Is Revoked	0
Elasticsearch Service Observed	0
Industrial Control System Device Accessible	0
MongoDB Service Observed	0
Neo4j Database Accessible	0
Oracle Database Server Accessible	0
SSH Software Supports Vulnerable Protocol	0
SSL/TLS Service Supports Weak Protocol	2

MEDIUM SEVERITY	1 finding
Apache Cassandra Service Observed	0
Apache CouchDB Service Observed	0
Certificate Is Expired	0
Certificate Is Self-Signed	1
Certificate Signed With Weak Algorithm	0
LDAP Server Accessible	0
Microsoft SQL Server Service Observed	0
MySQL Service Observed	0
PPTP Service Accessible	0
PostgreSQL Service Observed	0
RDP Service Observed	0
Redis Service Observed	0
Remote Access Service Observed	0
SMB Service Observed	0
SSH Supports Weak Cipher	0
SSH Supports Weak MAC	0
TLS Service Supports Weak Cipher Suite	0
VNC Service Observed	0
rsync Service Observed	0

LOW SEVERITY	1 finding
Certificate Lifetime Is Longer Than Best Practices	0
Certificate Without Revocation Control	1
FTP Service Observed	0
IP Camera Accessible	0
LDAP Server Allows Anonymous Binding	0
Telnet Service Observed	0

NJCCIC Resources



BUSINESS & GOVERNMENT RESOURCES

- NJ SISM
- Exception Request Form
- Cyber Disaster Recovery
- IT Security Publications
- Election Security

CYBERSECURITY BEST PRACTICES

- The Basics
- Account Security

CYBERSECURITY GUIDES

- Instructional Guides
- Mitigation Guides
- Social Engineering
- Cyber Safety & Tips
- AI, IoT, & Cryptography
- This Is Security Series

PRESENTATIONS

- General Information
- Schedule A Presentation

Connect with the NJCCIC

✉ NJCCIC@CYBER.NJ.GOV

☎ 1-833-4-NJCCIC
(1-833-465-2242)

@NJCYBERSECURITY

CYBER.NJ.GOV