NJ Cybersecurity & Communications Integration Cell

Prevent, Detect, Respond

Office of the Attorney General State of New Jersey

NJ Office of Homeland Security and Preparedness

Office of the ROIC Regional Operations & Intelligence Center New Jersey

State Police NJ

NJ Office of Information Technology

@NJCybersecurity

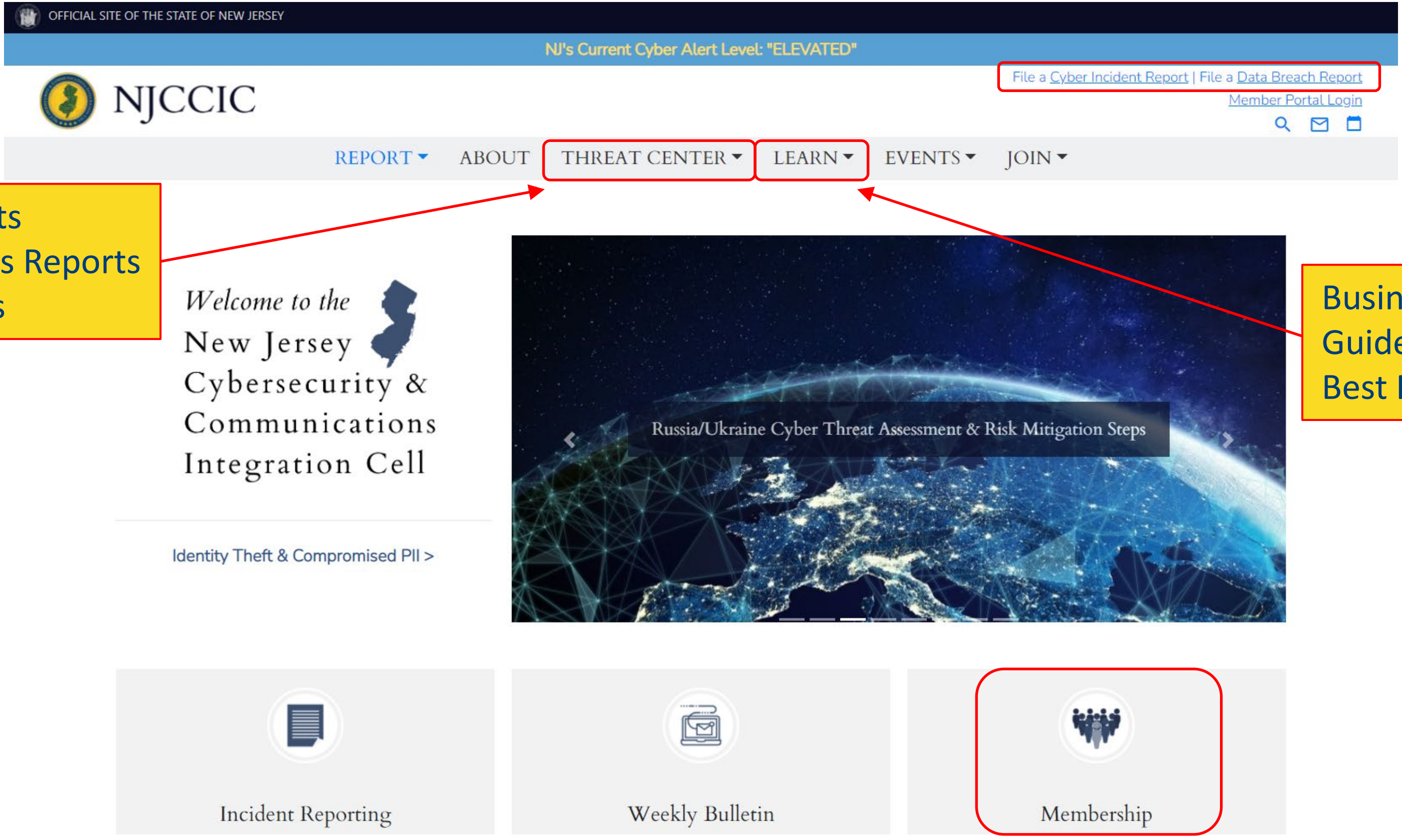
cyber.nj.gov

NJCCIC@cyber.nj.gov

Cybersecurity: How Can PII Be Compromised

October 21, 2022

Resource for New Jersey - www.cyber.nj.gov



OFFICIAL SITE OF THE STATE OF NEW JERSEY

NJ's Current Cyber Alert Level: "ELEVATED"

NJCCIC

File a Cyber Incident Report | File a Data Breach Report

Member Portal Login

REPORT ABOUT THREAT CENTER LEARN EVENTS JOIN

Welcome to the
New Jersey Cybersecurity & Communications Integration Cell

Identity Theft & Compromised PII >

Russia/Ukraine Cyber Threat Assessment & Risk Mitigation Steps

Incident Reporting

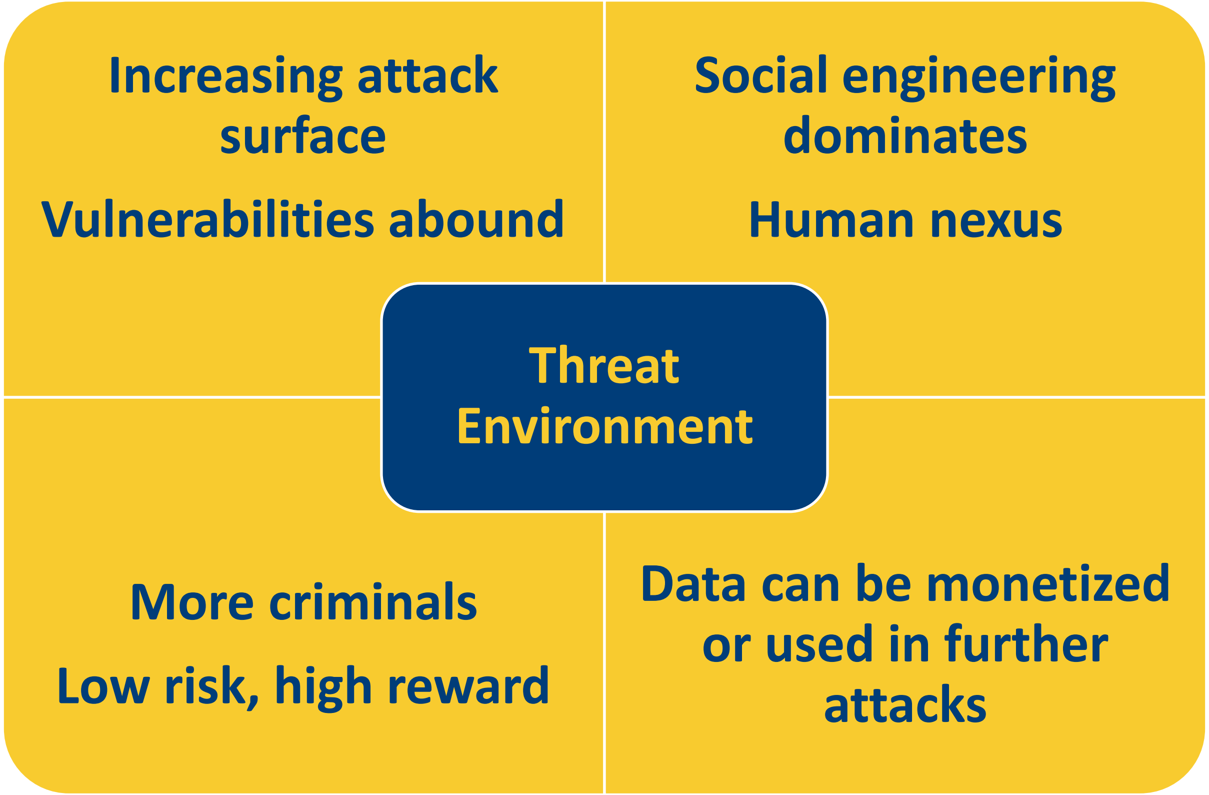
Weekly Bulletin

Membership

Current Threats
Threat Analysis Reports
Threat Profiles

Business Resources
Guides
Best Practices

Cyber Threat Landscape



Increasing attack surface

Vulnerabilities abound

Social engineering dominates

Human nexus

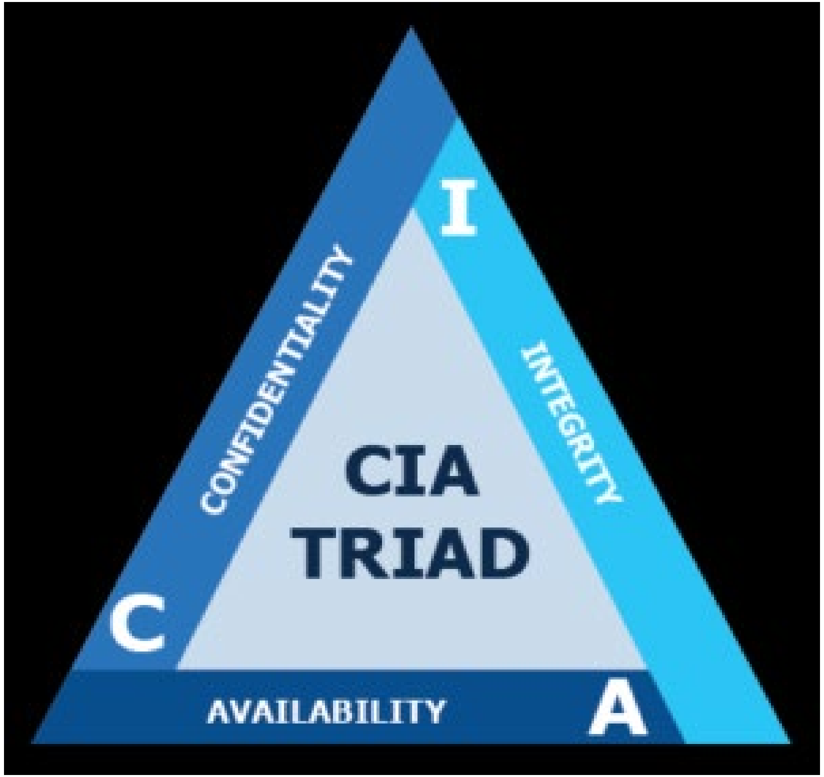
Threat Environment

More criminals

Low risk, high reward

Data can be monetized or used in further attacks

CIA Triad



Privacy and safety

Impacts of Cyber Threats

Risk-based Approach

Vulnerability	Threat	Consequence
People	Means	Financial
Processes	Motivation	Operational
Technology	Opportunity	Physical

If valuable data is accessible and not secured, it is a matter of when, not if, it is located and exploited.

What is PII?

New Jersey defines PII broadly to include **name, address, telephone number, Social Security number, driver's license number, and passport number** as well as height and weight, biometric information, race, religion, sexual orientation, health information, and commercial or financial information.

N.J.S.A. 56:8-161 et seq., applies to any company or person conducting business in New Jersey, which compiles or maintains computerized records that include personal information.
"Personal information" is defined as "an individual's first name or first initial and last name linked with any one or more of the following data elements:
(1) Social Security number (SSN);
(2) driver's license number or state identification card number; or
(3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

How Can PII Be Compromised?

- **Phishing attacks**
- **Impersonation scams**
- Credential-stuffing attacks
- Brute-force attempts
- Misconfigured or unpatched systems

Examples of PII Compromises

- Everyone is a target!
- Fraudulent wire transfers to close on property
- Payoff instructions altered during refinance transaction
- New payment instructions for rental payment

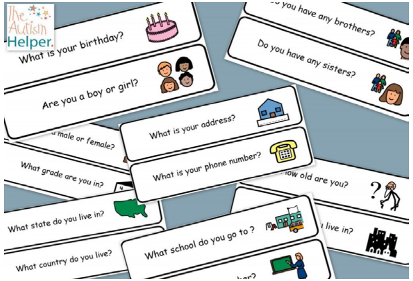
Best Practices

- Use verified, secure, and encrypted websites
- Navigate directly to authentic or official websites

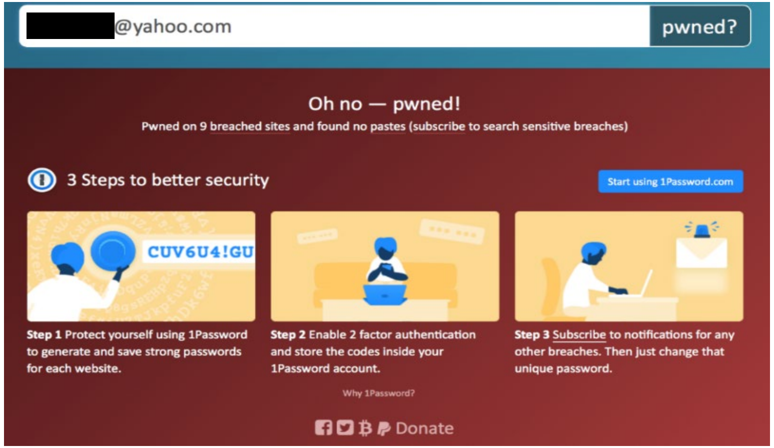
- Don’t share or post account info or passwords
- Avoid auto-saving info in OS, browser, website, apps
- Don’t post personal or work info online
- Make it hard to find or guess info about you

- Google yourself
- Reduce digital footprint (How Big is Your Footprint?)
- Ask family/friends to respect your privacy
- Don’t add anyone you don’t personally know or trust to social networks

- Stop and think before you click
- Safeguard your info and accounts regardless of communication



HaveIBeenPwned.com



[redacted]@yahoo.com

Oh no — pwned!

Pwned on 9 breached sites and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

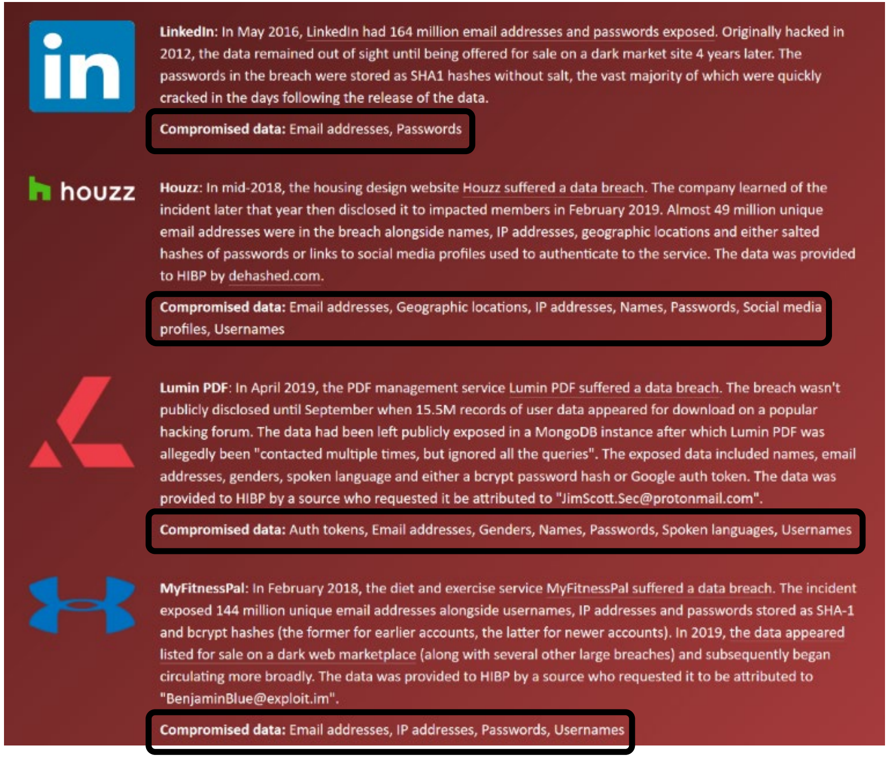
Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

Why 1Password?

- Check regularly
- Change passwords immediately
- Refrain from password reuse



LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

Houzz: In mid-2018, the housing design website Houzz suffered a data breach. The company learned of the incident later that year then disclosed it to impacted members in February 2019. Almost 49 million unique email addresses were in the breach alongside names, IP addresses, geographic locations and either salted hashes of passwords or links to social media profiles used to authenticate to the service. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Geographic locations, IP addresses, Names, Passwords, Social media profiles, Usernames

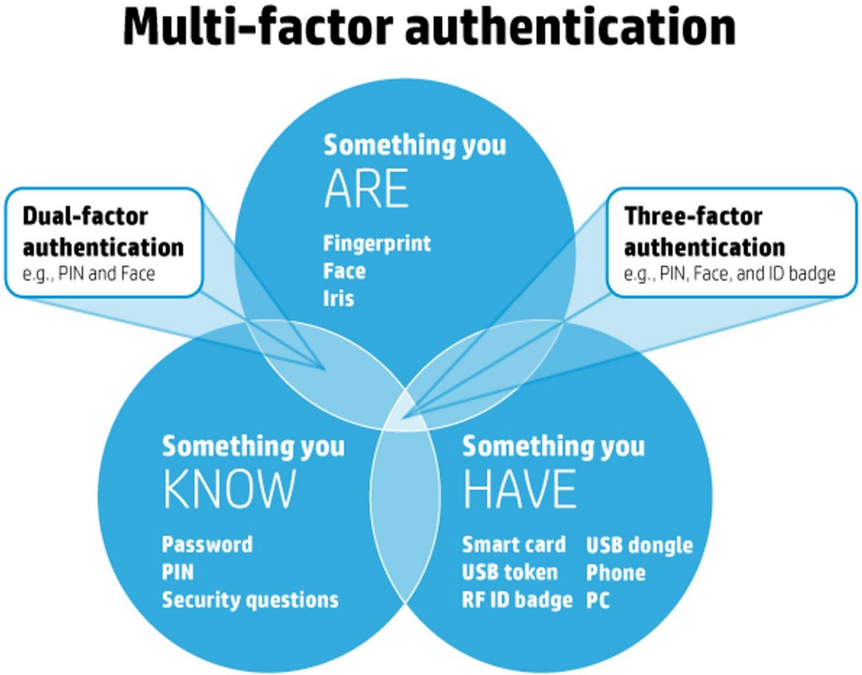
Lumin PDF: In April 2019, the PDF management service Lumin PDF suffered a data breach. The breach wasn't publicly disclosed until September when 15.5M records of user data appeared for download on a popular hacking forum. The data had been left publicly exposed in a MongoDB instance after which Lumin PDF was allegedly been "contacted multiple times, but ignored all the queries". The exposed data included names, email addresses, genders, spoken language and either a bcrypt password hash or Google auth token. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Auth tokens, Email addresses, Genders, Names, Passwords, Spoken languages, Usernames

MyFitnessPal: In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Compromised data: Email addresses, IP addresses, Passwords, Usernames

Multi-Factor Authentication (MFA)



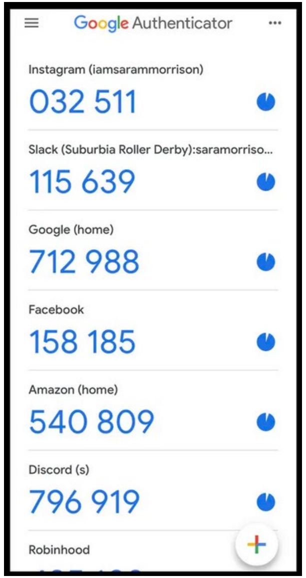
Enable (option) v. Enforce (mandatory)

Multi-Factor Authentication (MFA)

Best method to protect against account compromise as a result of credential theft

Choose **authentication apps or hardware tokens** over SMS or email codes

Establish PIN on cellular account to help prevent SIM swapping attacks



Instagram (iamsarammorrison)
032 511

Slack (Suburbia Roller Derby):saramorriso...
115 639

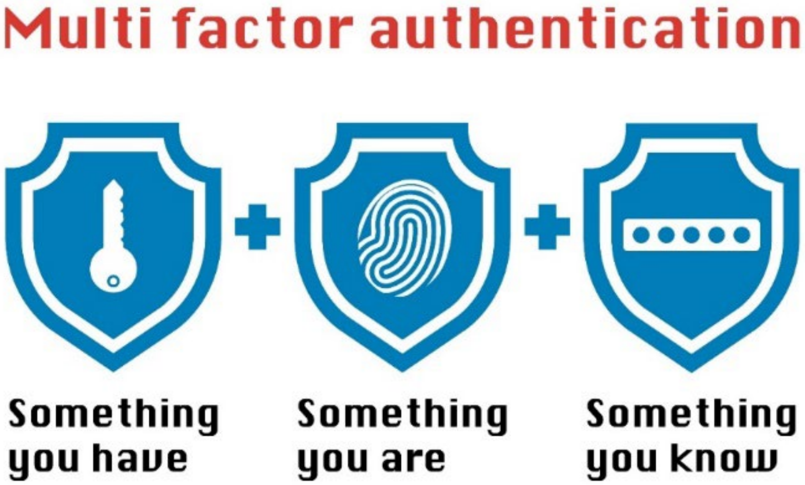
Google (home)
712 988

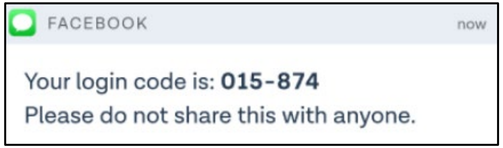
Facebook
158 185

Amazon (home)
540 809

Discord (s)
796 919

Robinhood



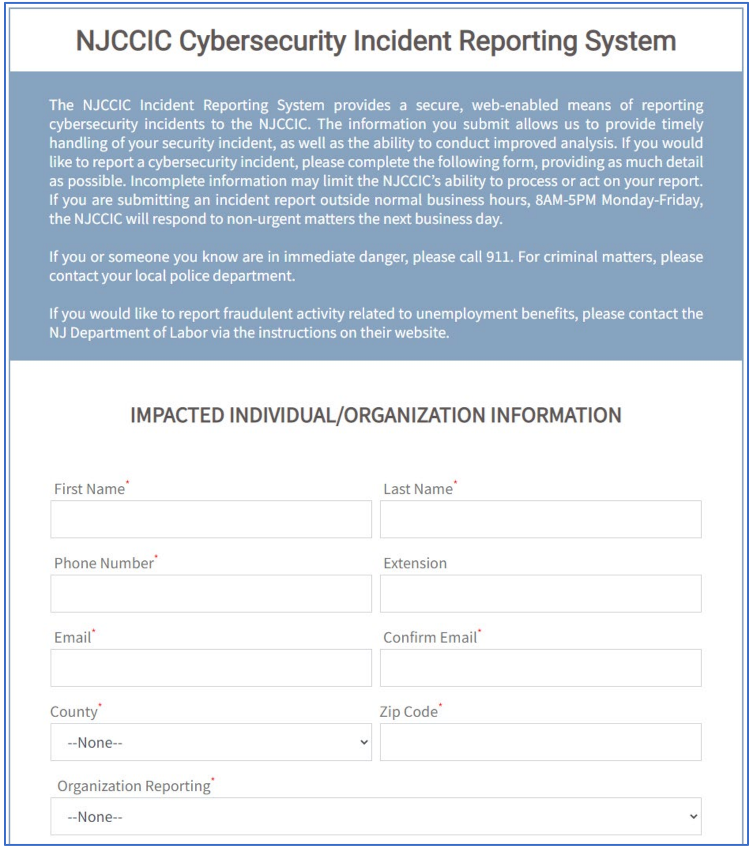


Your login code is: **015-874**
Please do not share this with anyone.

Report a Cyber Incident

https://www.cyber.nj.gov/cyber-incident

- Organizations may not be aware of specific threats, trends, suspicious indicators, or vulnerabilities
- Information as to what happened, attack vector, sector impact, and data exfiltration
- Provide guidance and offer direction on mitigation and prevention
- Report to law enforcement as insurance company requirement and organizations may not have resources
- Share information to protect others



NJCCIC Cybersecurity Incident Reporting System

The NJCCIC Incident Reporting System provides a secure, web-enabled means of reporting cybersecurity incidents to the NJCCIC. The information you submit allows us to provide timely handling of your security incident, as well as the ability to conduct improved analysis. If you would like to report a cybersecurity incident, please complete the following form, providing as much detail as possible. Incomplete information may limit the NJCCIC's ability to process or act on your report. If you are submitting an incident report outside normal business hours, 8AM-5PM Monday-Friday, the NJCCIC will respond to non-urgent matters the next business day.

If you or someone you know are in immediate danger, please call 911. For criminal matters, please contact your local police department.

If you would like to report fraudulent activity related to unemployment benefits, please contact the NJ Department of Labor via the instructions on their website.

IMPACTED INDIVIDUAL/ORGANIZATION INFORMATION

First Name*

Last Name*

Phone Number*

Extension

Email*

Confirm Email*

County*

--None--

Zip Code*

Organization Reporting*

--None--

TLP: White

Report a Data Breach

Organizations ARE mandated by law to report data breaches

- Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, are required to disclose any breach of security of those computerized records…following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person.
- Submit data breach report at cyber.nj.gov/breach:
  - Data breach details (number of NJ residents affected, data compromised, and consumer notification)
  - NJCCIC for intelligence purposes
  - NJ State Police for possible criminal activity
  - NJ Office of Attorney General for consumer impact

Data Breaches, Law, Reporting

- State of New Jersey Data Breach Report Form
  https://www.cyber.nj.gov/breach/

- NJ Office of the Attorney General, Office of Consumer Protection
  https://www.njconsumeraffairs.gov/ocp/Pages/cyberfraud.aspx

- Identity Theft and Compromised PII
  https://www.cyber.nj.gov/informational-report/identity-theft-and-compromised-pii

Resources

- **Don’t Take the Bait! Phishing and Other Social Engineering Attacks**

https://www.cyber.nj.gov/informational-report/dont-take-the-bait-phishing-and-other-social-engineering-attacks

- **Passwords, Passwords, Passwords**

https://www.cyber.nj.gov/instructional-guides/passwords-passwords-passwords

- **Spotting a Spoofing**

https://www.cyber.nj.gov/informational-report/spotting-a-spoofing

- **Impersonation Scams**

https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/impersonation-scams

- **Multi-Factor Authentication (MFA): A Critical Step for Account Security**

https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/multi-factor-authentication-mfa-a-critical-step-for-account-security

Connect with the NJCCIC

NJCCIC@cyber.nj.gov

www.cyber.nj.gov

1-833-4-NJCCIC

@njcybersecurity

Sign up for membership at no cost