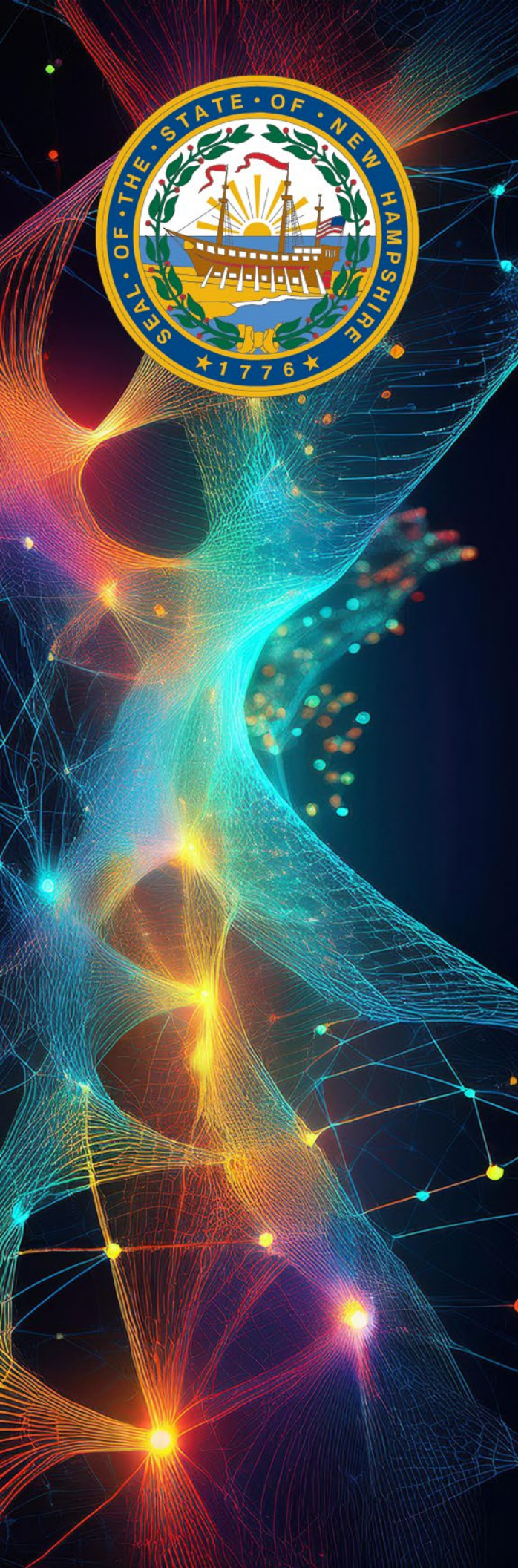


2025 New Hampshire Cyber Threat Assessment

Office of the Chief Information Security Officer

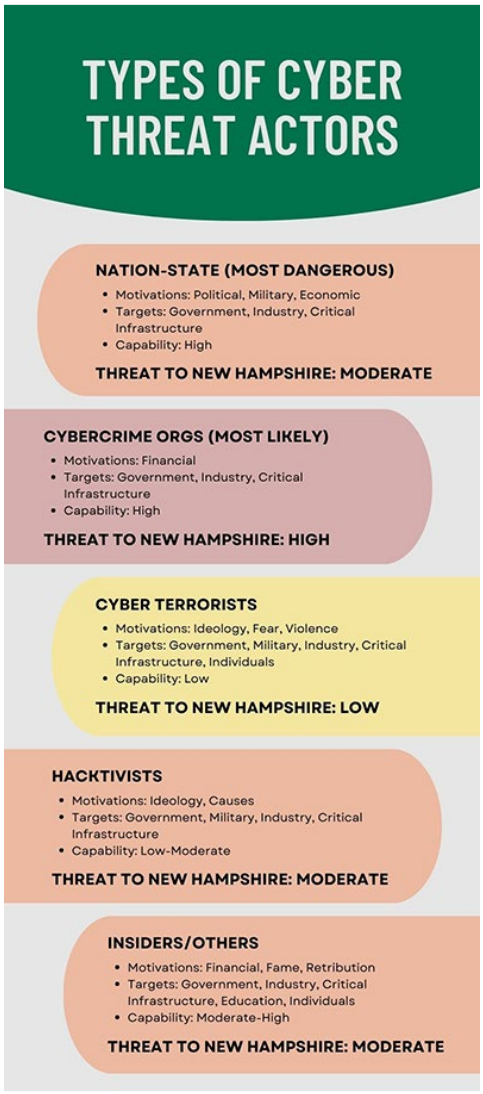
Department of Information Technology

“Phishers are phishing. Clickers are clicking. Grifters are grifting.”

Executive Summary

New Hampshire faces an evolving cyber threat landscape, characterized by cyberattacks that can be launched from anywhere in the world at any time of day or night.

- The most likely things users/administrators will see are phishing emails, attacks to compromise identities, business email compromise to enable good old-fashioned grifting, and ransomware attacks.
- Cybercrime organizations (Most Likely), Nation State Actors (Most Dangerous), Hacktivists, and others with diverse motivations and considerable technical capabilities pose significant threats.
- Enhanced by Generative AI, Phishing emails, links in text messages on mobile phones, and audio calls will be even more convincing than we have experienced to date which will require extensive training for our Human Intrusion Prevention Systems across Public Sector Organizations.



COMPROMISED LOGIN CREDENTIALS AS AN ATTACK VECTOR

In 2024, there were 63 cyber incidents in New Hampshire reported to the New Hampshire Public Risk Management Exchange (PRIMEX). 61 of these incidents were initiated with a Phishing email that resulted in a compromise of legitimate user credentials (usernames and passphrases). Only two were the result of unpatched vulnerabilities in systems that were exploited for access. Identity-based attacks are expected to remain the primary method of attack against New Hampshire public and private sector organizations, as well as the State's residents and businesses in 2025. This is why Executives use Fly-Away Kits!

INCIDENT REPORTING IS EVERYONE'S RESPONSIBILITY

If you work in State Government, it is very important to report a suspected cyber incident to DoIT Help Desk via email or phone as follows:

- Email: helpdesk@doit.nh.gov
- Phone: (603) 271-7555 (Outside of 7:30 AM to 4:30PM, dial the same number and select "Option 2")

TAKE AWAYS

Based on an analysis of cyberattack trends and emerging threats, in 2025 the State of New Hampshire will continue to see cyber-attacks against towns, cities, counties, critical infrastructure, health care organizations, K12 schools, higher education, and even individuals.

Most of these attacks will be from Cybercriminals and motivated by financial gain, but will still result in degradation of government services, financial loss, and disruptions to our normal way and pace of life.

These attacks, although financially motivated, may have second order effects or unintended consequences that also adversely impact public health, the welfare and safety of our residents, the economy and public interests of the State.

Effectively managing cyber risk requires a whole of state approach across New Hampshire. Public and private sector organizations at the federal, state, and local levels, as well as businesses large and small, must collaborate on security in depth, practice good cyber hygiene, implement cybersecurity best practices, and perhaps most importantly, improve the ability of the Human Intrusion Prevention Systems across the state through training, exercises and creating a culture of cybersecurity.

Bottom Line Up Front (BLUF)

New Hampshire faces an evolving cyber threat landscape, characterized by cyberattacks that can be launched from anywhere in the world at any time of day or night.

- The most likely things users or administrators will see are phishing emails, attacks to compromise identities, business email compromise to enable good old-fashioned grifting, and ransomware attacks.
- Cybercrime organizations (Most Likely), Nation State Actors (Most Dangerous), Hacktivists, and others with diverse motivations and considerable technical capabilities pose significant threats.
- Enhanced by Generative AI, Phishing emails, links in text messages on mobile phones, and audio calls will be even more convincing than we have experienced to date which will require extensive training for our Human Intrusion Prevention Systems across Public Sector Organizations.

Introduction

This cyber threat assessment is based on discussions while walking around the State and interacting with IT professionals, risk managers, organizational leaders, managed service providers, and private sector Cybersecurity professionals in a variety of individual and group settings. It is also informed by close collaboration with the other 54 State and Territorial CISO's across the country. Unclassified threat intelligence shared by public and private sector partners, and other open sources of cyber threat information were used in the obvious places.

This 2025 threat assessment is meant to give you a working knowledge without having to read too much at once or read about these things every day. It also describes some significant incidents, profiles of threat actors, systemic risks and emerging technologies in a way that can be understood by those who are not Cybersecurity professionals to inform better cybersecurity outcomes across New Hampshire.

Threat Actors – the "Bad Guys"

"Threat actor" is a broad term used to describe any individual or group that conducts malicious cyber acts against a person or organization. They include cybercrime organizations, nation-state actors, and hacktivists. Cyberterrorists and Insiders are additional categories but are simply variations on the other themes. What's the difference?

MOTIVATION

- Nation-state actors are primarily motivated by strategic, geopolitical, or military goals (espionage, cyberwarfare, influence operations).
- Cybercriminals are driven by financial gain, typically through theft, fraud, and ransomware.
- Hacktivists are ideologically motivated, seeking to make political statements or advance social causes.

TACTICS

- Nation-state actors employ sophisticated, long-term campaigns, often with advanced tools and deep resources (APTs, supply chain attacks, espionage).
- Cybercriminals tend to focus on highly profitable, scalable operations like ransomware, credit card fraud, and phishing attacks.
- Hacktivists often employ disruptive, symbolic attacks like DDoS, website defacement, and data leaks.

IMPACT

- Nation-state actors can cause widespread, strategic damage to national security, economy, and political stability.
- Cybercriminals primarily affect businesses and individuals, often causing significant financial losses and operational disruption.
- Hacktivists create social unrest and harm reputations, although their attacks are generally less destructive on a large scale.

Cybercrime Organizations – the most likely threat to New Hampshire

Transnational cybercriminal organizations present a significant and growing threat to New Hampshire, with their activities spanning continents and impacting a wide range of sectors. These groups operate with increasing sophistication, using advanced tools, techniques, and infrastructure to carry out financially motivated crimes, ranging from ransomware attacks to data breaches and identity theft. New Hampshire State and Local government, businesses, and individuals are all targeted, and these cybercriminals often use tactics that are difficult to attribute directly, complicating efforts to combat their actions.

HIGH PROFILE TARGETS

Healthcare and Critical Infrastructure: Hospitals and healthcare organizations continue to be high-value targets, as ransomware groups see the potential for immense pressure on victims to pay to restore critical systems. In 2024, there have been several incidents involving major hospitals and medical facilities in New Hampshire being paralyzed by ransomware, potentially risking patient lives and data security.

New Hampshire Municipalities and K12 Schools: Smaller targets, like city governments and local utilities, continue to be targeted due to often weaker security measures and the public nature of their services – they are also insured by PRIMEX, so the criminals know there is money to pay the ransom!

Large Corporations: Major U.S. corporations, particularly in sectors like energy, finance, and retail, have been targeted for the high potential payouts. In some cases, the attackers have not only encrypted data but also stolen intellectual property or customer data.

Primary threats to New Hampshire in 2025 will include:

RANSOMWARE ATTACKS

- **Prevalence**: Ransomware remains one of the most common and dangerous tactics used by cybercriminal organizations. In 2024, these attacks were more targeted, highly professionalized, and often involve "double extortion" – where victims are not only locked out of their data but also threatened with the public release of sensitive information unless a ransom is paid.
- **Tactics**: Attackers often gain initial access through phishing emails, exploiting unpatched vulnerabilities in software (e.g., remote desktop protocol, email servers), or by compromising supply chains. Once inside a network, the attackers encrypt critical data and demand payment, usually in cryptocurrency. In double extortion, if the victim refuses to pay, attackers may release stolen data, often causing reputational damage.
- **Examples**:
    - REvil Ransomware Group: In 2023, REvil, a notorious Russian-based ransomware gang, continued to target high-profile organizations globally. One of their significant attacks was on a major U.S. healthcare provider, where they encrypted data and demanded a multi-million-dollar ransom, ultimately leading to the exposure of sensitive patient records.
    - LockBit Ransomware Group: In 2024, LockBit, one of the most active ransomware-as-a-service (RaaS) groups, continued its campaign of extorting organizations worldwide. In April 2024, LockBit targeted several U.S. municipalities, causing major disruptions in public services. The group employed double extortion tactics, threatening to release sensitive data on the dark web if the ransom was not paid.

BUSINESS EMAIL COMPROMISE (BEC)

- **BEC Evolution**: In 2024, Business Email Compromise (BEC) schemes have become even more sophisticated, leveraging AI-generated deepfake voice and video technology to impersonate executives and increase the likelihood of success. Criminal organizations often conduct “whaling” attacks, where senior leaders (like Mayors, Town Administrators, Superintendents, etc.) are impersonated to initiate large financial transfers or disclose sensitive information.
- **Tactics**: Attackers use phishing emails to trick employees into providing login credentials, which are then used to gain access to government email systems. Once inside, the attackers monitor communications and engage in fraudulent wire transfers, fake invoices, or other financial schemes.

Did you Know?

From NH Primex: In 2024, BEC resulted in an excess of $7M dollars of fraudulent ACH Transfers and other financial losses in NH Municipalities.

FBI IC3 Reports: In 2023, the FBI’s Internet Crime Complaint Center (IC3) reported that BEC scams caused losses exceeding $2.7 billion in the U.S., with cybercriminal groups often linked to organized crime syndicates in Eastern Europe, West Africa, and Asia.

DATA BREACHES AND IDENTITY THEFT

Overview: Transnational cybercriminal organizations often target databases (State and Local Governments have a LOT of these) containing large amounts of personally identifiable information (PII), financial, or other regulated data. Once compromised, this data is sold on the dark web or used for identity theft, fraud, or other illicit activities.

- **Examples**:
    - 2023 T-Mobile Breach: A large-scale data breach at T-Mobile in 2023 exposed the personal data of millions of U.S. customers, including names, addresses, and phone numbers. Cybercriminals exploited vulnerabilities in the telecom's database, and the stolen data was sold on dark web forums.
    - 2024 Retail and Healthcare Breaches: In 2024, several retail and healthcare organizations were targeted by transnational cybercriminals who stole and sold sensitive consumer data on dark web markets. These breaches are often part of larger, coordinated campaigns involving multiple cybercriminal groups operating across borders.

In 2024, cyberattacks from criminal organizations in the U.S. and New Hampshire were more sophisticated, pervasive, and damaging than ever. Ransomware, BEC schemes, cryptocurrency theft, supply chain compromises, and data breaches are major concerns. The criminal landscape is highly dynamic, with cybercriminals leveraging advanced technologies such as AI and deepfakes to increase the effectiveness of their attacks. New Hampshire continues to enhance its cybersecurity defenses, but the evolving nature of these threats requires constant vigilance and adaptation of our most important defense: our Human Intrusion Prevention Systems (also known as "users").

Nation-State Actors – the most dangerous threat to New Hampshire

Nation-state cyber threats represent one of the most serious challenges to U.S. national security, economic stability, and critical infrastructure in New Hampshire. These threats come from foreign governments or state-sponsored groups engaging in cyber activities that target entities in New Hampshire. Here's a summary of these threats and who they are:

1. Cyber Espionage (Not likely in New Hampshire Governments, but in New Hampshire Industry/Higher Education)
    - **Objective**: Gain access to sensitive information, intellectual property, and government secrets.
    - **Actors**: China, Russia, Iran, North Korea.
    - **Tactics**: Advanced Persistent Threats (APTs), spear-phishing, and exploiting vulnerabilities in software systems.
    - **Impact**: Theft of trade secrets, compromise of diplomatic, military, and government communications, and economic espionage.
2. Cyberattacks on Critical Infrastructure (Applies to New Hampshire!)
    - **Objective**: Disrupt or damage essential services like energy, water, transportation, and communications.
    - **Actors**: Russia, China, Iran, North Korea.
    - **Tactics**: Malware, ransomware, and Distributed Denial-of-Service (DDoS) attacks.
    - **Impact**: Potential disruption of the economy, national security operations, and public services. Attacks on the electrical grid, transportation systems, and financial markets have been highlighted as key areas of concern.

3. Election Interference (Applies to New Hampshire!)
    - **Objective**: Undermine democracy, influence U.S. elections, and create political instability.
    - **Actors**: Russia (2016/2020/2024), China (2020/2024), Iran (2020/2024).
    - **Tactics**: Disinformation campaigns, hacking political organizations (e.g., email leaks), social media manipulation, and fake news.
    - **Impact**: Erosion of public trust in democratic institutions and processes, polarization of U.S. society.
4. Information Warfare and Propaganda (Applies to New Hampshire)
    - **Objective**: Manipulate public perception, sow confusion, and divide societies.
    - **Actors**: Russia, China, Iran.
    - **Tactics**: Use of bots, fake accounts, deepfakes, and other means of amplifying false narratives or polarizing content across social media.
    - **Impact**: Heightened social tensions, reduced confidence in institutions, and creation of societal fractures.

Hacktivists – New Hampshire may see this, depending on the "cause."

OBJECTIVE

To promote a political, social, or ideological agenda by disrupting or defacing online services, often through cyberattacks and digital protests.

- **Actors**: These groups are typically motivated by political or ideological beliefs and may be loosely organized with fluid membership. Prominent hacktivist groups include Anonymous and LulzSec.
- **Tactics**:
    - Distributed Denial-of-Service (DDoS): Overloading a website or online service with traffic to make it unavailable.
    - Defacement: Changing the appearance of a website or replacing its content with messages aligned to their cause.
    - Data Leaks: Exposing sensitive information, often to embarrass or discredit organizations or governments.
    - Espionage and Disruption: Targeting corporations, governments, or individuals associated with specific issues or policies.
- **Impact**: Disruption of critical services, reputational damage to organizations, and leaking of sensitive data to the public. Hacktivist attacks can also provoke broader social unrest and undermine public trust in institutions.

EXAMPLES

- **Anonymous**: A decentralized collective of hacktivists that has targeted governments, corporations, and organizations it views as corrupt or unethical, including large-scale DDoS attacks and data breaches.
- **LulzSec**: Known for high-profile attacks against entities like Sony and PBS, often combining activism with mischief and defacement.
- **Involvement in Global Movements**: Hacktivist groups have been linked to larger global movements such as Occupy Wall Street, or anti-government protests, using cyberattacks as a form of digital resistance.

Cyber Terrorists – Don't Believe What You See in the Movies!

Cyberterrorists, like hacktivists, use cyberattacks to advance their ideological agendas. Some cyber terrorists are nation-state actors; others act on their own or on behalf of a non-government group. To date, traditional foreign and domestic terrorist groups that use violence to achieve their goals have not demonstrated the advanced capabilities necessary to carry out significant cyberattacks. However, some of the hacktivist groups, who claim to be carrying out cyberattacks in support of their ideologies and causes, may also be members of and proxies for terrorist groups.

Generative AI and Cyber Crime

This is so impactful it gets its own section for 2025!

In New Hampshire, Cybercriminals are increasingly using generative AI to enhance their attacks and streamline their operations. Some of the primary ways they are leveraging this technology include:

1. **Phishing and Social Engineering**: Generative AI tools, especially those focused on language generation (like GPT), are being used to craft highly convincing phishing emails, SMS, or messages. These messages can be tailored to a specific individual or organization, mimicking the tone, language, and style of legitimate communications. This makes the phishing attempts much harder to spot.
    - **Personalization**: Cybercriminals can input specific details about the target (e.g., from public social media profiles or breached databases) to generate more relevant and convincing messages.
    - **Scalability**: With generative AI, attackers can automate the creation of thousands of unique phishing messages, increasing the likelihood of success.
2. **Malware Code Generation**: Generative AI can assist in writing and refining malware code. By using AI to generate obfuscated or polymorphic code, cybercriminals can create more sophisticated malware that is harder to detect by traditional antivirus software.
    - **Custom Payloads**: AI can help design custom malware payloads tailored to exploit specific vulnerabilities in a target's system.
    - **Automated Development**: Instead of writing code manually, attackers can use AI to generate malware, making the process faster and more efficient.
3. **Deepfake Technology**: In 2024, we saw the first use of a Cyber Criminal using Generative AI to create an audio deepfake at the New Hampshire Hospital. Deepfake manipulated video, audio, or images that look and sound realistic but are entirely fabricated will be used for various malicious purposes, such as:
    - **Impersonation**: Deepfake videos or audio recordings of executives, employees, or even government officials can be used to conduct fraud, deceive individuals, or manipulate situations.
    - **Extortion and Reputation Damage**: Cybercriminals can use deepfake videos to create damaging content, threatening reputational harm or extortion.
4. **Automated Exploit Discovery**: Generative AI can assist in identifying vulnerabilities in software systems by automating the process of finding bugs or weaknesses that could be exploited. AI-powered tools can analyze code, spot potential flaws, and generate potential exploit strategies, making it easier for attackers to breach systems.

- **Zero-Day Exploits**: AI may assist in discovering zero-day vulnerabilities that have not yet been identified by security researchers, giving cybercriminals a distinct advantage in launching attacks.

5. **AI-Driven Botnets**: Generative AI can enhance the capabilities of botnets—networks of compromised devices controlled remotely by cybercriminals. AI can improve the efficiency of botnet operations by:
   - **Evading Detection**: Using generative techniques to dynamically change botnet behavior, making it harder for security systems to identify malicious activity.
   - **Coordinating Attacks**: AI can optimize the coordination of large-scale attacks, such as Distributed Denial-of-Service (DDoS) attacks, by making the botnet more adaptive and intelligent.
6. **Cracking Passwords and Captchas**: Generative AI models can be trained to perform advanced attacks like cracking passwords or bypassing CAPTCHAs (Yes, R2D2 can pass the "I'm not a robot" test.) While traditional brute-force attacks rely on simple trial-and-error, AI can be trained to recognize patterns in passwords or use generative models to guess credentials more accurately.
   - **Password Cracking**: Generative AI models can predict common passwords or phrases based on language patterns, increasing the chances of success in credential stuffing attacks.
   - **Captcha Bypass**: AI can be used to break CAPTCHA systems, enabling attackers to automate actions that would otherwise require human intervention.
7. **Automated Attack Campaigns**: Generative AI can facilitate the automation of large-scale cyberattack campaigns. With AI, cybercriminals can generate attack scripts or tactics that evolve over time, creating campaigns that adapt to changing conditions, security patches, or countermeasures deployed by defenders.
   - **Targeted Ransomware Attacks**: AI could be used to identify the most lucrative targets for ransomware campaigns, automating and refining the approach to maximize the attack's effectiveness.

As generative AI becomes more advanced, it will continue to present both opportunities and challenges for New Hampshire cybersecurity professionals.

Incident reporting is everyone's responsibility

If you work in State Government, it is very important to report a suspected cyber incident to the DoIT helpdesk via email or phone as follows:

- Email: helpdesk@doit.nh.gov
- Phone: (603) 271-7555 (Outside of 7:30 AM to 4:30PM, dial the number and select "Option 2")

If you are a New Hampshire City, Town, County, Police Department, Fire Department or K12 and a member of the New Hampshire Public Risk Management Exchange (PRIMEX) who suspects a cyber incident has occurred, contact PRIMEX immediately to open a claim and get the dedicated cyber first responders engaged.

If you are a public sector entity and not a member of PRIMEX, and you suspect an incident has occurred, contact the New Hampshire Department of Safety's Information and Analysis Center at Report a Cyber Incident or to nhiac.cyber@dos.nh.gov.

If you are a New Hampshire private citizen or agent for a business, contact your local law enforcement non-emergency number to report the crime.

To sum it all up…

Based on an analysis of cyberattack trends and emerging threats; the motivations, capabilities, and targeting by the various threat actor types; geopolitical issues; and systemic cyber risks, the State of New Hampshire will continue to see cyber-attacks against towns, cities, counties, critical infrastructure, health care organizations, K12 schools, higher education, and even individuals. Most of these attacks will be from Cybercriminals and motivated by financial gain, but will still result in degradation of government services, financial loss, and disruptions to our normal way and pace of life. These attacks, although financially motivated, may have second order effects or unintended consequences that also adversely impact public health, the welfare and safety of our residents, the economy and public interests of the State.

It is unrealistic to expect any one organization to defend against nation-state actors, criminal syndicates, hacktivists, cyber terrorists, and other threat actor groups who can launch attacks from anywhere in the world at any time of day or night. Effectively managing cyber risk requires a proactive and collaborative approach across New Hampshire. Public and private sector organizations at the federal, state, and local levels, as well as businesses large and small must collaborate on security in depth, practice good cyber hygiene, implement cybersecurity best practices, and perhaps most importantly, improve the ability of the Human Intrusion Prevention Systems across the state through training, exercises and creating a cybersecurity culture. The Cyber Criminals don't get to win!

DID YOU KNOW?

In 2024, there were 63 cyber incidents in New Hampshire reported to the NH Public Risk Management Exchange (PRIMEX) that resulted in an Incident Response Claim. 61 of these incidents were initiated with a Phishing email that resulted in a compromise of legitimate user credentials (usernames and passphrases). Only 2 were the result of unpatched vulnerabilities in systems that were exploited for access.

According to the 2023 Verizon Data Breach Report, up to 80% of all breaches were the result of stolen or otherwise compromised login credentials. Various reports estimate there are around 7 billion sets of compromised credentials available or for sale on the Internet.

Identity-based attacks are expected to remain the primary method of attack against New Hampshire public and private sector organizations, as well as the State's residents and businesses in 2025.