NHMA
NEW HAMPSHIRE MUNICIPAL ASSOCIATION

Cybersecurity for Elected Officials



Primex
NH Public Risk Management Exchange

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

1

Presenters



Cori Casey

Primex
Risk Management Consultant
Primex[3]



Richard Rossi

Cybersecurity Advisor – NH

CISA, U.S. Department of Homeland Security

2

What is the purpose of this training?

Understanding the challenges of cybersecurity in NH

↓

Familiarization with available resources

↓

Discussing the role of elected officials in securing communities

3

Why is cybersecurity training important for NH Elected Officials?

1 Public Trust

Your employees, citizens, and visitors entrust you with critical and private information. They expect that it is being handled securely.

2 End User to IT Ratio

Private sector IT to staff ratio is between 1:18 - 1:25. Counties, cities and towns are often much worse.

3 You are a target

Local government entities in New Hampshire are frequently targeted. Think: cyber coverage. Employee credentials are involved in many of the cyber attacks in NH.

As a leadership team, you help to set the tone for the importance of cybersecurity within your organization.

4



TODAY'S CYBER THREAT ENVIRONMENT

5

Today's Cyber Threat Actors…

Nation-States

- China
- Russia
- Iran
- North Korea
- Others…



Criminal Hackers

- Financially Motivated Groups
- Ideologically Motivated Hacktivists

6

Cyber Threat Environment Trends



Data as a Commodity

Interconnected Systems Increase Threat Environment

Hacking as a Service (HaaS)

- Ransomware, DDOS
- Initial Access Brokers

7

Cyber Threat Environment Trends



Ubiquity of Malicious Tools

- Ease of Use
- Destructive Capabilities

Targets of Opportunity

Supply Chain Campaigns and Zero Day Markets

- External Dependency Management

8

Today's Cyber Threat Actors Are Sophisticated…



9

But They Don't Always Need To Be

DARKReading

91% Of Cyberattacks Start With A Phishing Email

Phishing remains the number one attack vector, according to a new study that analyzes why users fall for these lures.

The majority of cyberattacks begin with a user clicking on a phishing email. Ever wondor why users continue to fall for phishing emails?

According to a new report from PhishMe that found that 91% of cyberattacks start with a phish, the top reasons people are duped by phishing emails are curiosity (13.7%), fear (13.4%), and urgency (13.2%), followed by reward/recognition, social, entertainment, and opportunity.

"Fear and urgency are a normal part of every day work for many users," says Aaron Higbee, co-founder and CTO of PhishMe. "Most employees are conscientious about losing their jobs due to poor performance and are often driven by deadlines, which leads them to be more susceptible to phishing."

Higbee says PhishMe based the study on more than 40 million simulation emails by about 1,000 of its customers around the world. The study took place over an 18-month span from January 2015 through July 2016.

HOT TOPICS | EDITORS' CHOICE

Disappearing Act: Dark Reading Caption Contest Winners 2
Marilyn Cohodas, Community Editor, Dark Reading, 3/12/2018

Microsoft Report Details Different Forms of Cryptominers 2
Kelly Sheridan, Staff Editor, Dark Reading, 3/13/2018

Who Does What in Cybersecurity at the C-Level 2
Steve Zurier, Freelance Writer, 3/16/2018

NEWS SUBSCRIBE TO NEWSLETTERS

10

But They Don't Always Need To Be

CSO FROM IDG

Home > Information Security

ANALYSIS

Zero-days aren't the problem -- patches are

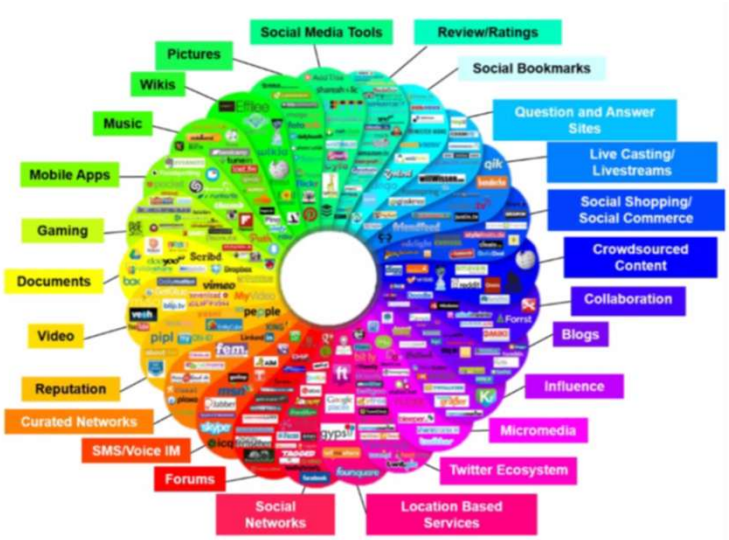
Everyone fears the zero-day exploit. But old, unpatched vulnerabilities still provide the means for malicious hackers to carry out the vast majority of hacks

Most hackers follow the path created by a very few smart ones -- and zero days make up a very small percentage of attacks. It turns out that patching vulnerable software, if implemented consistently, would stop most hackers cold and significantly reduce risk.

11

But They Don't Always Need To Be

- Network Scans
- Information about the organization, employees, and executives found online
- Discarded information



12

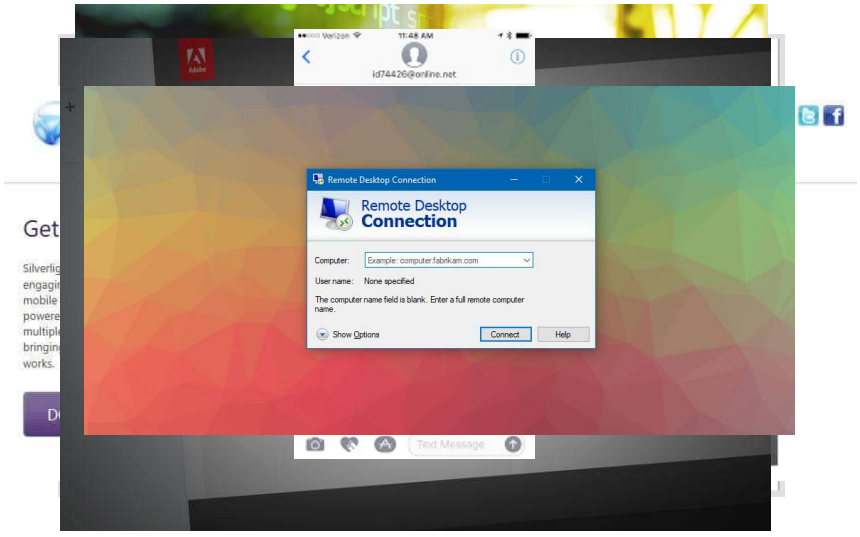


13

Common Methods of Infection

The following can all be vectors of infection for ransomware attacks:

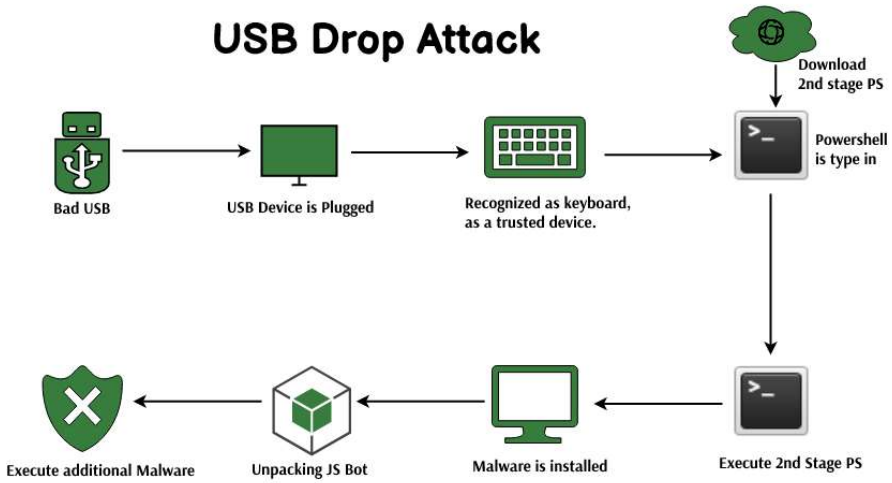
- Phishing
- Compromised Websites
- Malvertising
- Exploit Kits
- Downloads
- Messaging Applications
- Brute Force via RDP



14

Removable Media Threats





15

15



16

Governance

Conceptually, IT Governance includes:

- The **framework and processes** that ensure IT **supports and enables organizational objectives,**
- That IT risks are **managed,**
- That IT resources are **used responsibly**, and
- That accountability for IT decisions is **defined and enforced**.



17

Source: CISSP CBK

17

Governance

NIST CSF 2.0 – Governance Function

NIST defines *Governance* in CSF 2.0 as the function through which:

> The organization's **cybersecurity risk management strategy, expectations, and policy** are established, communicated, and monitored.

The CSF Governance categories include:

- **Organizational Context (GV.OC)** – ensuring stakeholders, mission needs, and legal obligations are understood.
- **Risk Management Strategy (GV.RM)** – establishing risk tolerance, priorities, and assumptions.
- **Roles, Responsibilities, and Authorities (GV.RR)** – ensuring accountability and clarity in cybersecurity responsibilities.
- **Policy (GV.PO)** – defining and enforcing organizational cybersecurity policies.
- **Oversight (GV.OV)** – using performance and risk outcomes to drive improvement.
- **Supply Chain Risk Management (GV.SC)** – establishing and monitoring cyber supply chain processes.

18

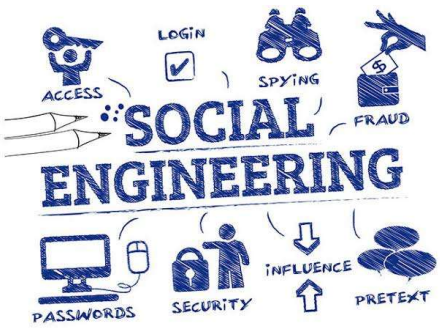
Source: NIST CSF 2.0

18



19

Social Engineering



What is a social engineering attack?

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

20

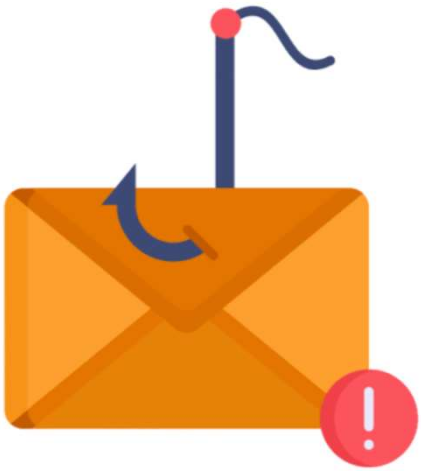
20

Phishing

What is a phishing attack?

Phishing is a form of **social engineering**. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year.



21

21

What Can This Look Like?

Suspicious sender's address. The sender's address may imitate a legitimate business. Cybercriminals often use an email address that closely resembles one from a reputable company by altering or omitting a few characters.

Generic greetings and signature. Both a generic greeting—such as "Dear Valued Customer" or "Sir/Ma'am"—and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.

Spoofed hyperlinks and websites. If you hover your cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.

Spelling and layout. Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.

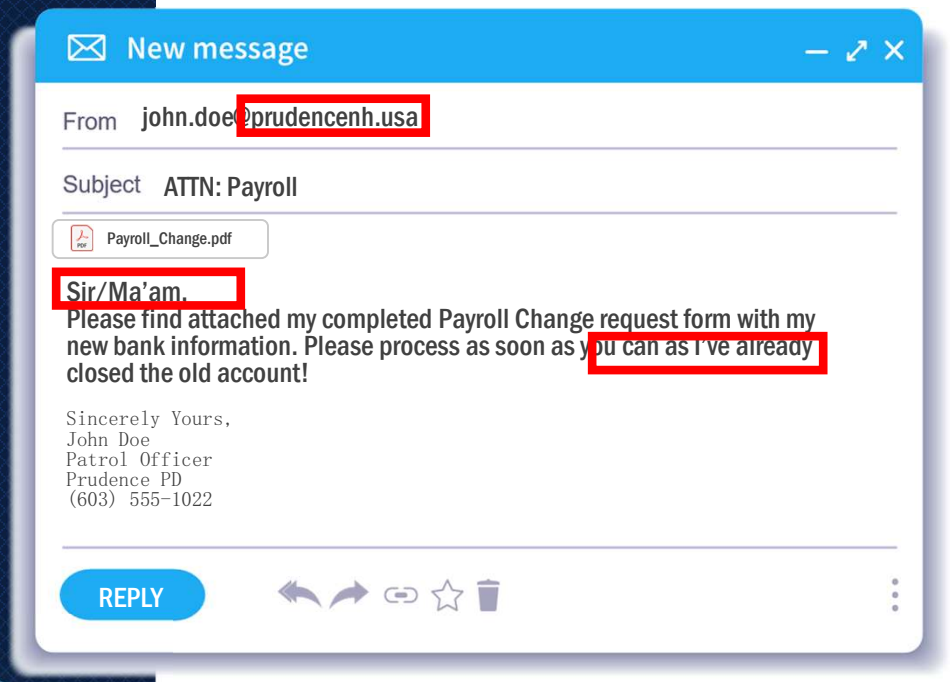
Suspicious attachments. An unsolicited email requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.



22

22

Would you believe this email?



23

23

Vishing



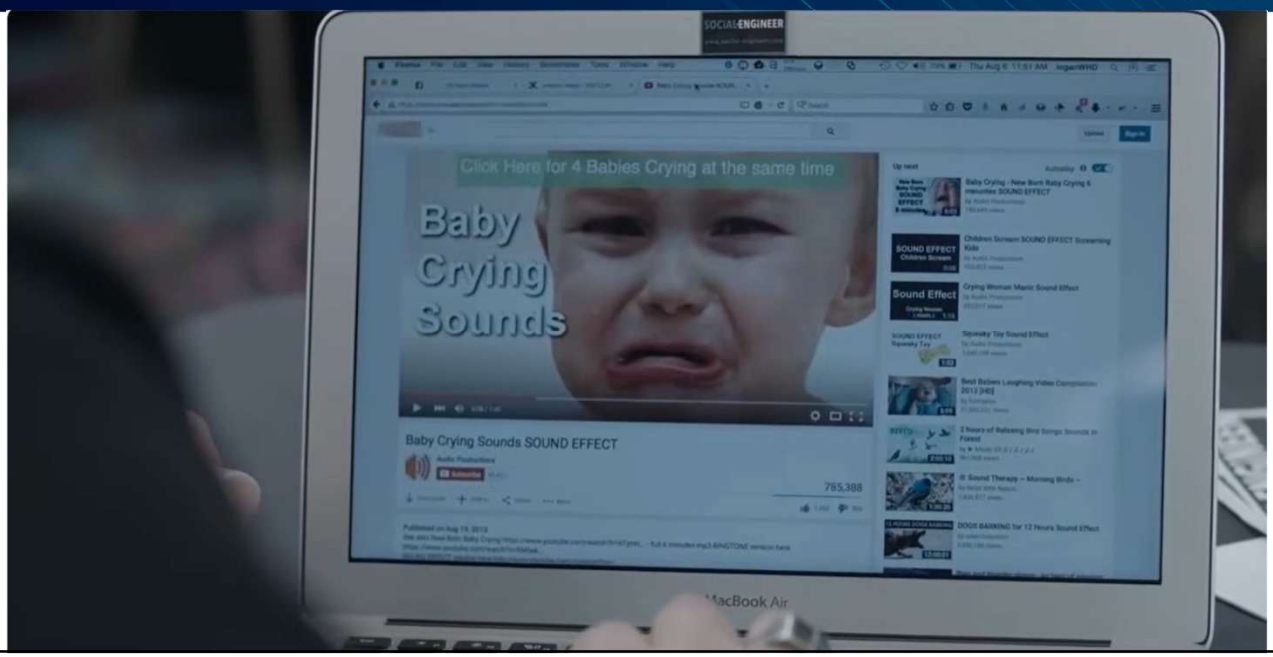
What is a vishing attack?

Vishing is the **social engineering** approach that leverages voice communication. This technique can be combined with other forms of social engineering that entice a victim to call a certain number and divulge sensitive information. Advanced vishing attacks can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services. VoIP easily allows caller identity (ID) to be spoofed, which can take advantage of the public's misplaced trust in the security of phone services, especially landline services. Landline communication cannot be intercepted without physical access to the line; however, this trait is not beneficial when communicating directly with a malicious actor.

24

24

What Can This Look Like?



25

Smishing

What is a smishing attack?

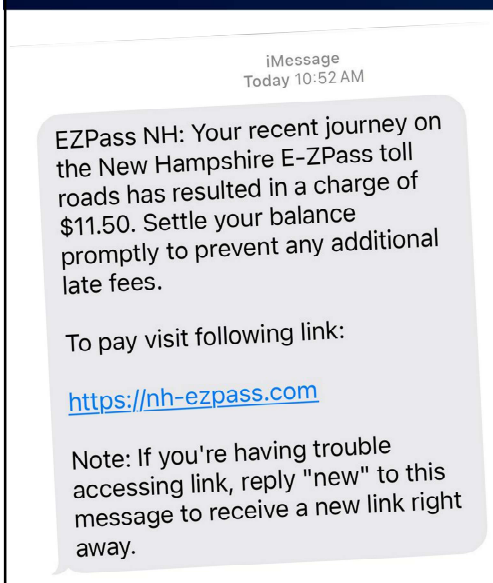
Smishing is a form of **social engineering** that exploits SMS, or text, messages. Text messages can contain links to such things as webpages, email addresses or phone numbers that when clicked may automatically open a browser window or email message or dial a number. This integration of email, voice, text message, and web browser functionality increases the likelihood that users will fall victim to engineered malicious activity.

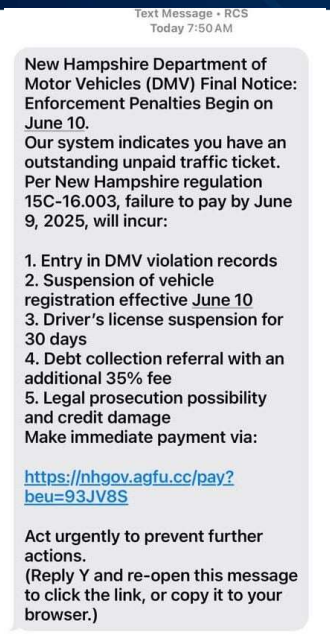


26

26

What Can This Look Like?







27

27

How do you avoid being a victim?

- ✓ **Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company through independent means.**
- ✓ **Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.**
- ✓ **Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.**
- ✓ **Don't send sensitive information over the internet before checking a website's security. (See Protecting Your Privacy for more information.)**
  - ✓**Pay attention to the Uniform Resource Locator (URL) of a website. Look for URLs that begin with "https"—an indication that sites are secure—rather than "http." Look for a closed padlock icon—a sign your information will be encrypted.**

28

28

How do you avoid being a victim?

- ✓ If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group.
- ✓ Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.
- ✓ Take advantage of any anti-phishing features offered by your email client and web browser
- ✓Enforce multifactor authentication (MFA).

29

29



30

Beyond the Headlines: What is Ransomware?

Ransomware 101

- Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.
- Malicious actors then demand ransom in exchange for decryption.

31

Beyond the Headlines: What is Ransomware?



32

Infects… Encrypts… Extorts

- Ransomware incidents can severely impact businesses.
- Malicious actors have become more sophisticated.
- Ransom demands for millions of dollars are becoming commonplace.
- Ransomware incidents have become more destructive and impactful in nature and scope.



33

Trend: Double Extortion

- **Weaponized**: One part Ransomware, One Part Data Breach
- **Old Paradigm**: Victim's data encrypted,
  actor locks victim out of their own files.
  If victim refuses to pay the ransom, the actor destroys their files.
- **New Paradigm**: Attacker steals data before encryption.



34


ESSENTIAL CYBERSECURITY PRACTICES
CISA
Primex
NH Public Risk Management Exchange

35


ESSENTIAL STEP TO SAFEGUARD YOUR DATA
USE STRONG PASSWORDS

36


ESSENTIAL STEP TO SAFEGUARD YOUR DATA
UPDATE SOFTWARE

37


LEVEL UP YOUR DEFENSES WITH CYBERSECURITY BEST PRACTICE
BACK UP DATA

38


ESSENTIAL STEP TO SAFEGUARD YOUR DATA
RECOGNIZE AND REPORT PHISHING

39


LEVEL UP YOUR DEFENSES WITH CYBERSECURITY BEST
ENCRYPT DATA

40


LEVEL UP YOUR DEFENSES WITH CYBERSECURITY BEST PRACTICE
LOGGING AND MONITORING

41


ESSENTIAL STEP TO SAFEGUARD YOUR DATA
ENABLE MFA

42

What is the potential impact of a cyber attack?

43

RR1

By the numbers (business days):

8
days of operational disruption from a typical cyber event.

19
days required to fully remediate and restore affected systems.

1 in 3
organizations experience data loss that can lead to secondary attacks and legal consequences.

1 in 8
New Hampshire organizations will face a cyber incident this year.

44

Slide 44

RR1 I can’t remember where we landed on keeping this one or not?
Rossi, Rick, 2026-10-01T16:23:24.258

Let's take a moment and think about our own habits.

45

Do you use repeat passwords or use the same passwords at **work** and **home**?

1	2	3
I would never do that!	Sometimes, but I try not to.	All the time. They are hard to remember!

46

Do you use a **password manager**?

1	2	3
Yes, all my passwords are securely stored in a password manager.	No, I've thought about it. But I don't know what to use or where to start.	No. What's that and how do I get one?

47

How confident are you in recognizing signs that an email account may have been **compromised**?

1	2	3
I regularly check and know what to look for.	I try to check, but I don't do it as often as I should.	I'm not sure what signs to look for and would like to learn more.

48

Artificial Intelligence (AI)

Managing risk

49

It's already here… whether you asked for it or not.

Trust but verify	Know about Right to Know (91:A)	Professional vs. Private tools
• All results must be checked. • Cite all use, when appropriate or required by policy. • Remember… **DON'T HALLUCINATE!**	• What search inputs are required to release to the public? • Consult with your legal counsel and leadership prior to use.	• Only authorized AI tools should be utilized. • Do **all** professional AI work from work devices, **not** personal ones.

50

Concerns?



The law is playing catch-up with the technology.



Is governance being thought of? Create your guardrails.

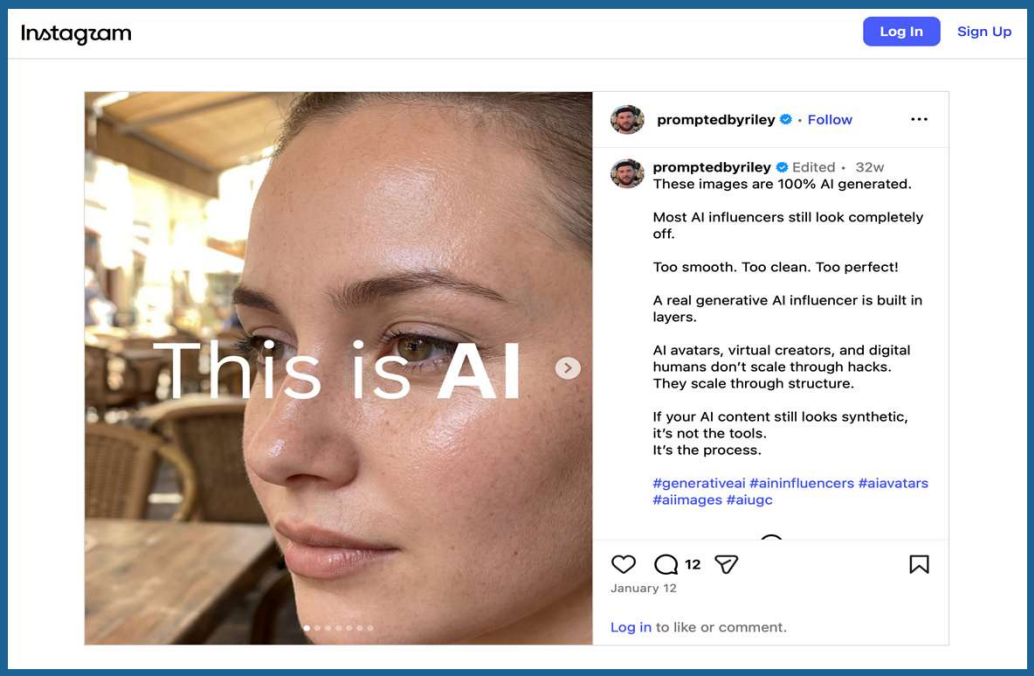


When will **you** learn more about, and if necessary, regulate organizational AI use?



You may not have asked for it, but it's already here.

51



52



53

IBM X-Force Threat Intelligence Index 2026

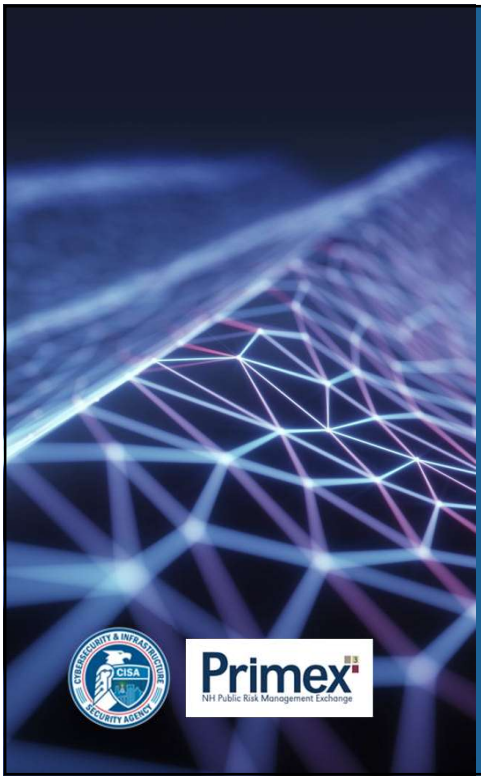
Prepare for AI-accelerated attacks

- **44%** — Year-over-year increase in the exploitation of public facing software or system applications
- **56%** — Share of disclosed vulnerabilities that did not require authentication to successfully exploit
- **300,000** — Number of AI chatbot credentials observed for sale on the dark web
- **49%** — Increase in active ransomware groups compared to the prior year

54

Governance is key

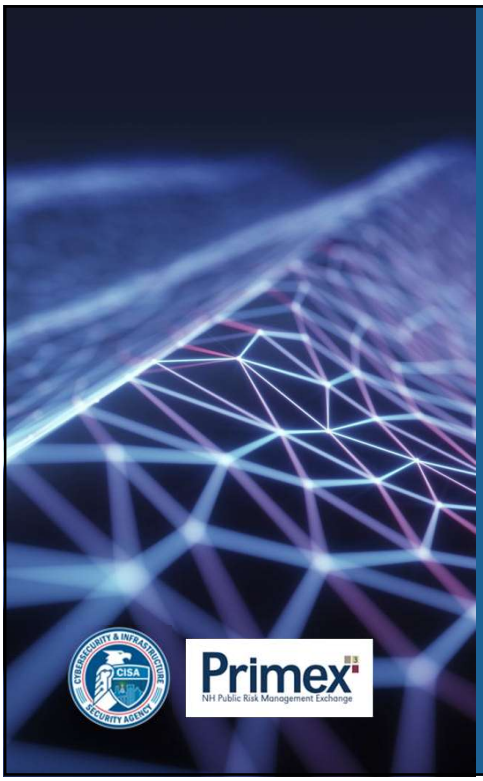
55



Critical Policies

- **Acceptable Use Policy –**
  what is your team allowed to use municipal technology for? Anything they're not allowed to do? Include security awareness and training or carve out separately.
- **Incident Response Plan –**
  does your team know what to do if a cyber incident occurs?
- **Continuity of Operations Plan –**
  how would the team continue to deliver services and support without tech?
- **Password Policy –**
  are passwords and password management expectations clearly stated in policy?

56



Critical Policies

- **Bring Your Own Device (BYOD) Policy –**
  do you have employees, elected officials, volunteers, or third-party vendors who join their own devices onto the network? How would you respond if a personal device were infected or if an individual brought an infection home?
- **Data Handling Policy –**
  how is your team handling PII?
- **Vendor and Third-Party Risk Management Policy –**
  who is reviewing your contracts? Are you conducting security assessments? Do you have vendor security and data breach notification requirements?

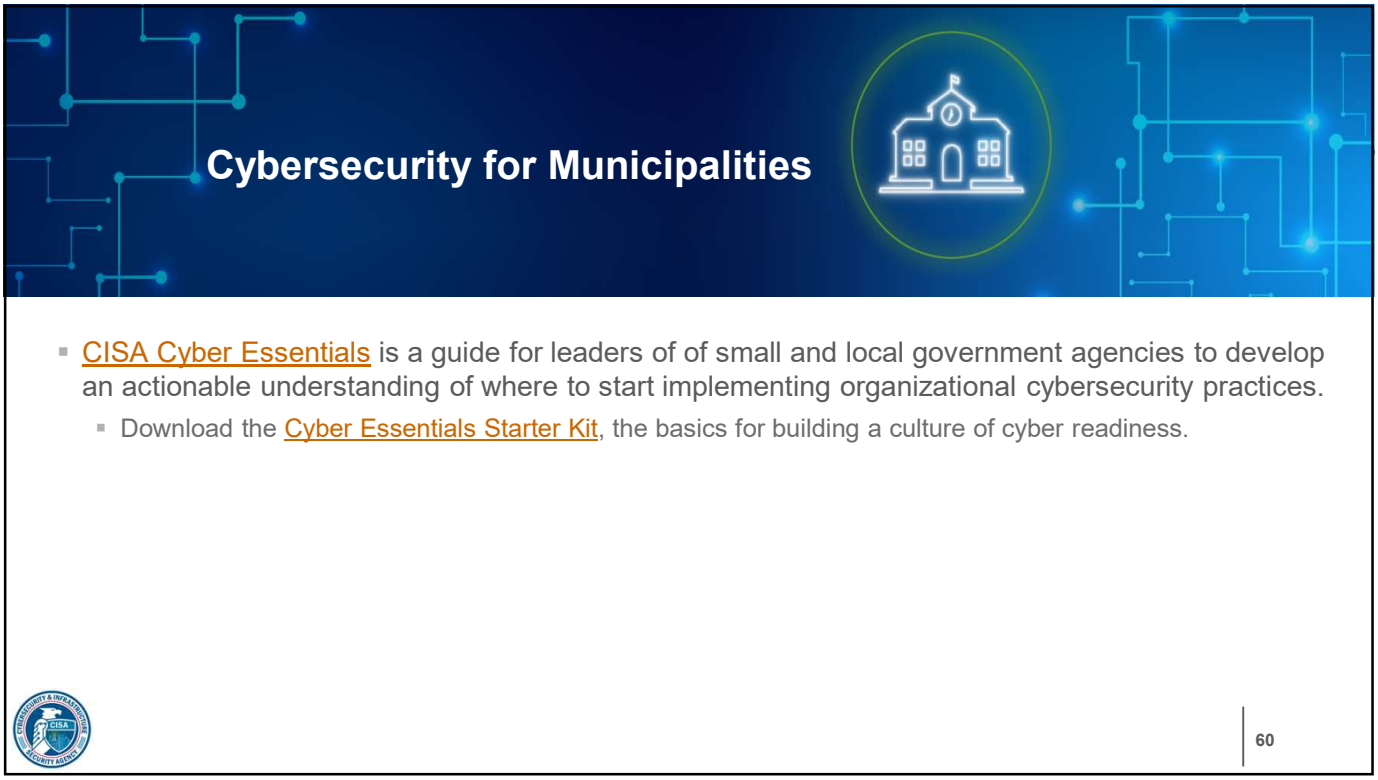
57

FREE CISA RESOURCES

58


Leveraging Resources
Looking to harden your defenses?
Want to know how an adversary sees your organization?
CISA assessments are voluntary, non-regulatory, and free.
Recommended Pathway
Cybersecurity Baseline Assessment
Vulnerability Scanning
Technical Services
Free Cybersecurity Tools
Active Shooter Program
Cyber & Physical Tabletop Exercises
M365 Security Baselines
Logging Made Easy
3-4hrs over 1 Day
Remotely Conducted
Free Services/Resources
Tailored resources across sectors and security posture
59

59


Cybersecurity for Municipalities
CISA Cyber Essentials is a guide for leaders of of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.
Download the Cyber Essentials Starter Kit, the basics for building a culture of cyber readiness.
60

60

Any Questions?



Primex
NH Public Risk Management Exchange

Trust. Excellence. Service.

61