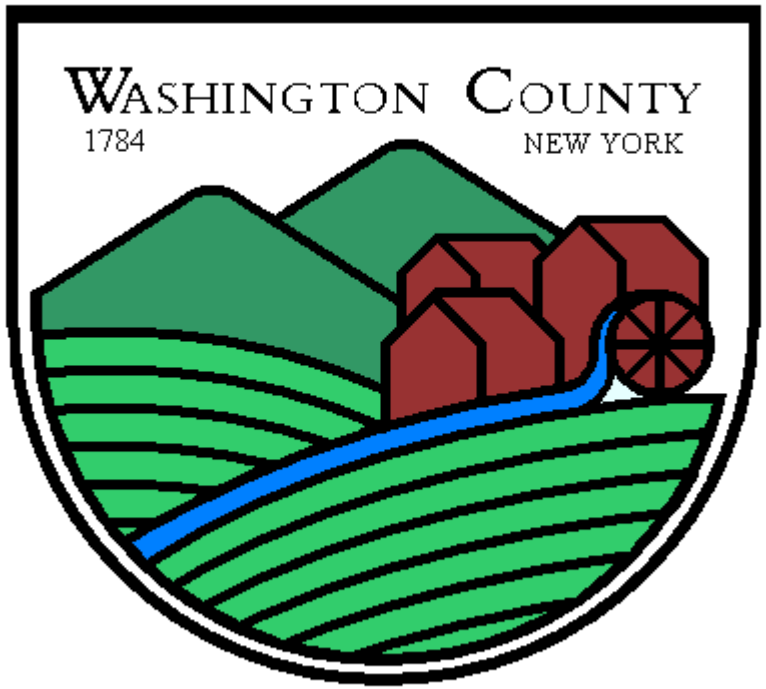
Be Cyber Aware: An Intro to Cybersecurity for Municipalities



Agenda

- What is Cybersecurity
- Learning of and recognizing the threat
- Steps you can take to reduce your risk
- Questions

What is Cybersecurity?

- What is cybersecurity?
- Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. It seems that everything relies on computers and the internet now—communication (e.g., email, smartphones, tablets), entertainment (e.g., interactive video games, social media, apps), transportation (e.g., navigation systems), shopping (e.g., online shopping, credit cards), medicine (e.g., medical equipment, medical records), and the list goes on.
- Cybersecurity Infrastructure Security Agency

Why Cybersecurity and What Does It Mean To Me?

- Everyone has a role in Cybersecurity
- As municipalities, we create, store and process data
- Citizens rely upon the services that local government is providing and with that we are charged with protecting this data
- You are a conduit to the other agencies such as the County and NYS State
- One part at a time, don’t be intimidated, it’s ongoing and ever changing

We are all targets

- 16 Critical Infrastructure Sectors
  - Government Facilities
    - Villages
    - Towns
    - Cities
    - County
    - State
    - Elections
    - Education –School Districts/Colleges
  - Emergency Services/Public Safety
  - Healthcare and Public Health
  - Water and Wastewater
  - Information Technology
  - Communication

What Can Happen ?

- Data loss
  - Personally identifiable
  - Financial
- Disruption of services
  - Affecting the welfare of our citizens
- Destruction of infrastructure or data
  - Costly
- Disinformation
  - False information, turmoil

Types of Threats to Municipalities

- Phishing/SpearPhishing
  - Phishing attacks make up 80% of reported security incidents according to CISCO's 2021 Cybersecurity Threat Trends report, about 90% of data breaches occur due to phishing. Spear phishing is the most common type of phishing attack, comprising 65% of all phishing attacks.
  - More than 90% of cyberattacks infiltrate organizations via email.
  - According to the FBI, there has been an 400% increase year over year in phishing attacks.

Types of Threats to Municipalities

- SMS phishing (smishing)
- Business Email Compromise (BEC)
- Malware
- Websites and Links
- Ransomware
  - Nearly 500 million attacks in 2021
  - 127% increase in the US
- Wireless Connections
- External Dependencies
- Social Engineering (on the rise)
- Misinformation/Disinformation
- Vulnerability Exploits

Statistics noted in the NYSAC Cybersecurity Primer for Local Government Leaders

Local Government Cyber Events Reported to NYS Intelligence Center

2020-2021*

- 46 County Governments
- 22 Municipal Governments
- 11 School Districts
- 6 Emergency Services Organizations

*These are reported events, the actual number of events is higher than reported.

General Breaches and Ransomware Facts

- About 1 in 6,000 emails contain suspicious URLs, including ransomware. (Fortinet, 2020)
- 71 percent of those impacted by ransomware have been infected. Half of the successful ransomware attacks infect at least 20 computers in the organization. (Acronis, 2020)
- The average ransom fee requested has increased from $5,000 in 2018 to around $200,000 in 2020. (National Security Institute, 2021)
- The average downtime an organization experiences after a ransomware attack is 21 days. (Coveware, 2021)
- 42 percent of companies with cyber insurance policies in place indicated that insurance only covered a small part of damages caused by the ransomware attack. (Cybereason, 2021)

Washington County

Recognizing the Threat

Phishing

- Email disguised as a contact, asking you to look at a proposal, invoice, document
- Malicious actor attempts to trick you into giving out sensitive information or taking an action such as clicking on a link
- Often a sense of urgency
- Be suspicious of all emails that contain an attachment or link especially those that are not expected

Washington County

Recognizing the Threat

Phishing

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.

Washington County

Recognizing the Threat

SpearPhishing

- Focused attack
- Malicious actor uses social media and other open-source information
- Email is more personal, often targeting top management such as Chairman, Department Head, Supervisor
- May take advantage of current events

Washington County

Recognizing the Threat

SMS phishing

- Smishing - text based phishing on mobile devices
- Attacker sends message trying to trick recipient on clicking on link
- The message may include your name and location garnered from online tools
- Link may lead to a credential phishing site or malware designed to compromise the phone itself and lead to exfiltration of sensitive data

Recognizing the Threat

Business Email Compromise

- Direct Deposit Variant
- W-2 and Personally Identifiable Information (PII)
- Financial Theft
- Purchase Order Fraud

Recognizing the Threat

Malware

- Malicious software and malicious apps can log keystrokes, take over the computer, and lead to exfiltration of data
- Can source from various means including attachments in emails and links to malicious sites
- Be cautious when asked to enable content

Recognizing the Threat

Websites and Links

- Know your links
- Malicious actors will use slight variations to trick you
- Variations may include misspellings, extra characters or hyphens where a period should be
- When in doubt don’t click on it, but use trusted resources to identify legitimate domain

Recognizing the Threat

Ransomware

- Malware designed to deny organization access to data on their computer
- Data is encrypted and locked
- Malicious actor/group holds data for ransom
- Threatens you to pay or your data will be released

Recognizing the Threat

Wireless Connections

- Be cautious of WiFi as the connections can be non-secure
- Malicious actors can eavesdrop, monitor traffic and redirect you do malicious sites
- Malicious actors can also create a malicious WiFi network that has a name similar to the public/hotel network tricking you to connect to their network instead

Recognizing the Threat

External Dependencies

- Know the risk of those that you do business with
- How does the third party protect the store and/or process of the organization’s data
- If a third party creates software for you, do they code securely

Steps You Can Take To Reduce Your Risk

- First step is being aware
- Encourage a security awareness culture
- Good Cyber Hygiene
  - **Multi-Factor Authentication (MFA)**
  - Secure your devices
  - Least privilege access
  - Limit administrative accounts
  - Change default passwords
  - Train
  - Regularly update hardware devices
  - Regularly update software programs
  - Have a reliable backup, backup regularly
  - End point security to detect and address malware

Steps You Can Take To Reduce Your Risk

- Limit what you store in email
- Use Strong, Unique Passwords

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hours	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69kyears	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Steps You Can Take To Reduce Your Risk

- Continue to review emails, especially those unsolicited, in their entirety, examining the from address, subject and body, looking for spelling errors, sense of urgency, link and attachment information
- **Never** provide your credential information, especially from an attachment or a link within email
- Be cautious about the information you share publicly

Steps You Can Take To Reduce Your Risk

- Turn off WiFi when not using
- Never connect to public WiFi, unless connected via VPN, virtual private network
- Use trusted sources
- Know the apps you download and understand the privacy policy so that you are not unknowingly sharing location and personal information
- Organizational firewall, spam filtering, vulnerability scanning and malicious domain blocking
- Know where to report unusual activity

Summary

- Have a healthy paranoia
- Remember the first slide…One part at a time, don’t be intimidated, it’s ongoing and ever changing
- You have a key role and are our best defense
- Thank you for taking this step to reduce risk

Questions and Contact Information

- Questions?
- Contact information: kpratt@washingtoncountyny.gov
- (518) 746-2106 Washington County Attorney's Office
- Survey

Resources

- Cybersecurity Primer for Local Government Leaders https://www.nysac.org/files/Cybersecurity%20Primer%20for%20Local%20Government%20Leaders.pdf
- Cybersecurity and Infrastructure Security Agency (CISA) https://www.cisa.gov/cybersecurity
- New York State Division of Homeland Security and Emergency Services (DHSES) https://www.dhses.ny.gov/cybersecurity-services
- New York State Office of Information Technology Services Cybersecurity https://its.ny.gov/ciso
- Multi State Information Sharing and Analysis Center (MS-ISAC) /Center for Internet Security(CIS) https://www.cisecurity.org/ms-isac
- Global Cyber Alliance (GCA) https://gcatoolkit.org/smallbusiness/
- Federal Bureau of Investigation (FBI) https://www.fbi.gov/investigate/cyber
- National Institute of Standards and Technology (NIST) https://www.nist.gov/itl/smallbusinesscyber
- Stop. Think. Connect. https://www.stopthinkconnect.org/
- Stay Safe Online https://staysafeonline.org