nj municipalities

Official Publication of the New Jersey State League of Municipalities

October 2020

Cyber Security & the Pandemic

PREVIEW

105th Annual Conference– presented virtually

COVID-19 Tech Lessons

Focus:

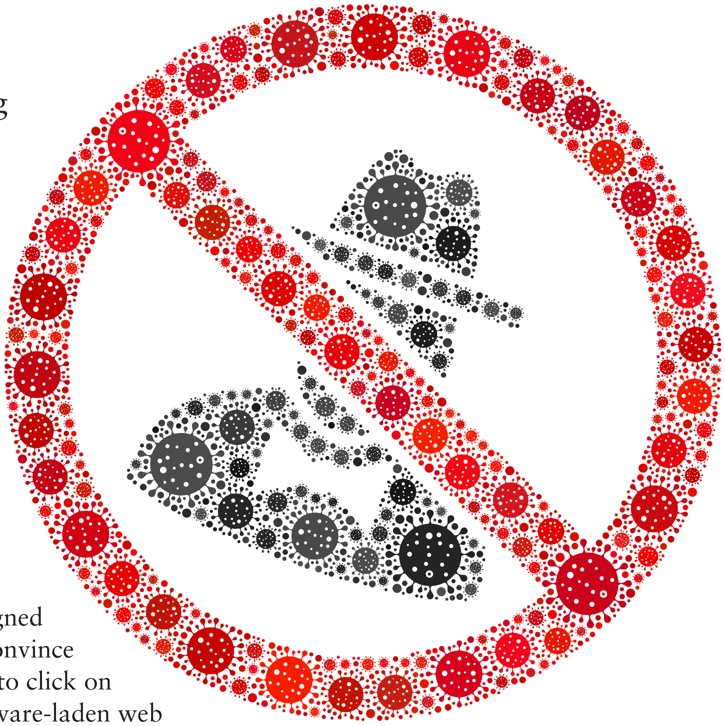
Cyber Security & Remote Work

Cyber Security Challenges and COVID-19

Network safety in the office and working from home

EDWARD COONEY, MBA, *Vice President and Account Executive, Conner Strong & Buckelew, and Underwriting Manager for the Municipal Excess Liability Joint Insurance Fund and Cyber Task Force;* *and* MICHAEL GERAGHTY, *Chief Information Security Officer for the State of New Jersey, and Director of the N.J. Cybersecurity and Communications Integration Cell (NJCCIC)*

A police sergeant was working on a Saturday during the height of the pandemic when he clicked on an email that was labeled as a COVID-19 resource. Suddenly, a menacing message blanketed the computer screen. The entire computer network was taken hostage and the attacker demanded a $500,000 ransom to regain the network. The attacker also threatened to release sensitive police documentation to the web such as arrest records, ongoing investigations, camera footage, etc.



The damage could have been exponential, not only resulting in diminished productivity and the cost of the ransom, but for police departments this could also mean losing access to criminal databases and result in endangering officers in the field. It took two months to resolve the issue and cost the town $1 million dollars.

This is not a hypothetical scenario. This incident happened to a local police department in New Jersey and is just one of countless other cyber-attacks plaguing police departments, municipalities, and public entities across the country.

A new level of security

The COVID-19 pandemic created a whole new level of cyber security anxiety for local governments due to massive increases in viruses, phishing campaigns, and fake websites related to COVID-19. The potential risk for network breaches also intensified due to potential lapses in security from employees working remotely.

Phishing emails are easy for cyber criminals to deploy and have an excellent success rate because they look just like regular emails. They contain relevant messaging and are designed to convince you to click on malware-laden web links or open a malware-ridden file that can activate ransomware or a virus that can infiltrate your network.

With so many questions about COVID-19 many people fell into this cyber trap opening these emails or unknowingly visiting malware-backed fake websites to find answers. To put this in perspective, Google reported Coronavirus searches outpaced most other major search topics by four-fold in March 2020.

Ransomware delivered via phishing emails and unprotected ports is the most frequent cyber incident for public entities, and most other industries.

Recognizing scams

Learning how to recognize phishing scams needs to be a top priority for every single public employee. Here are some simple rules from the MEL Cyber Task Force to help avoid these cyber potholes.

- Never open unsolicited emails.
- Avoid clicking on links and opening attachments from unsolicited emails.
- Examine the From, Date, CC, and Subject lines before opening to look for odd spelling, unknown names, badly composed messaging.
- Be aware that attacks are often disguised as COVID-19 information, fundraising campaigns, personal protective equipment supplies, COVID-19 related Business Grants, tracking apps, unemployment assistance, etc.
- Only use trusted sources (websites you know) and never click on links.

Securing remote work

Another significant cyber security issue for municipalities has been trying to ensure network safety in the wake of the major shift to employees working remotely due to the pandemic. Things happened so quickly that many networks were left vulnerable. Unfortunately, some have already been hacked but may never know it, or may find out weeks, months, or even years later.

If your municipality doesn't already have remote work procedures and policies in place as part of your Cyber Risk Management plan, now is the time to create them. Existing plans should be reviewed and revised to better protect your networks going forward.

The New Jersey Cyber Security and Communications Integration Cell (NJCCIC) recommends implementing these protections:

Two-Factor Identification: This ensures that the person logging into your network is who they say they are and can help protect against weak or compromised passwords. In addition to entering the username/password a person would receive a text or email to confirm their identity. This is easy to set-up and is built into software such as Office 365™ or G-Suite™ but needs to be activated.

Endpoint Protection: Making sure computers have up-to-date security patches, hard drives are encrypted, and strong anti-virus is activated that the municipality can manage remotely. When you are working on-site it is easy to push updates, but when not connected to the domain or offsite on an unsecured network the risk of compromise increases.

Virtual Private Networks (VPNs): Any employee working remotely should only be connecting to the office through a VPN which provides login access through a secured network that also includes identity verification.

Update, Update, Update: Anti-virus protection, Windows updates, and security updates need to be performed as soon as they are available. This is particularly critical for employees using their home computers, or who have had work computers home for an extended period. Having cloud-based anti-virus controls is highly recommended.

By the Numbers:

The Municipal Excess Liability Joint Insurance Fund (MEL) statistics show that **12% to 15% of municipalities** are successfully attacked once per year with costs and ransom demands accelerating into the hundreds of thousands of dollars per incident.

The MEL has already reported a **23% increase** in the costs of these attacks versus 2019, and the year isn't over yet.

Since the pandemic started, the Secret Service has also **prevented about $1 billion in emergency funds** from being lost to malicious actors perpetuating cybercrimes, but they are concerned there is the potential of **up to $30 billion of emergency funds that could be at stake**.

Education: Constant reinforcement of cyber safety awareness and best practices through education and training is a must for all leaders and employees. Something as simple as using your work computer to help your child with their homework could result in malware attaching to the computer and then spreading to your office network when proper precautions aren't taken.

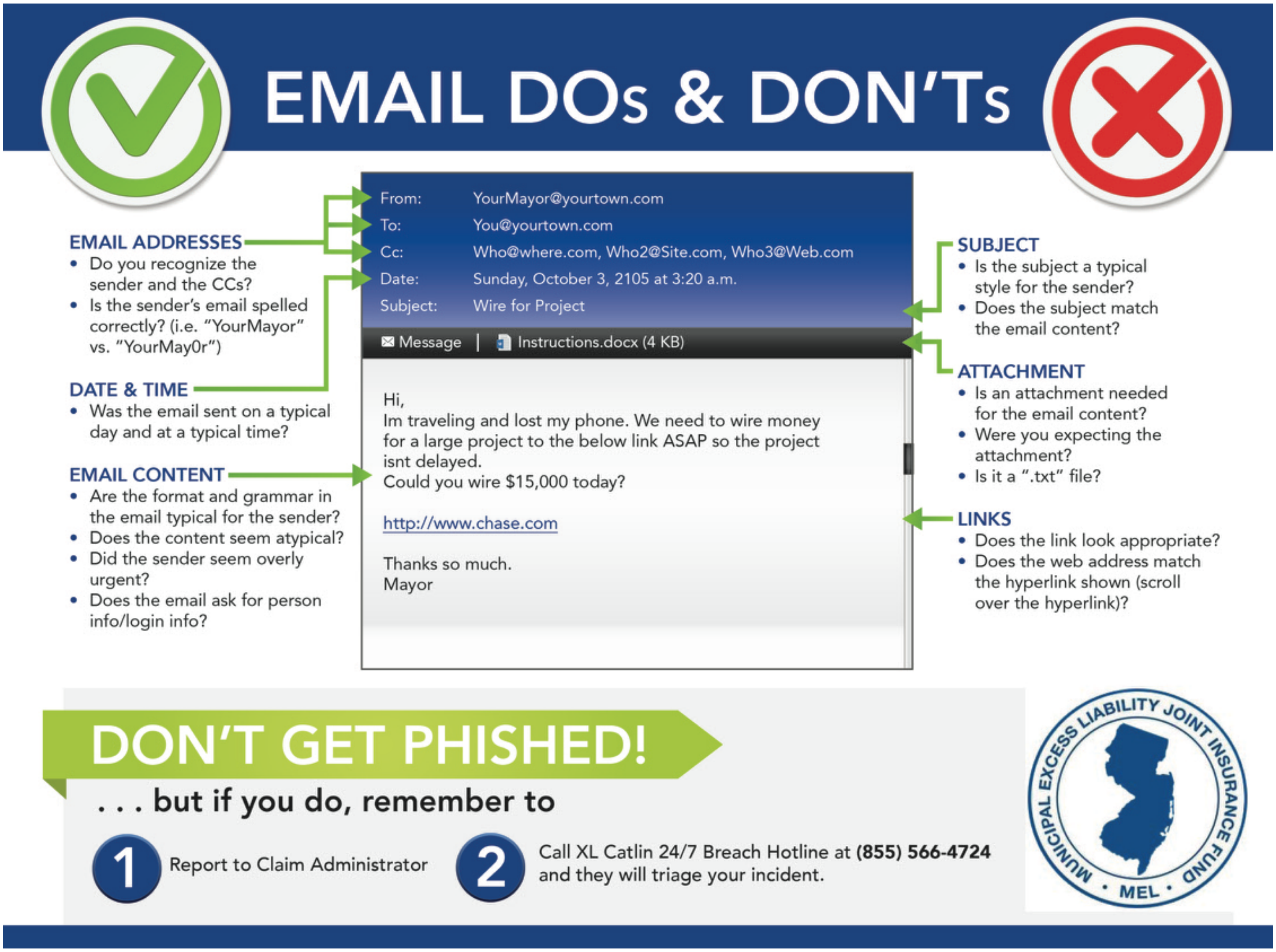
Security assistance

The NJCCIC has seen an uptick in reports of cyber crime since the pandemic started, due in part to the risk that remote working has added to controlling cyber security. The NJCCIC has also provided notifications of over 2,000 compromised credentials to municipalities since May, a service they offer for free.

Whether it is COVID-19, an earthquake or a hurricane, bad actors will always look for opportunities to exploit them. One accidental click on a phishing email or visit to a fake website could leave your town locked out of your network or your vital data and information shared on the dark web.

The most important thing to remember is that you can put all these cyber security plans into place, but if you don't put them into practice it is the same thing as letting a stranger or criminal walk right through your front door.

@ For more information and resources about Cyber Risk Management visit the MEL's website https://NJMEL.org or the latest in cyber security news and strategies visit the NJCCIC website, www.cyber.nj.gov.



EMAIL DOs & DON'Ts

From: YourMayor@yourtown.com
To: You@yourtown.com
Cc: Who@where.com, Who2@Site.com, Who3@Web.com
Date: Sunday, October 3, 2105 at 3:20 a.m.
Subject: Wire for Project

✉ Message | Instructions.docx (4 KB)

Hi,
Im traveling and lost my phone. We need to wire money for a large project to the below link ASAP so the project isnt delayed.
Could you wire $15,000 today?

http://www.chase.com

Thanks so much.
Mayor

EMAIL ADDRESSES
- Do you recognize the sender and the CCs?
- Is the sender's email spelled correctly? (i.e. "YourMayor" vs. "YourMay0r")

DATE & TIME
- Was the email sent on a typical day and at a typical time?

EMAIL CONTENT
- Are the format and grammar in the email typical for the sender?
- Does the content seem atypical?
- Did the sender seem overly urgent?
- Does the email ask for person info/login info?

SUBJECT
- Is the subject a typical style for the sender?
- Does the subject match the email content?

ATTACHMENT
- Is an attachment needed for the email content?
- Were you expecting the attachment?
- Is it a ".txt" file?

LINKS
- Does the link look appropriate?
- Does the web address match the hyperlink shown (scroll over the hyperlink)?

DON'T GET PHISHED!

. . . but if you do, remember to

1. Report to Claim Administrator
2. Call XL Catlin 24/7 Breach Hotline at **(855) 566-4724** and they will triage your incident.