Thanks for Joining!

Cyber Security

Keeping you and your Organization Safe in a Cyber World

ESIP
EMERGENCY SERVICES INSURANCE PROGRAM
BY McNeil&Co.

Who Are We

David Denniston

Director of Risk Management

- Past Chief, Cortlandville Fire Department
- President, Cortlandville Fire Department
- Fire Commissioner, Virgil Fire District
- Board Member, AFDSNY

Who Are We

Lee Price, *NRP, CIC*

Risk Management Training Specialist

- 30-year veteran of fire and EMS
- Retired City of Cortland Fire Captain
- Director, Tompkins Cortland Community College EMS Training Program

Evolving Problem

- Malicious hackers are attacking at a rate of one attack every 39 seconds
- Of 1,200 organizations in 19 industries surveyed, 81% said they were victim to a successful cyber attack in 2019
- Attacks target personal information and financial information

Real World Examples

Fire Service Organization attacks:

- December 2018 – Virus attack - $25,000 loss
- March 2020 – Ransomware attack on a system - $30,000 loss
- July 2020 – Phishing attack - $20,000 loss
- October 2020 – Spear-Phishing email - $400,000 loss

Types of Attacks

We’re going to review each of these in detail:

- Phishing attacks
- Malware attacks
- Web attacks
- Denial of service attacks
- Insider Threats

Attacks can happen to any computer-based device

Phishing Attacks

- Type of social engineering that tricks a user into clicking a link, sending an email or responding to a malicious request
- Can entice a victim to provide passwords, credit card information, etc.
- Phishing can occur through email, texting or all social media platforms
- Spear-phishing – Attack using specific information portraying themselves as a known person to the victim

Malware Attacks

- 92% of Malware is delivered by email (often due to phishing attacks)
- Malware is code that stealthily compromises and affects a system or network
- Malware has been deployed by countries, businesses and criminal actors
- Can destroy a network or kill performance of a system

Types of Malware

Ransomware

- Will block a victim from accessing their system or threaten data corruption
- Demands a ransom to release the access to prevent data loss.

Spyware

- Code that enters a system or network that monitors activity and shares data
- Can be used to steal passwords, PII, pin numbers and payment information

Viruses

- Code that inserts itself into a particular applications
- Once the app is activated, the virus can steal data, launch denial of service attacks or conduct ransomware attacks

Inside Actors

- Disgruntled members who access systems or share data for personal revenge or gain
- Can hurt us in many ways:
  - Sharing access with a criminal actor or competitor
  - Accessing and sharing confidential or sensitive information
  - Intentionally causing harm to operations, data and/or records
- Most difficult to detect/prevent but monitoring helps

Prevention and Protection

Have an IT/Cyber security manager:

- Qualified person to manage security and access to the systems
- Monitors the integrity of the data and the network
- Audits user’s use of systems
- Responsible to keep up with changes in personnel and systems

Basics of Cyber Security

- Use protection software
  - Anti-virus or anti-malware with real time monitoring
  - Set to regularly scan systems for virus and malware
- Keep systems and operating systems updated
  - Most operating system updates are for security updates
  - Also make sure routers and modems have most current firmware updates
- Use router and access point security
  - Open Wi-Fi networks are exposed to theft of service and open to access
  - Change the router and modem setup passwords from factory defaults

Basics of Cyber Security

- Use Firewalls
  - Limits external access from unauthorized users
  - Can also prevent malware and internal threats from accessing outward
- Remove unnecessary software and services
  - Factory default configurations and applications can be vulnerable to malware
  - Apps running in the background can be captured by malware
- Regular Backups
  - Save data to a secure place, externally or on a credible cloud service
  - Use encryption to protect access to the backup data
- Always log out or lock a system when a system will be unattended

Email Threat Recognition

Common indicators of a scam or phishing email:

- Look at the sender's address – suspicious?
- Is the greeting or signature too generic or vague?
- Roll the cursor over the hyperlinks or website
  - URLs are not legitimate, spelled differently or have wrong extension
- Spelling and Grammar not meeting expectations for the source
- Suspicious attachments
  - Unsolicited email with attachments
- False sense of urgency to click a link or attachment

Common Email “Hooks”

- “We need information, or your account will be closed”
- “Immediately click the link below to...”
- “Time sensitive, review the attachment to verify your accounts”
- “Click the following link to verify your SSN or to unlock your account”

BREAK DOWN OF Q2 SIMULATED PHISHING EMAILS

Zoom Password Request Received

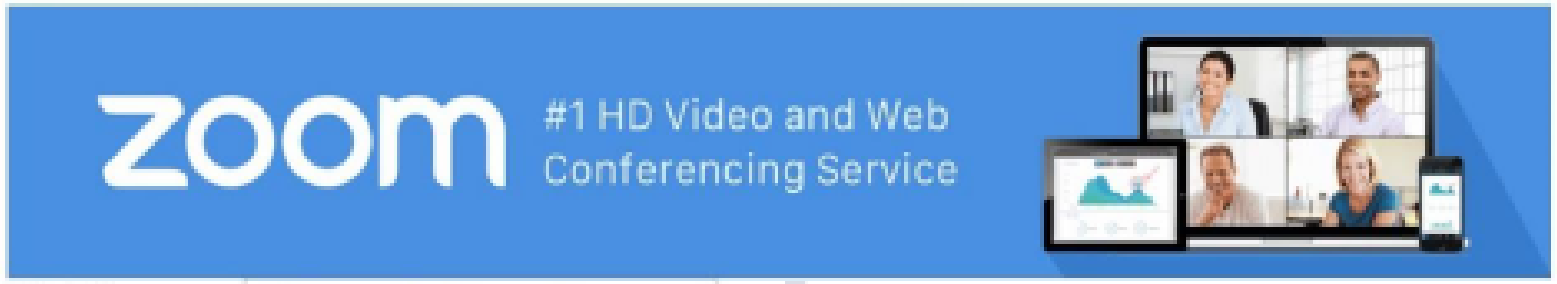
ZS

Zoom Support <zoom.support@techsupport-corp.com>

To

1

4/10/2020



Christina,

http://zoom.techsupport-corp.com/c890326b29?l=36
Click or tap to follow link.

2

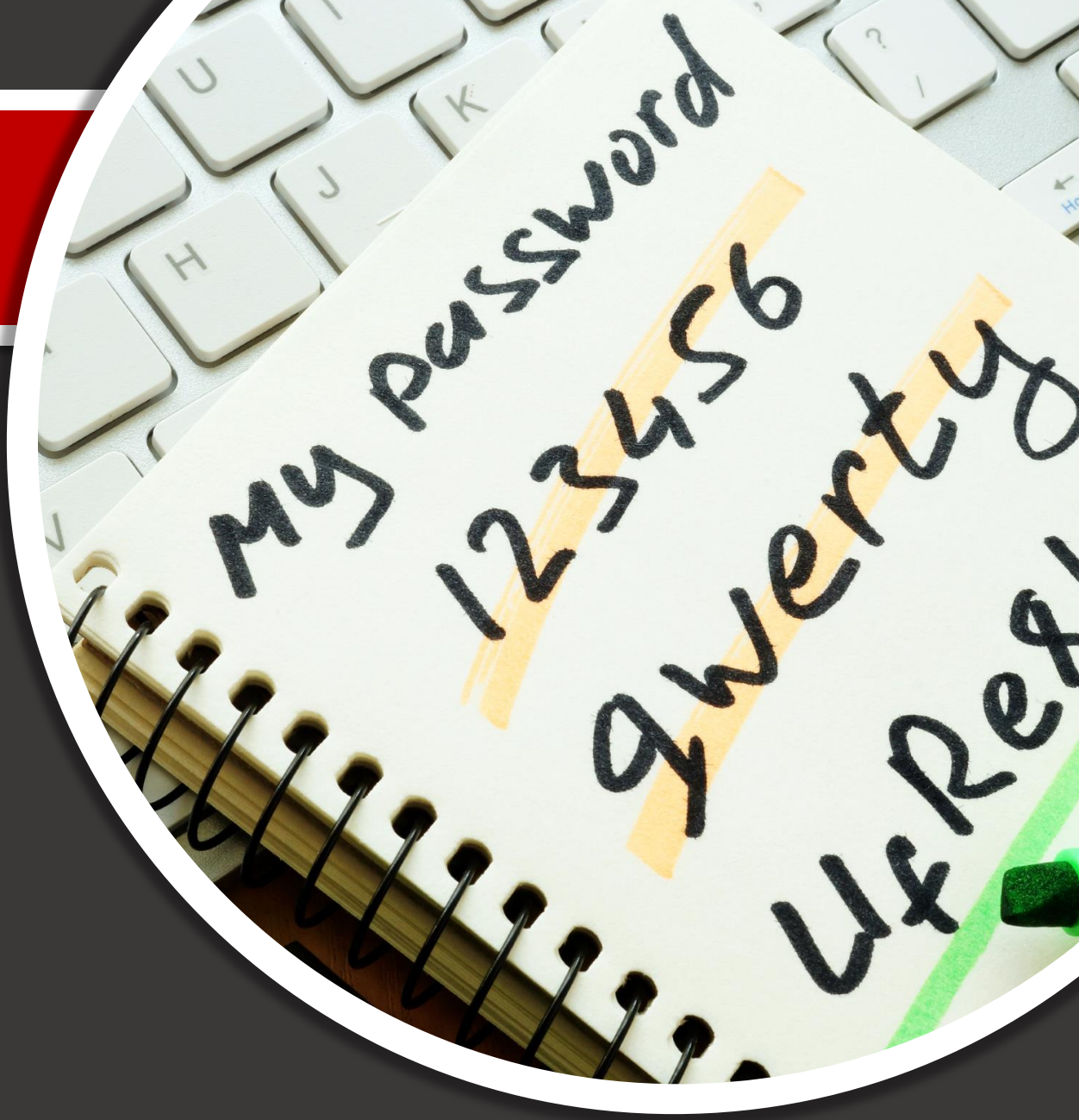
We have recei unt. If you are not aware of this activity, please click here. (Thursday, April 09, 2020)

Thank you,

Zoom Team

Use Complex Passwords

- Passwords can be easily stolen or compromised
  - Change passwords regularly
  - Never share a password
  - Avoid passwords that can be personally linked
    - Important dates, names and number combinations
  - Use different passwords across all systems
- Greater complexity means more security
  - Familiar phrases of more than 15 characters
  - Combinations of upper- and lower-case, numbers and special characters



Organizational Security

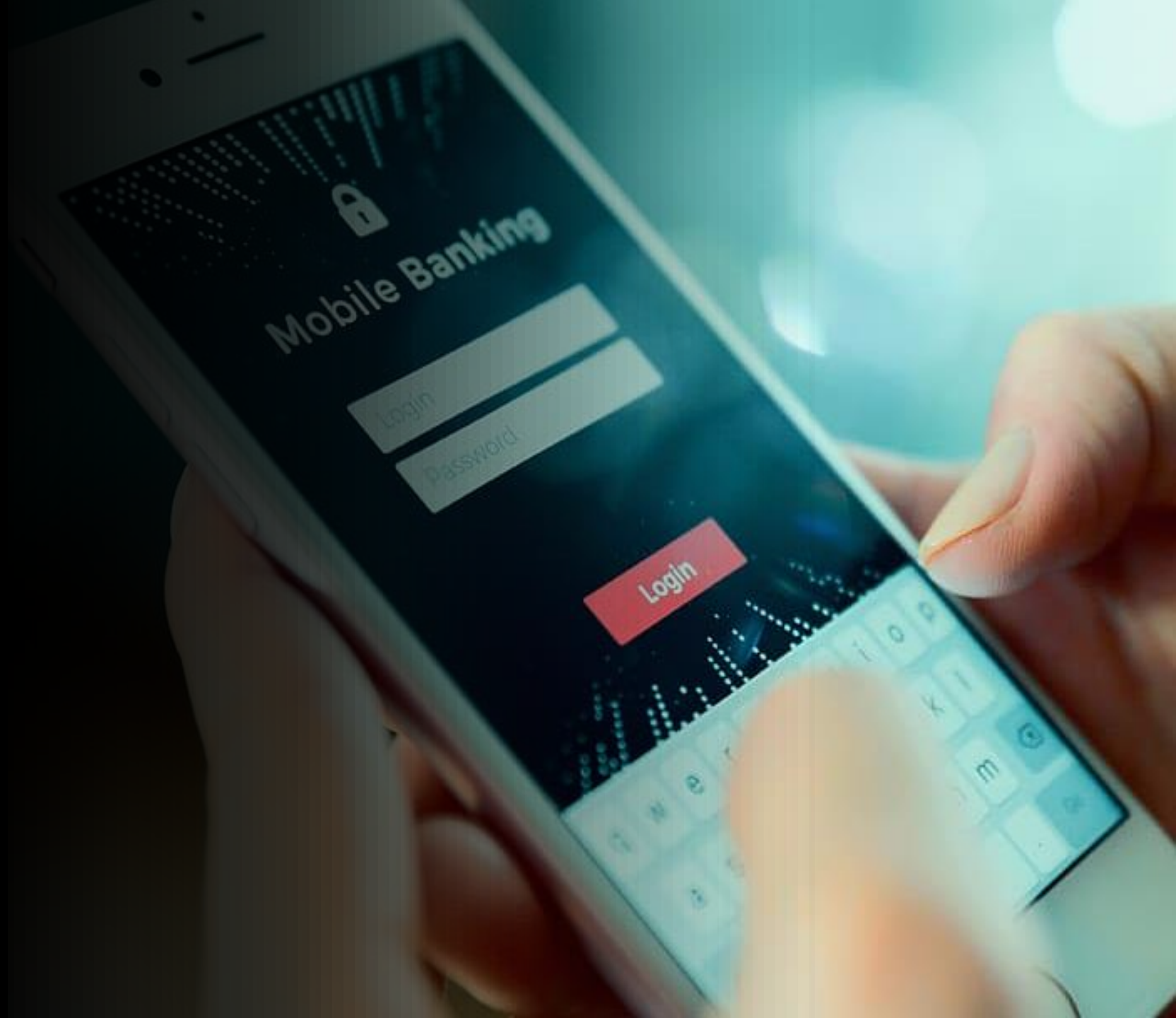
- Limit access to operational and financial systems
- Establish comprehensive computer and social media policies
- Train members on safe computer and network systems usage
- Block access to undesirable sites
- Keep all software and firmware up to date

Wireless Security

- Use the strongest encryption available
- Use unique administrator passwords and SSIDs
- Reduce Wi-Fi signal strength
- Disable remote management
- Limit access of any “Guest” network you provide

Mobile and Personal Devices

- Don’t use applications that are from unknown sources
- Avoid apps that are known to be questionable
- Be suspicious of random text messages, even from those you may be familiar with



Strong Policies

- Organization must take cyber security seriously
- All members need to understand
- Policy must be monitored with monthly check up
- Remind member on a regular basis
- Too late is Too late

How has COVID affected Cyber Security

- More zoom meetings
- Remote access
- Increase in online orders

Recovering from an Attack

- Call for experienced IT support
- Disconnect from the internet
- Backup important files to an isolated place
- Scan your machine
- Reinstall the operating system (wipe the device clean)
- Restore files
- Ensure security protections are in place

We Are Here To Help

- A recording of this presentation will be available on eLearning
- A Certificate will be available for attending. Our automated system should send you one within 5 days

Email us at riskmanagement@mcneilandcompany.com

Call us at 1-800-822-3747 ext. 176