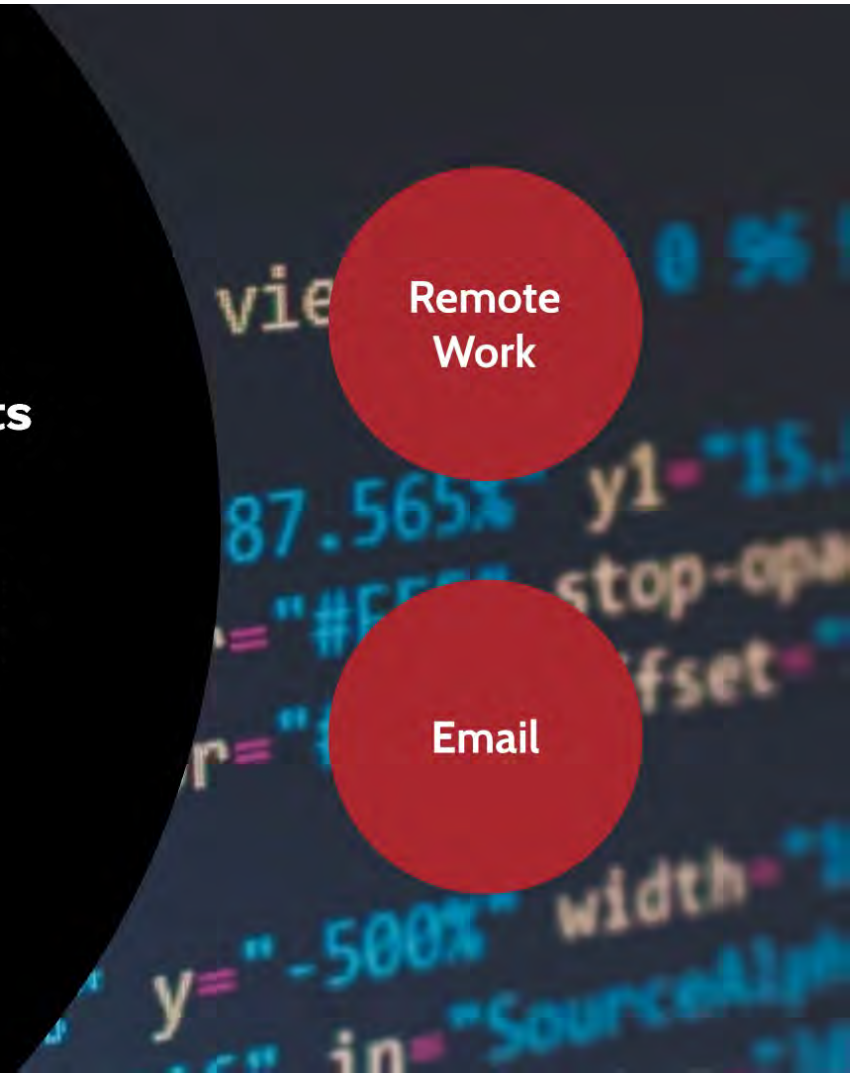
Protect Your City from Cyberattacks
The Threat
Solutions
Q&A

The Threat

Every hour, **26% of local governments** report a cyberattack.

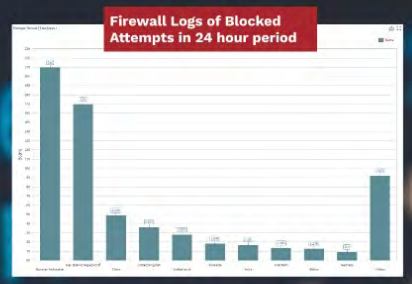
State / Local Attacks have increased **50%** since 2017 - BlueVoyant Report

Just because you are small doesn't mean you aren't a target.

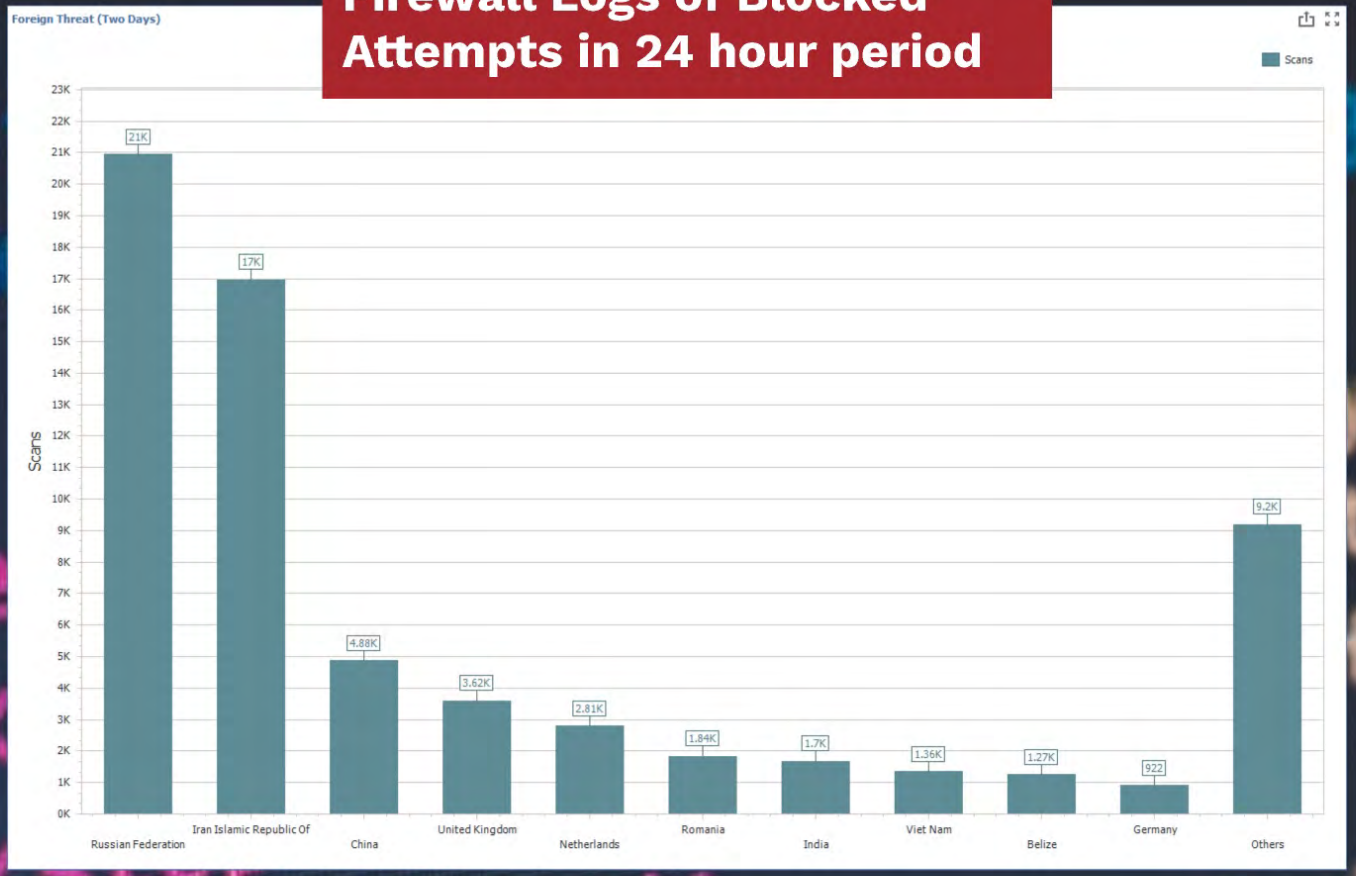


Increase Attacks on Remote Access Systems

- The pandemic has forced workers to do their jobs from home.
- Solutions were implemented quickly to adapt.
- Mobile Phishing to Steal Government Credentials Increased 67% in 2020 - Nextgov.com



Firewall Logs of Blocked Attempts in 24 hour period

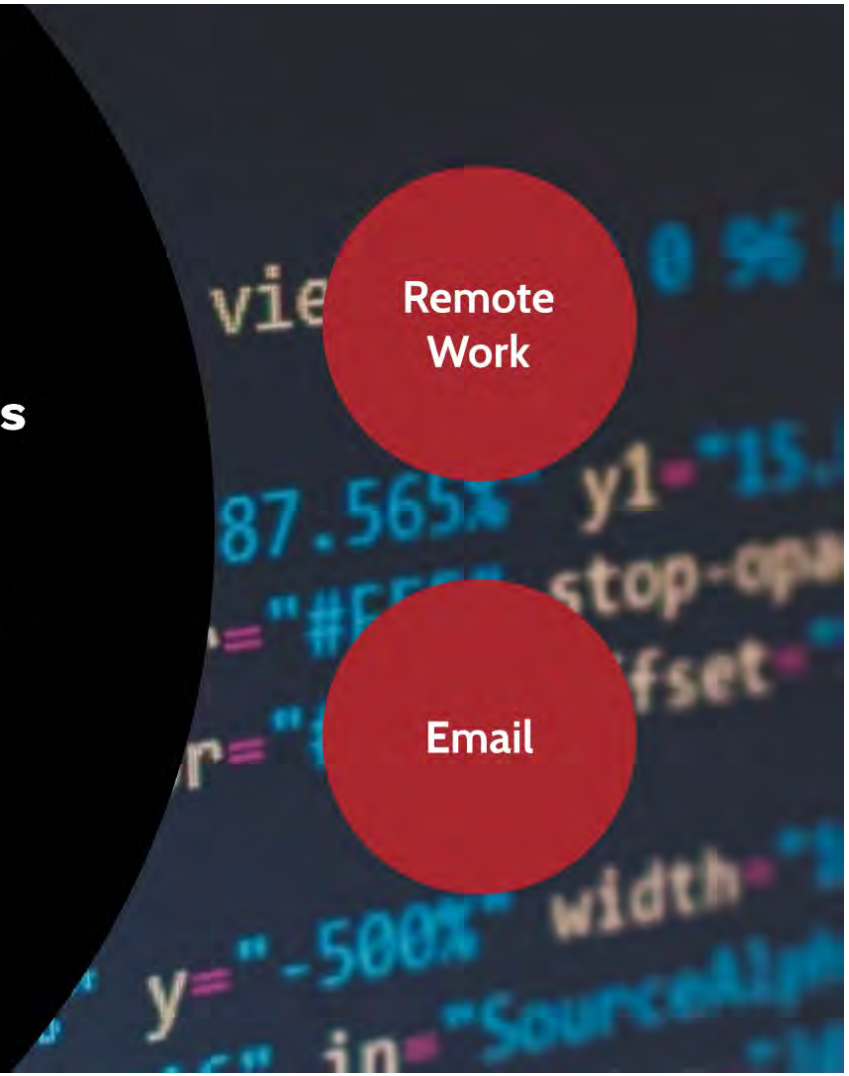


The Threat

Every hour, **26% of local governments** report a cyberattack.

State / Local Attacks have increased **50%** since 2017 - BlueVoyant Report

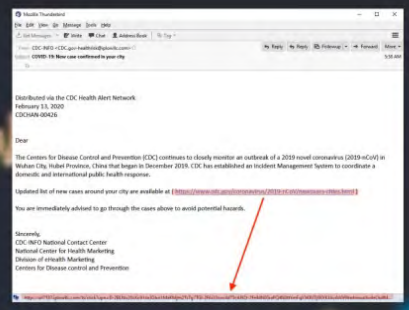
Just because you are small doesn't mean you aren't a target.



Email is Dangerous

The most widely used mechanism by hackers to gain access to organizations.

- Malware
- Phishing
- Social Engineering



Distributed via the CDC Health Alert Network
February 13, 2020
CDCHAN-00426

Dear

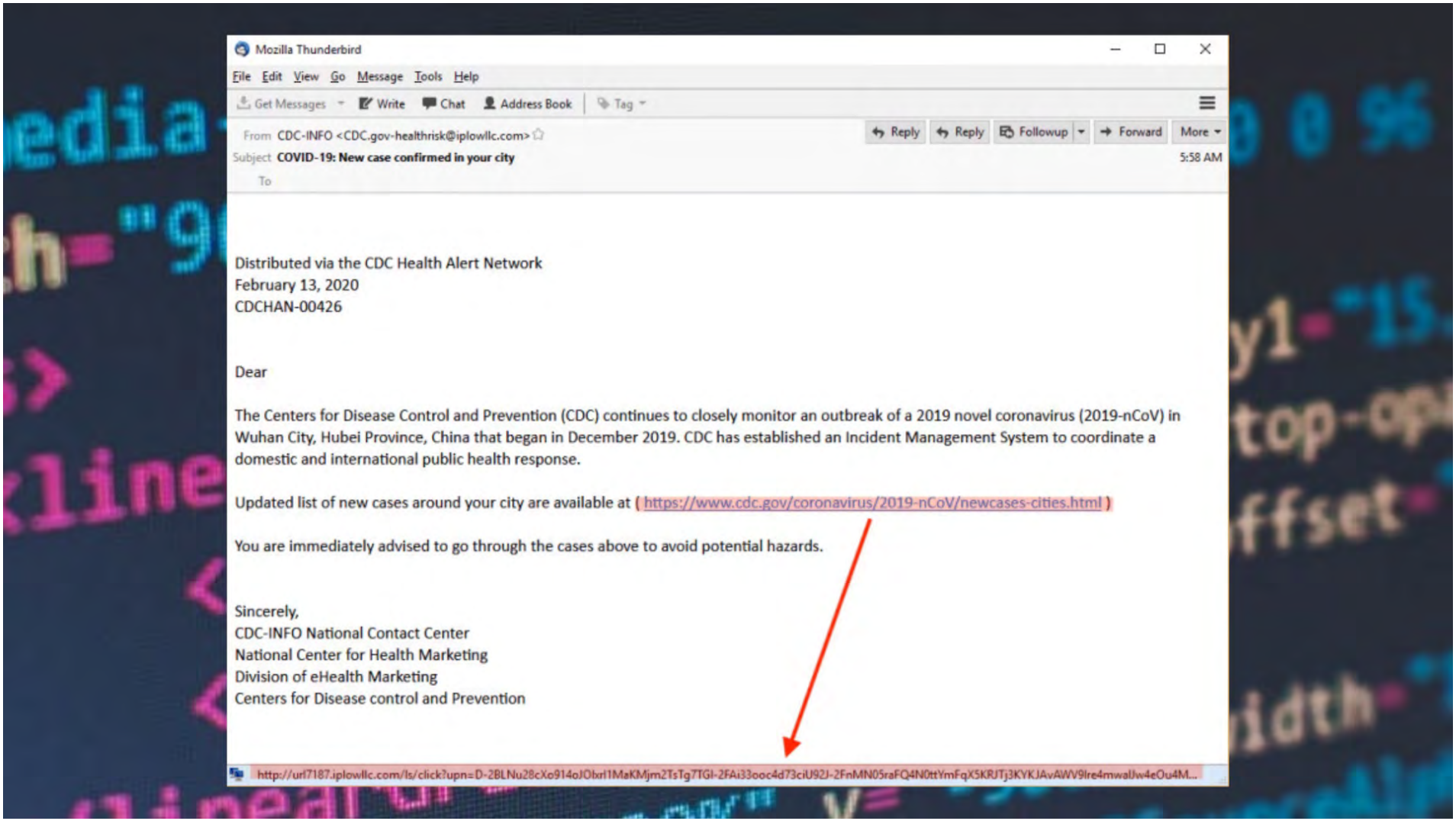
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newsroom-index.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

Sobering Statistics


Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages Write Chat Address Book Tag
From CDC-INFO <CDC.gov-healthrisk@iplowllc.com>
Subject COVID-19: New case confirmed in your city
To
Reply Reply Followup Forward More
5:58 AM
Distributed via the CDC Health Alert Network
February 13, 2020
CDCHAN-00426
Dear
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.
Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)
You are immediately advised to go through the cases above to avoid potential hazards.
Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention
http://url7187.iplowllc.com/ls/click?upn=D-2BLNu28cXo914oJObrl1MaKMjm2TsTg7TGI-2FAi33ooc4d73ciU92J-2FnMN05raFQ4N0ttYmFqX5KRJTj3KYKJAvAWV9lre4mwalJw4eOu4M...

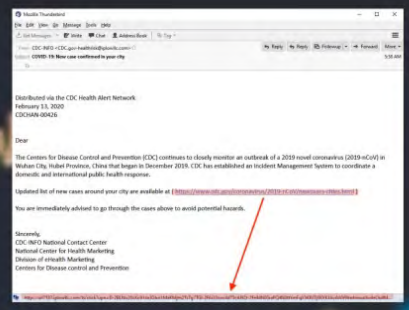
This is Not Going Away

- 92% of malware is delivered by **email**.
- Over the last year, **MacOS** malware has increased by 165%.
- Ransomware attacks are estimated to cost **$6 trillion** annually in 2021.
- Baltimore has had to pay **$18 Million** from a Ransomware attack
- Atlanta has spent more than **$5 million**
- **Fake invoices** are the #1 disguise for distributing malware

Email is Dangerous

The most widely used mechanism by hackers to gain access to organizations.

- Malware
- Phishing
- Social Engineering



Distributed via the CDC Health Alert Network
February 13, 2020
CDCHAN-00426

Dear

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at {https://www.cdc.gov/coronavirus/2019-nCoV/newsroom-china.html}

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

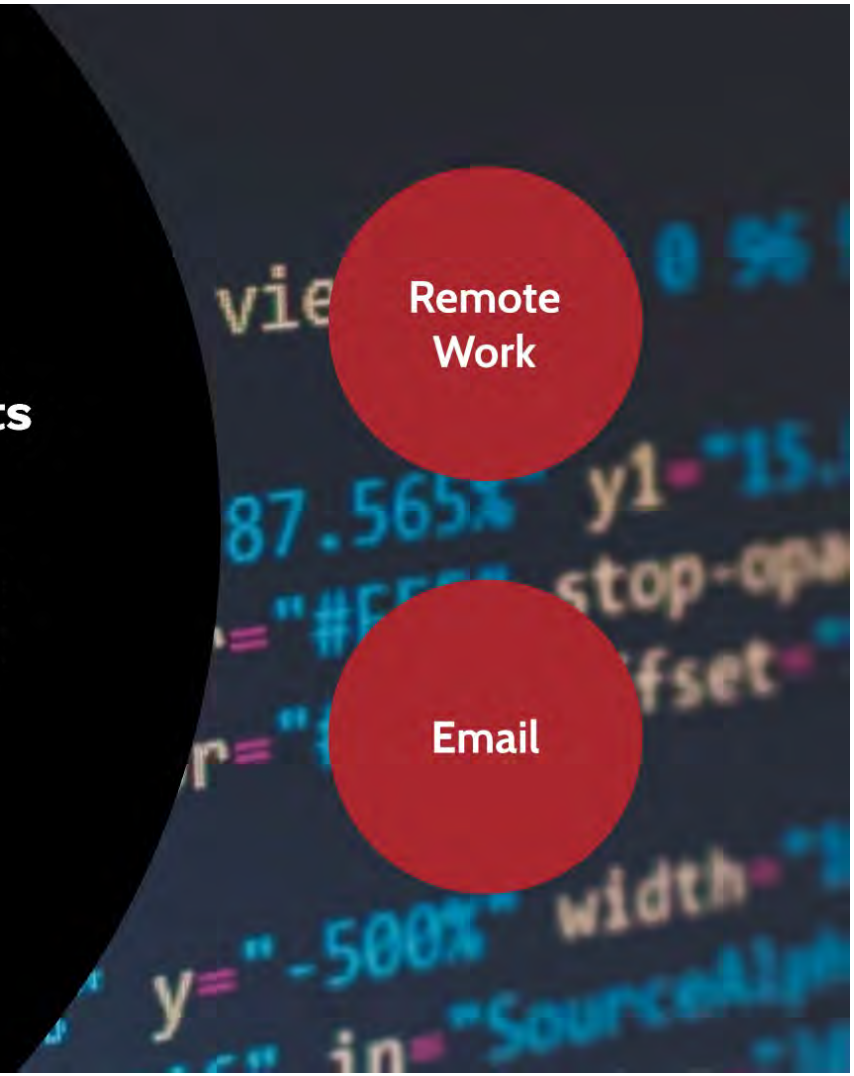
Sobering Statistics

The Threat

Every hour, **26% of local governments** report a cyberattack.

State / Local Attacks have increased **50%** since 2017 - BlueVoyant Report

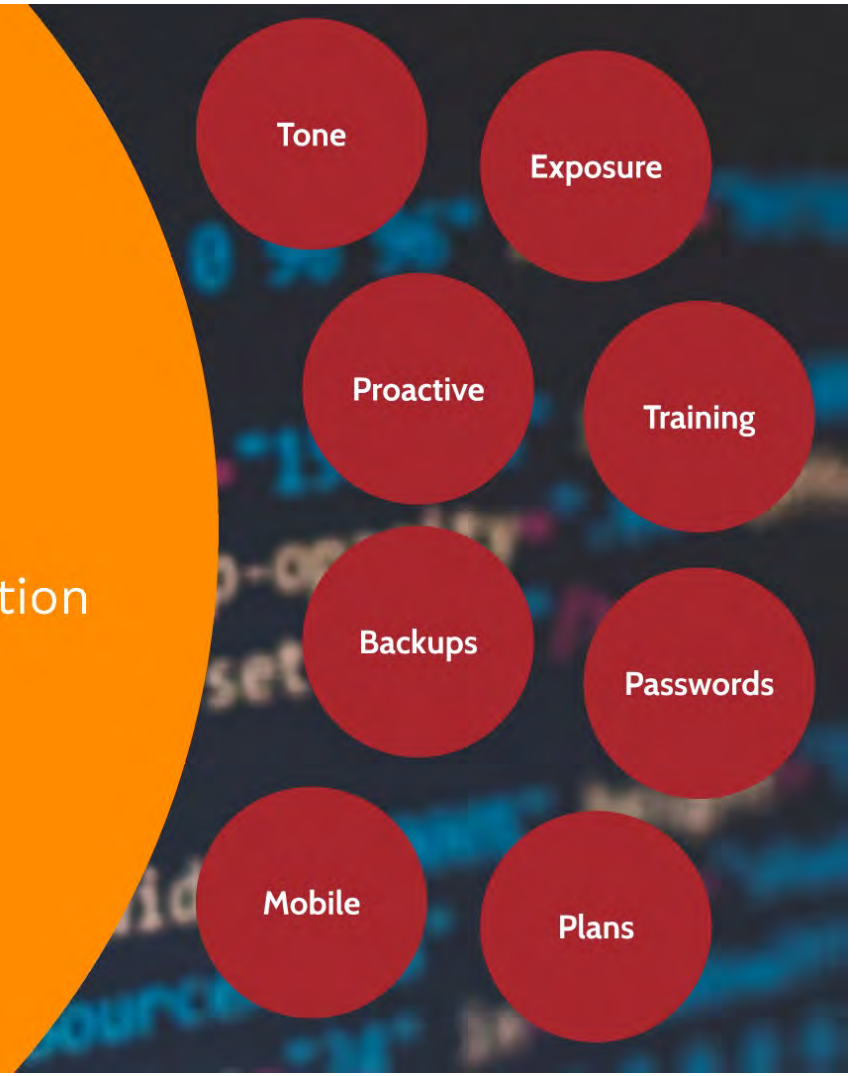
Just because you are small doesn't mean you aren't a target.



Protect Your City from Cyberattacks
The Threat
Solutions
Q&A

Solutions

Securing your computer network is an **ongoing battle**. There is no **SINGLE** solution to provide 100% protection.



Tone from Top

Elected officials need to take IT Security seriously and adequately provide the needed resources.

Local leaders should work to promote a shift toward cybersecurity as a governing priority.

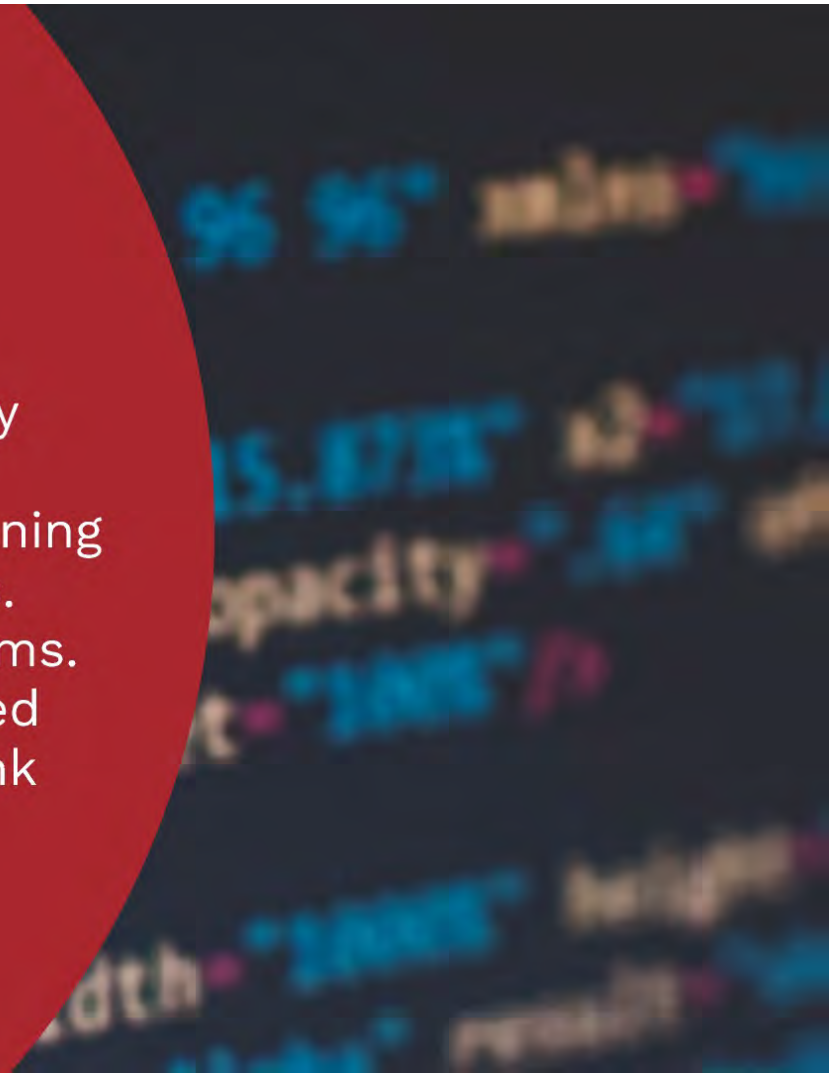
Audits should be performed to located vulnerabilities.

Reduce your external exposure

- Do not host your website on internal servers
- Invest in advanced firewalls
- Use 2FA for Email and VPN access
- Block foreign access to your systems (Country Blocking)
- Secure WiFi Access

Be Proactive

- Conduct regular security vulnerability assessments
- Use external (third-party) email scanning system that monitors and tests links.
- Update computers, software & systems.
- Keep Anti-Virus/Anti-Malware updated
- Develop and enforce controls on bank information changes & wires.



Security Awareness Training

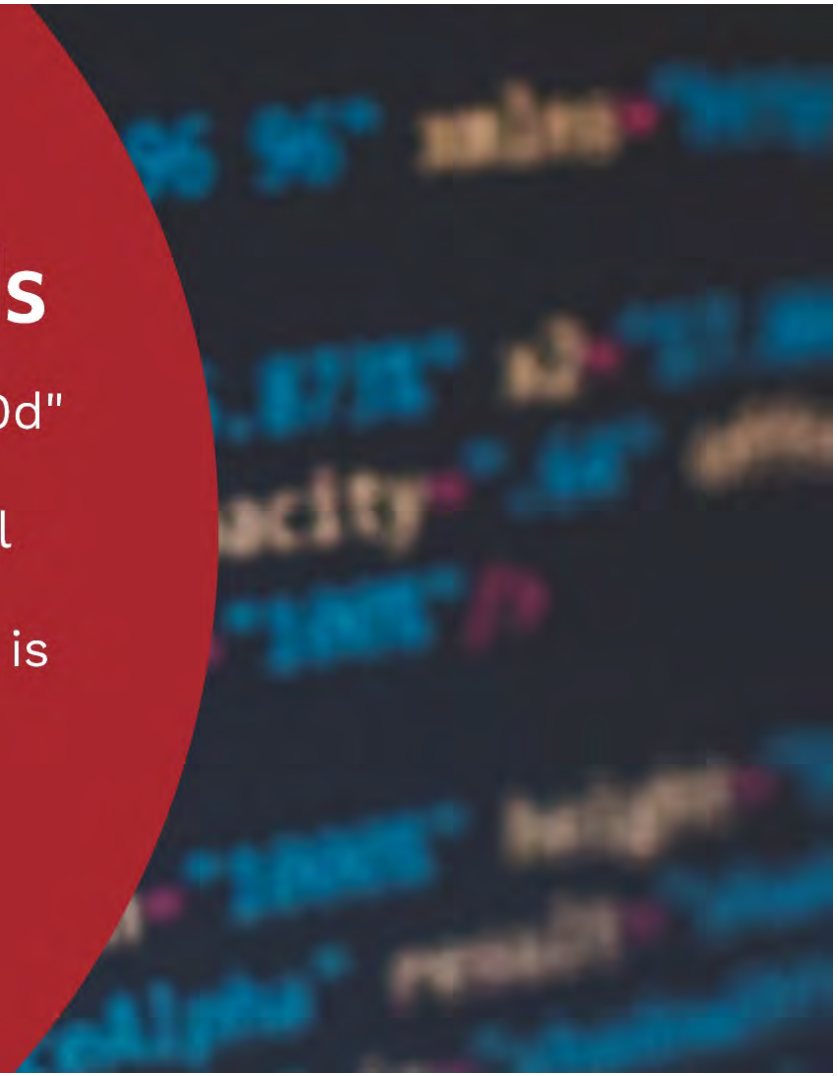
- While investing in sophisticated software & hardware is important, investing heavily in people is also critical.
- There should be ongoing IT security training for all employees and this should be tested throughout the year.

Verifiable Backups

- Store these backups offline or separate from your network
- Restoring those backups should be periodically tested.
- Best recovery option for Ransomware.

Use Strong Passwords

- Gone are the days when "P@ssw0d" will work.
- Use a password management tool like – LastPass or 1Password
- Multi-factor authentication (MFA) is a valuable tool against attacks

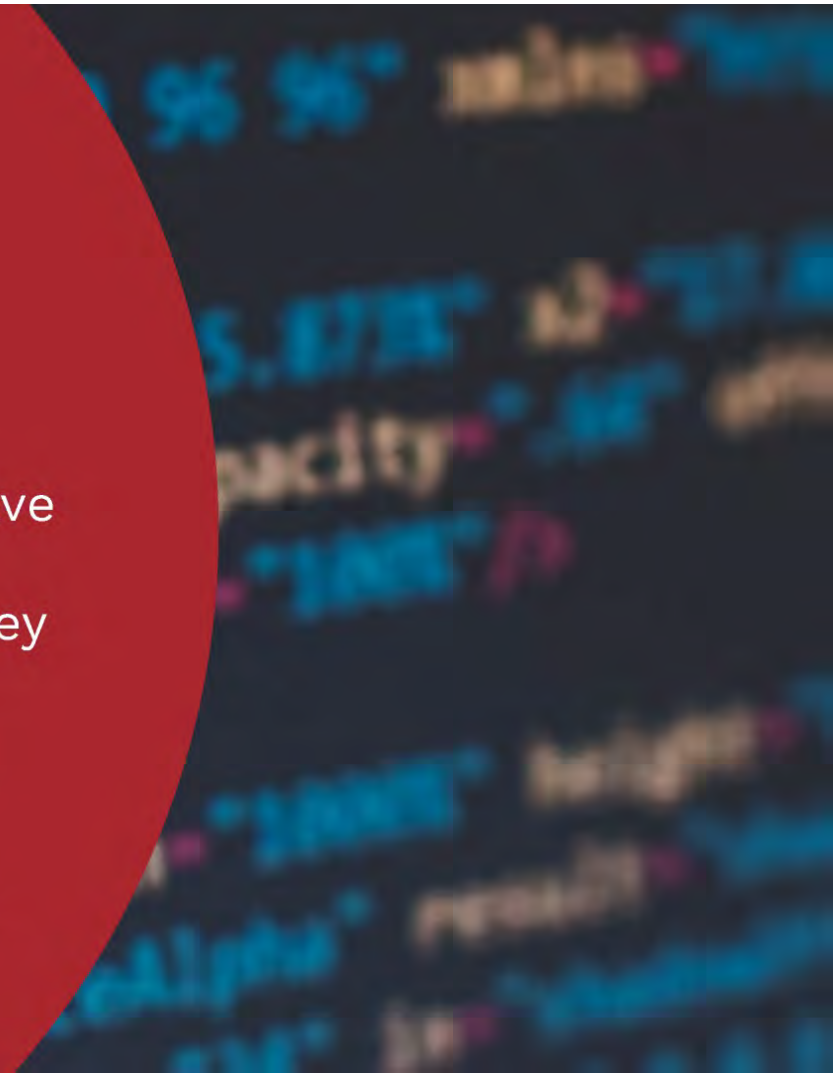


Mobile Device Management

- Consider encryption on mobile devices
- Mobile Device Management with remote location & wipe tools
- Don't use unsecured public Wi-Fi.

Create policies or plans to manage potential attacks

- Every local government should have a cybersecurity response plan.
- The plan should include several key components:
  - Employee awareness training
  - Designated response team
  - Notification Protocols
  - Inventory and Prioritization of system



Additional Resources

The Center for Internet Security
cisecurity.org

Cybersecurity & Infrastructure Security Agency
cisa.gov

David E. Sems, CPA, CITP, CFF
440-580-3193
david.sems@strongsville.org