COVID-19 Updates and Resources for Local Governments

Tuesday, March 23, 2021

Welcome Greeting

Kayla Rosen
Departmental Analyst,
Community Engagement and Finance,
Department of Treasury

Tools and Resources for Local Governments: 11th Webinar

Tuesday, March 23, 2021 – 2 p.m. – 3 p.m.

I. **Welcome & Introductions**
   Heather Frick, Bureau Director, Bureau of Local Government and School Services, Michigan Department of Treasury

I. **Treasury Update**
   a. **CARES Act Grant**
   b. **FDCVT Grant**
   c. **Overviews of Recreational Marijuana Payments**
   d. **American Rescue Plan**
   Eric Bussis, Chief Economist and Director of the Office of Revenue and Tax Analysis, Michigan Department of Treasury

I. **Cybersecurity for Local Governments**
   Derek Larson, Acting Deputy Chief Security Officer, Department of Technology, Management and Budget (DTMB)

I. **Question and Answer**

II. **Closing Remarks**
   Heather Frick, Bureau Director, Bureau of Local Government and School Services, Michigan Department of Treasury

Welcome & Introductions

Heather Frick
Bureau Director,
Bureau of Local Government and School Services,
Department of Treasury

Treasury Local Government Funding Update

Eric Bussis
Chief Economist and Director
Office of Revenue and Tax Analysis
Michigan Department of Treasury

Agenda

Treasury Update

- CARES Act Grant
- FDCVT Grant
- Overviews of Recreational Marijuana Payments
- American Rescue Plan

CARES Act Grant Programs

First Responder Hazard Pay Premiums Program (FRHPPP)

- Payments made to 740 applicants, supporting approximately 37,500 first responders
- 97 applications were selected for further federal subrecipient monitoring
- Audits are nearly complete and only seven audits still unfinished

Public Safety and Public Health Payroll Reimbursement (PSPHPR)

- Updated payment estimates are now online for applicant review
- Payments will be issued after receiving outstanding information from applicants and final reviews
- Of the 492 awards, 65 applications were selected for further federal subrecipient monitoring

Coronavirus Relief Local Government Grants (CRLGG)

- Payments made to 688 local units of government
- 72 applications were selected for further federal subrecipient monitoring
- Preliminary reviews are completed and audits are progressing
    - Eight recipients have not responded

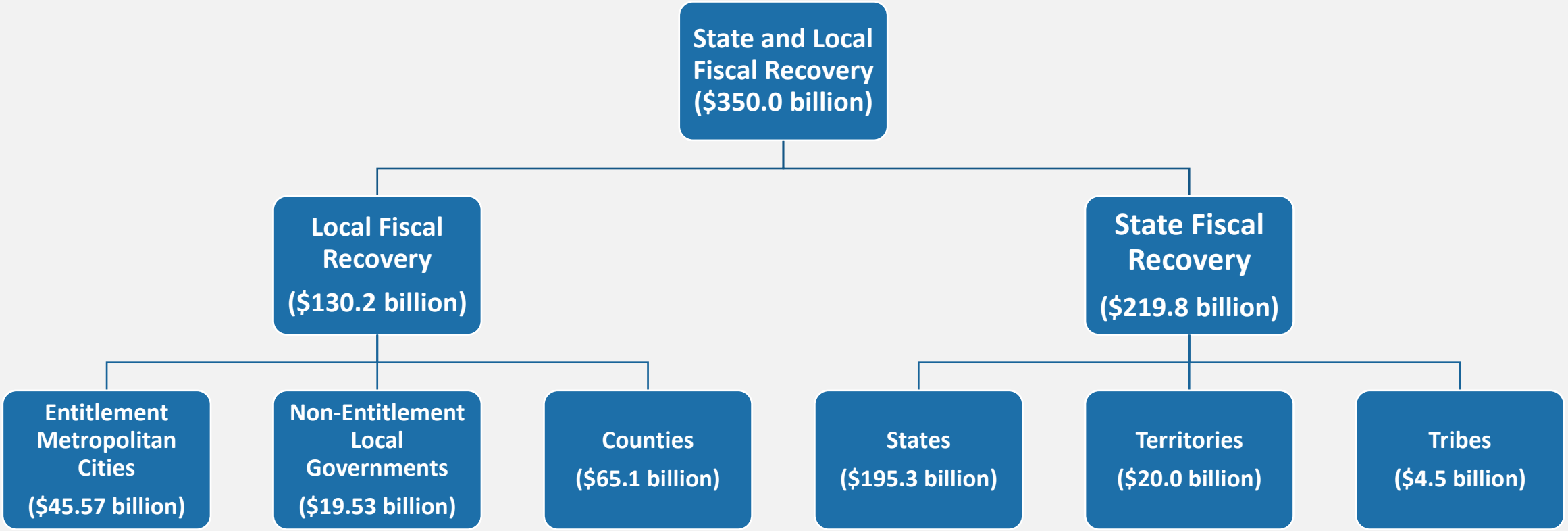
Financially Distressed Cities, Villages and Townships (FDCVT) Grant Program

- Cities, villages and townships experiencing at least one condition of "probable financial distress" as outlined in the Local Financial Stability and Choice Act are eligible
- A total of $2.5 million in funding has been appropriated in fiscal year 2021
- **Municipalities interested in applying for an award must submit applications to the state Treasury Department by 11:59 p.m. on Monday, May 17, 2021**

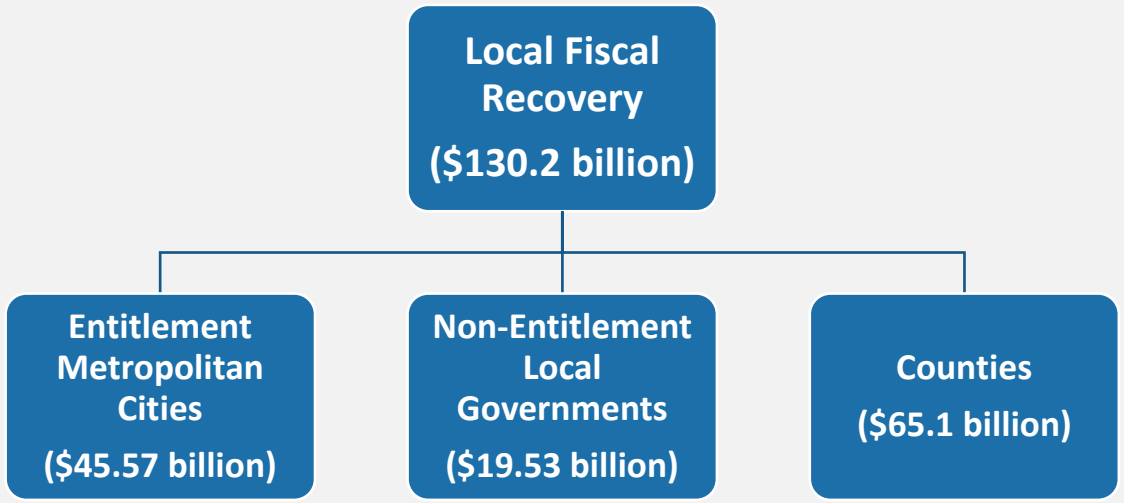
Overviews of Adult-Use Marijuana Payments

- **$9.9 million was issued to counties, cities, villages, and townships**
  - Local units can use the payments as general-purpose revenue
  - Excise tax should be recorded in account 439 within the general fund
- **Annual distributions based on the number of licenses active as of 9/30**
- **Initial year distributions may not reflect future payments**
- **Distributions to the Michigan Transportation Fund, which will flow to Cities, Villages, and County Road Commissions have not been made and are pending appropriation**

American Rescue Plan Act (ARPA)



American Rescue Plan Act (ARPA)



Entitlement Metropolitan Cities

- Based on Community Development Block Grant (CDBG) Entitlement Formula
- Direct payments from US Treasury

Non-Entitlement Local Governments

- To be allocated proportionately based on population
- Funding will first flow to the state, which will have 30 days to distribute to local governments, includes two allowable 30-day extensions
- Allocations to these local governments is capped at 75% of its most recent budget as of January 27, 2020

Counties

- Based on an allocation that considers the county's relative population
- Direct payment from US Treasury

American Rescue Plan Act: Certification, Uses, and Prohibitions

- Allowable uses include the following:
  - Response to public health emergency or its negative economic impacts, including assistance to households, small businesses, non-profits, and affected industries (tourism, travel, and hospitality)
  - Provide premium pay for essential workers, within caps
  - Provide government services to the extent of revenue lost
  - Make necessary investments in water, sewer, or broadband infrastructure
- Prohibited from using funds for pension contributions

All items listed above subject to further US Treasury interpretation and guidance.

American Rescue Plan Act: Many Unknowns

- **Specific amounts allocated to local units of government**
  - Estimates were released by Congressional Oversight Committee
    - State amounts for non-entitlement local governments are national estimates
    - Villages were not included but may receive distributions
    - Population data for non-entitlement communities can be selected by the state
    - Estimates for non-entitlement communities do not include the cap on distributions, which is 75% of the budget as of January 27, 2020
- **Calculation of the 75% of budget cap: General Fund or Total Budget**
- **Methodology for calculation of revenue losses**
  - Overall or by tax type
  - Actual drop or compared to forecast
- **Implementation of the tax cut prohibition for states**
- **Many other regulations, reporting, and restrictions**

How Local Governments Can Prepare

Rod Taylor
Administrator
Community Engagement and Finance
Michigan Department of Treasury

American Rescue Plan Act: How Local Governments Can Prepare

- **Go slow and be conservative with estimates**
- **Update or develop a strategic plan**
- **Be transparent**
- **Think long-term**
  - The state plans to be deliberate and focus spending on transformational projects
- **Focus on financial stability**
  - Best practice is to use one-time funding for one-time purposes
- **Be prepared to document and plan for future audits**
- **Plan for a possible single audit**

www.michigan.gov/CEFD
www.michigan.gov/treasury

@MiTreasLocalGov
@MITreasury

Michigan Department of TREASURY

What is a “Virus”?

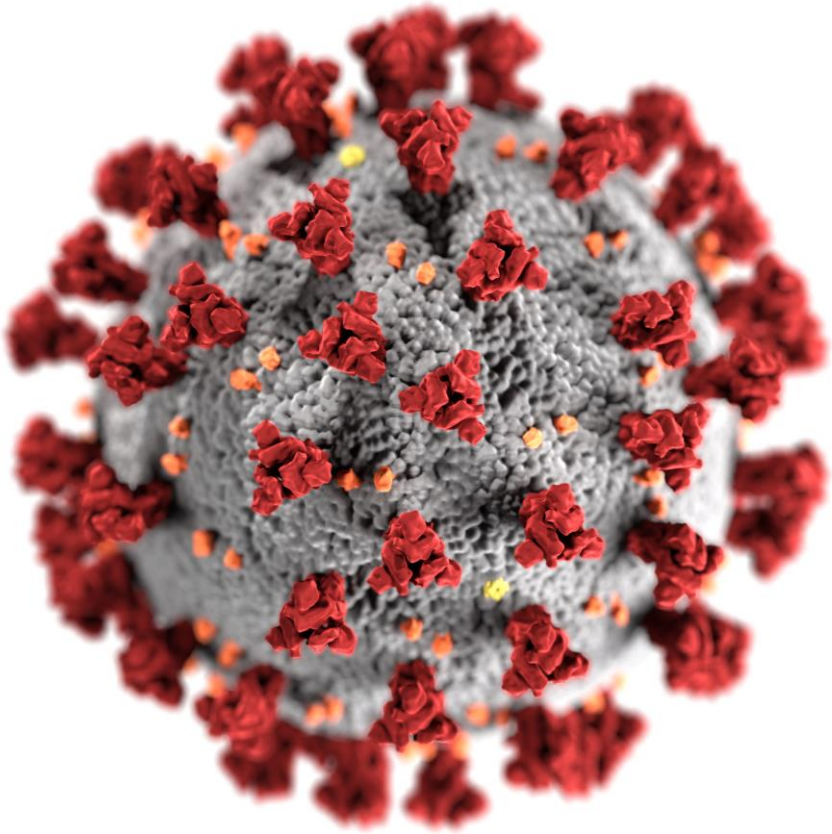
Cybersecurity in Michigan

Presented by Derek Larson
Acting Deputy Chief Security Officer
Tuesday, March 23rd, 2021

DTMB | Cybersecurity & Infrastructure Protection

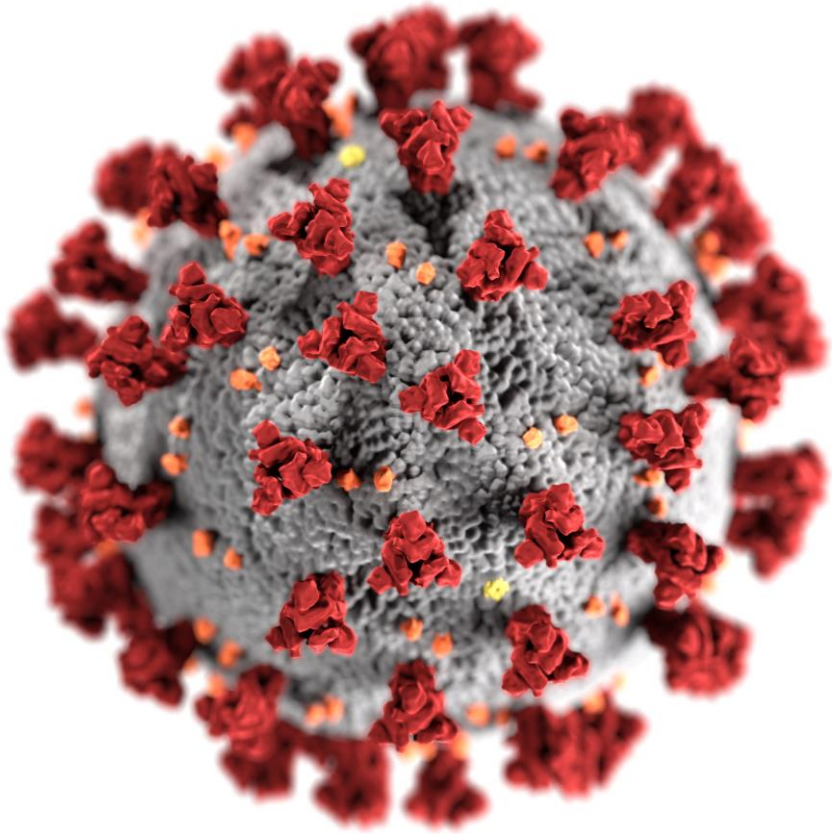
COVID 19 and Cybersecurity

- COVID-19 pandemic has caused many headaches, but…
- It also gives us an opportunity to talk about cybersecurity.
- Businesses can use the pandemic as an opportunity to protect their organization and employees.



Coronavirus vs. Computer Viruses

- A virus, like the coronavirus, looks for hosts (i.e. people) to infect.
- At a VERY HIGH LEVEL, the virus:
  - Inserts itself in healthy cells.
  - Changes the make up of the cell to duplicate itself.
  - Makes copies, which then go and repeat the process with other cells.
- Some viruses are not as serious and a healthy host recovers.
- Other viruses are very serious and destroy the host.

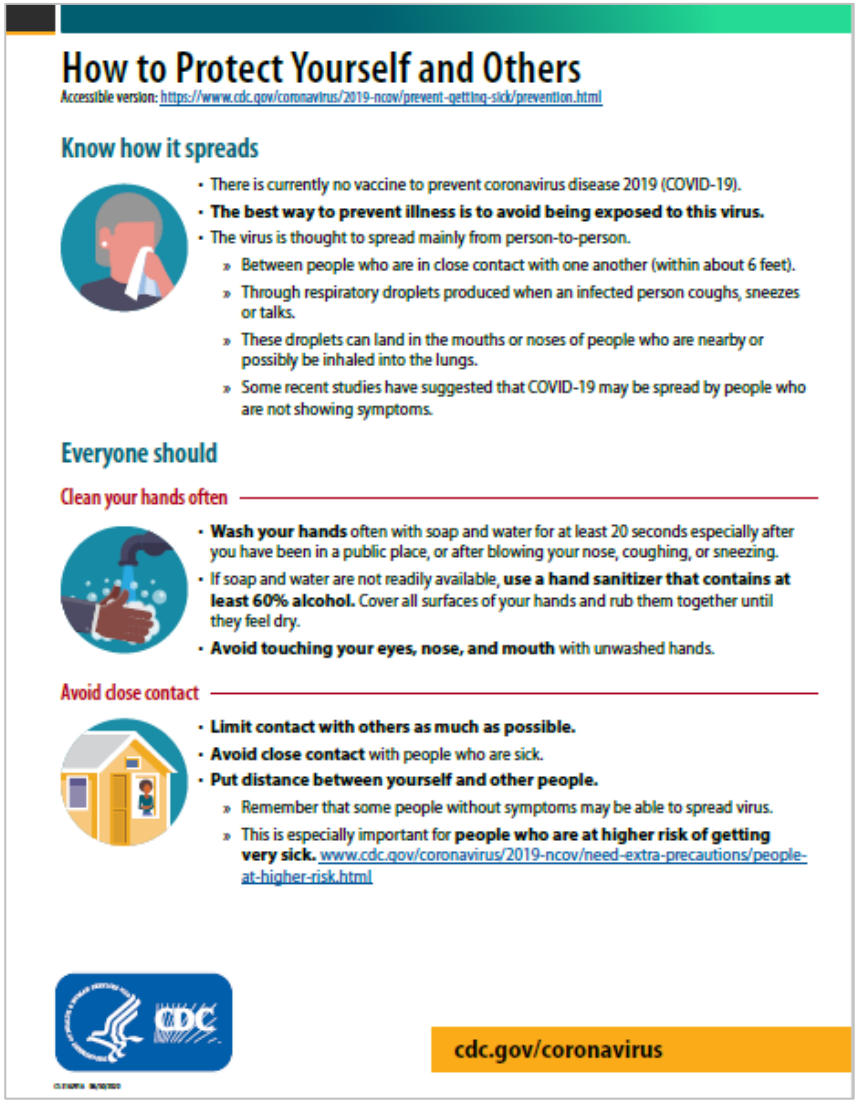


Coronavirus vs. Computer Viruses

- A computer virus is a small piece of code that fuses with other programs or files.
- At a VERY HIGH LEVEL, a computer virus:
  - Attaches itself to files or programs.
  - Changes the code of the file to duplicate itself.
  - Makes copies of itself, which then infect other files and repeat the process.
  - Checks for other computers on a network to infect those as well.
- Some viruses are not as serious and you can restore the computer without too much data loss.
- Other viruses are very serious and destroy the device and any data on it.

CDC Helps Protect Us from Bio Threats

- Preventing the spread of biological viruses involves regulations, policy, services, guidance, and education:
  - Safe handling of food and restaurant inspections
  - Trash collection
  - Education on personal protection
  - Bulletins on emerging threats
  - Outreach and recommendations from various levels of government
  - More…



How to Protect Yourself and Others

Accessible version: https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html

Know how it spreads

- There is currently no vaccine to prevent coronavirus disease 2019 (COVID-19).
- **The best way to prevent illness is to avoid being exposed to this virus.**
- The virus is thought to spread mainly from person-to-person.
  - Between people who are in close contact with one another (within about 6 feet).
  - Through respiratory droplets produced when an infected person coughs, sneezes or talks.
  - These droplets can land in the mouths or noses of people who are nearby or possibly be inhaled into the lungs.
  - Some recent studies have suggested that COVID-19 may be spread by people who are not showing symptoms.

Everyone should

Clean your hands often

- **Wash your hands** often with soap and water for at least 20 seconds especially after you have been in a public place, or after blowing your nose, coughing, or sneezing.
- If soap and water are not readily available, **use a hand sanitizer that contains at least 60% alcohol.** Cover all surfaces of your hands and rub them together until they feel dry.
- **Avoid touching your eyes, nose, and mouth** with unwashed hands.

Avoid close contact

- **Limit contact with others as much as possible.**
- **Avoid close contact** with people who are sick.
- **Put distance between yourself and other people.**
  - Remember that some people without symptoms may be able to spread virus.
  - This is especially important for **people who are at higher risk of getting very sick.** www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/people-at-higher-risk.html

cdc.gov/coronavirus

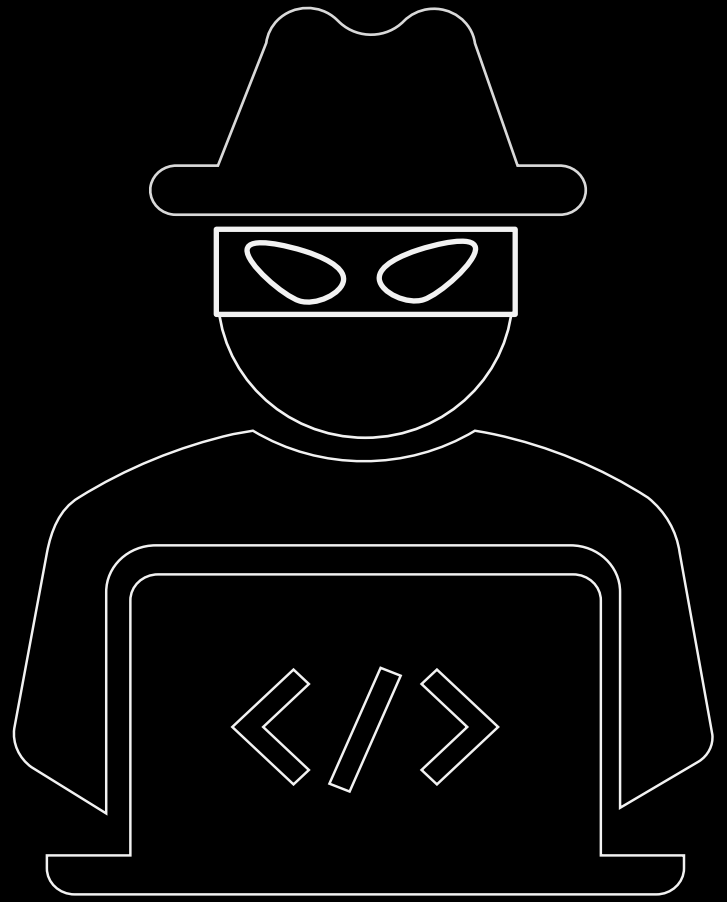
National Cybersecurity Standards Protect Us

- Preventing the spread of computer viruses involves regulations, policy, services, guidance, and education:
  - National standards for readiness
  - (Emerging) policies
  - Education on personal protection
  - Bulletins on emerging threats
  - Outreach and recommendations from various levels of government
  - More…

1075

One Big Difference Between Most Biological Viruses and Computer Viruses:

People Make Computer Viruses with Particular Outcomes in Mind



Who Are These People That Create Viruses?

Various Threat Actors…

Cybercriminals, Nation-States, Hacktivists, Competitors

Disgruntled Employees, Contractors, Business Partners

Compromised Accounts

Who Want…

- Financial gain
- Personal advantage
- Professional revenge
- Outsider influence
- Economic gain
- Corporation or national espionage
- Political or social change
- Military or economical advantage

And Are After…

- Logins & passwords
- Credentials & identifying info
- Emails
- IMs
- Browsing history
- Documents & internal communications
- Photographs
- ***Anything*** that they can use

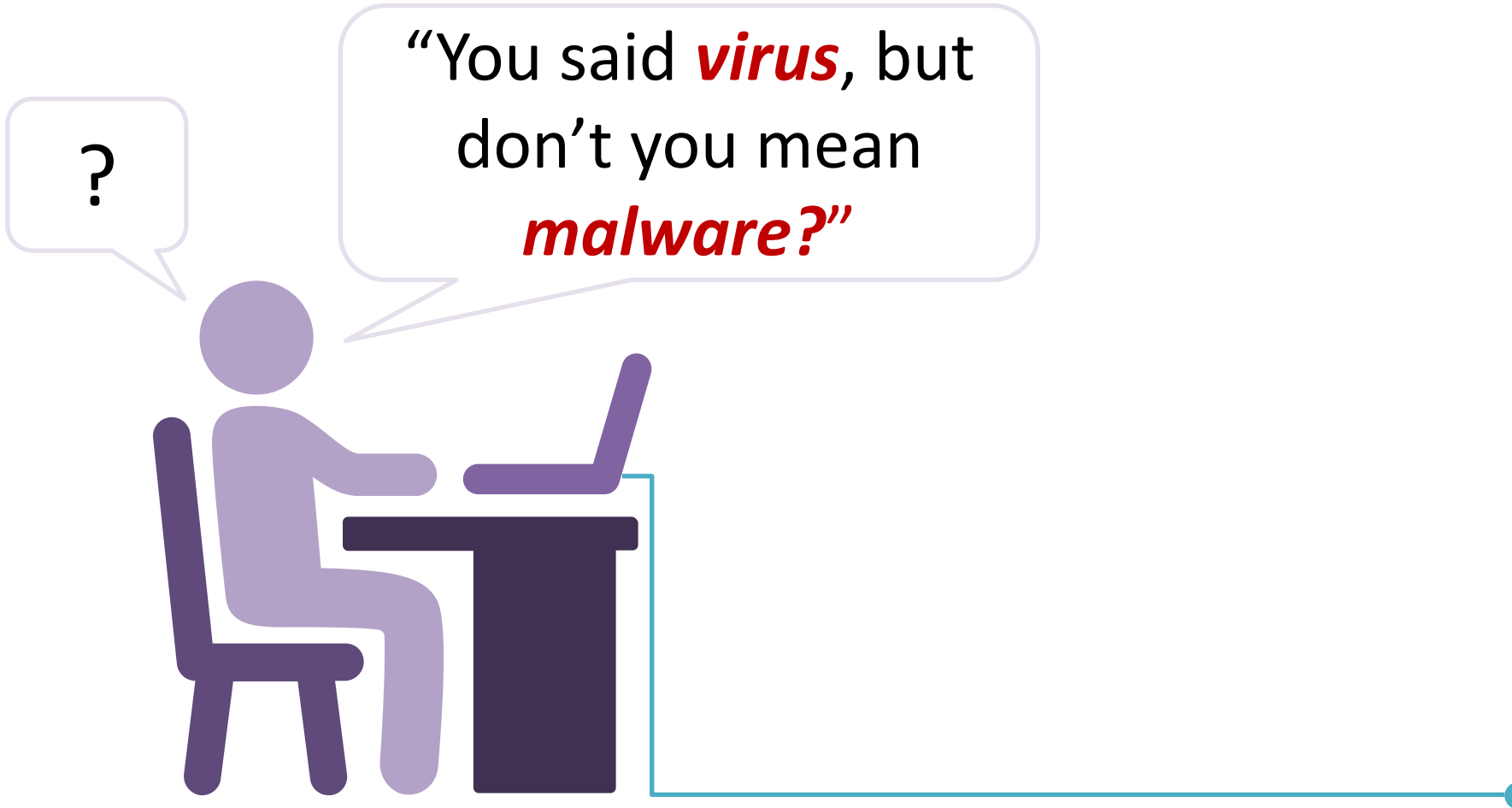
So They Can Get…

Your personal (financial) information

Access to greater business/organization networks

“Virus” Can Be a Misnomer

“Virus" is often misused to refer to malicious threats in general.



There Are All Kinds of Threats Out There


Ransomware


Worms


Rogue Security Software


Spyware


Trojan Horse

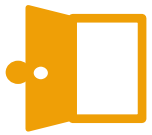

Logic Bomb


Adware


Keystroke Logging


Browser hijacking


Rootkit


Backdoor


Malvertising

And as the technology evolves, the threats evolve with it.

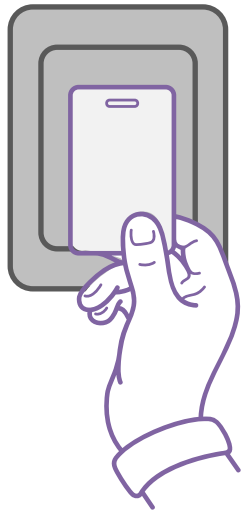
Malicious Cybersecurity Actions

Social Engineering	• Tricks YOU into doing something YOU shouldn't.
Denial-of-Service	• Floods system with traffic and no one can use it.
Remote Access	• Accesses systems remotely without permission.
Web Browsers	• Exploits vulnerabilities and unpatched browsers.
Web Servers	• Exploits unpatched systems and applications.

Threats Aren't Just Virtual

Physical access to workstations, servers, and networks also needs to be monitored and protected to stop malware.

A stolen or unlocked workstation can be an opening for hackers.

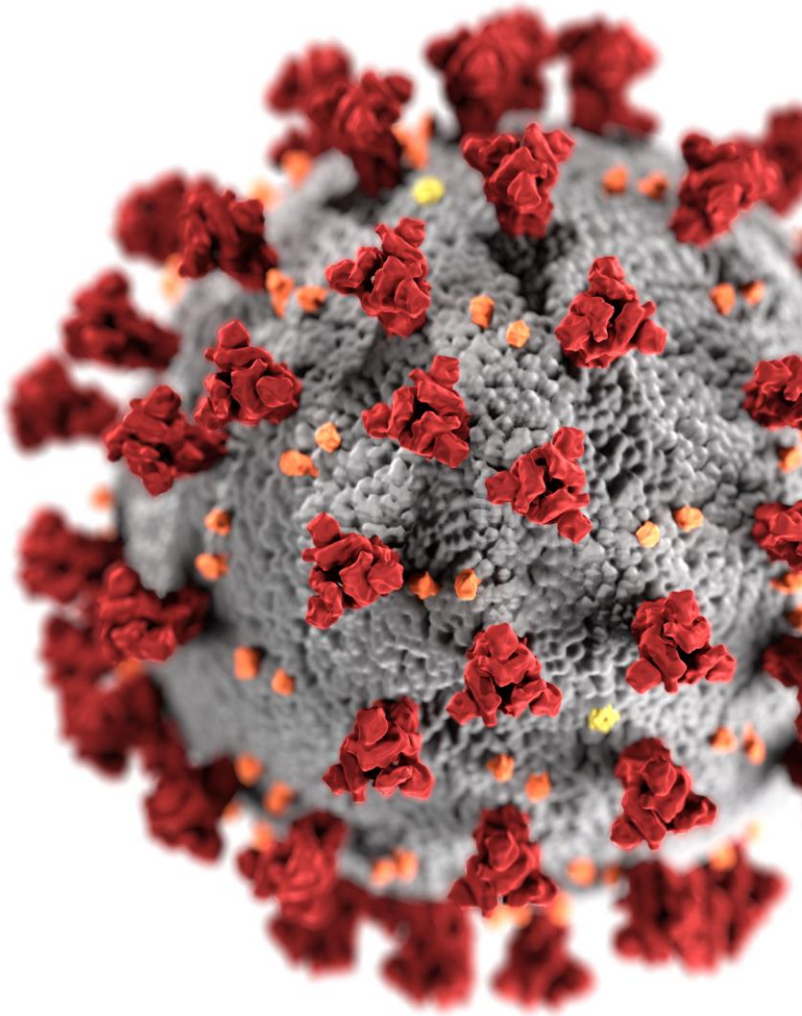


Some rooms and department areas require additional badge access… and piggybacking isn't approved.

It's why team members should wear badges and sign in when visiting other buildings.

COVID-19 Has Raised Additional Vulnerabilities

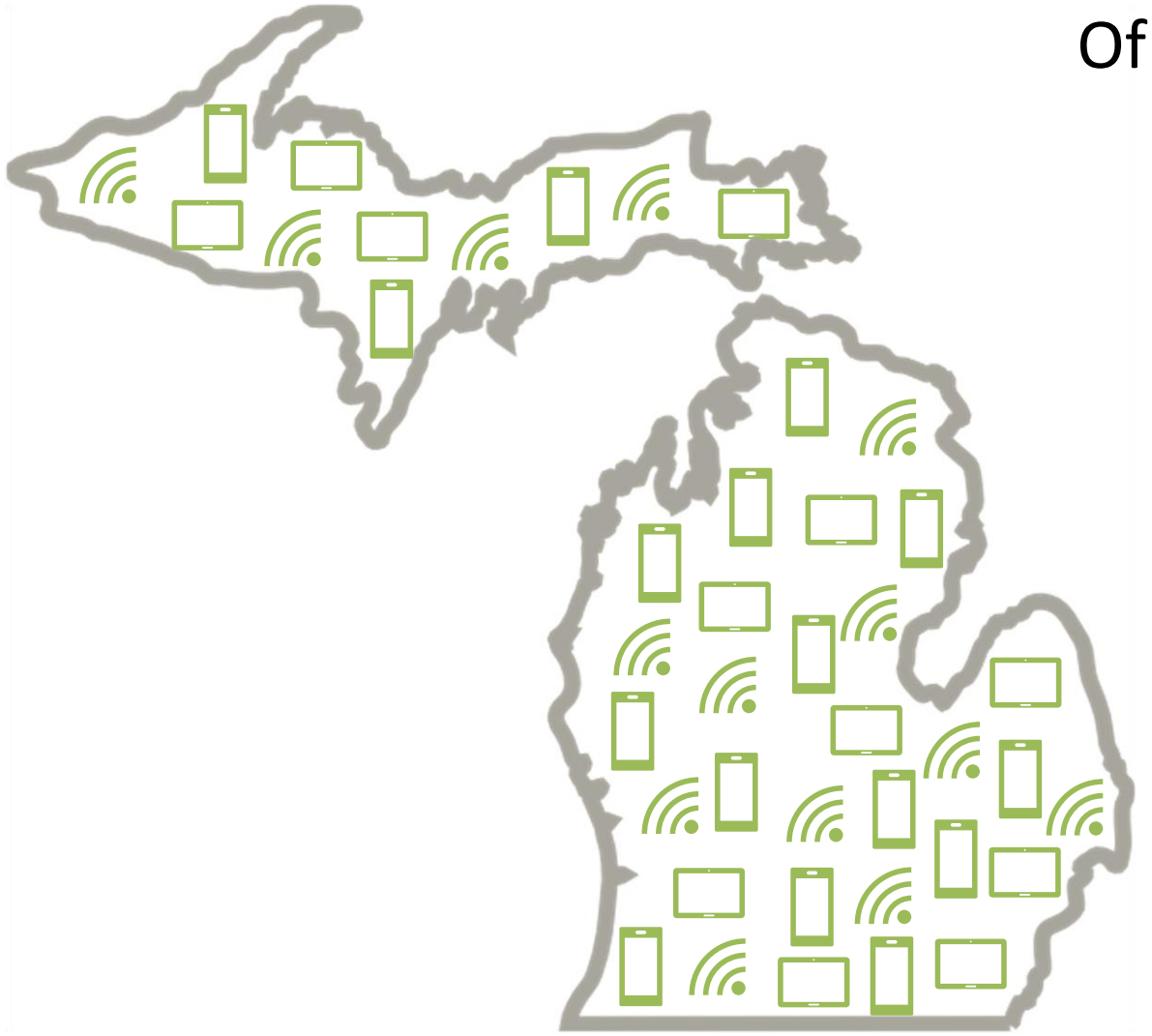
- As the State of Michigan worked to control the spread of COVID-19, many residents were forced to isolate at home.
- Security issues arose from:
  - Working from home on older or unpatched computers.
  - Using mobile technologies and unprotected WiFi.



With New Risks from Working from Home…

- Staying safe from malware has new challenges with teams working from home:
  - Connecting home printers and non-work devices to business/organization networks.
  - Encouraging virtual private network (VPN) tools to access the network securely.
  - Learning the risks to using video conferencing tools, such as Zoom, and accessing them safely.

Vulnerabilities from Mobile Devices…



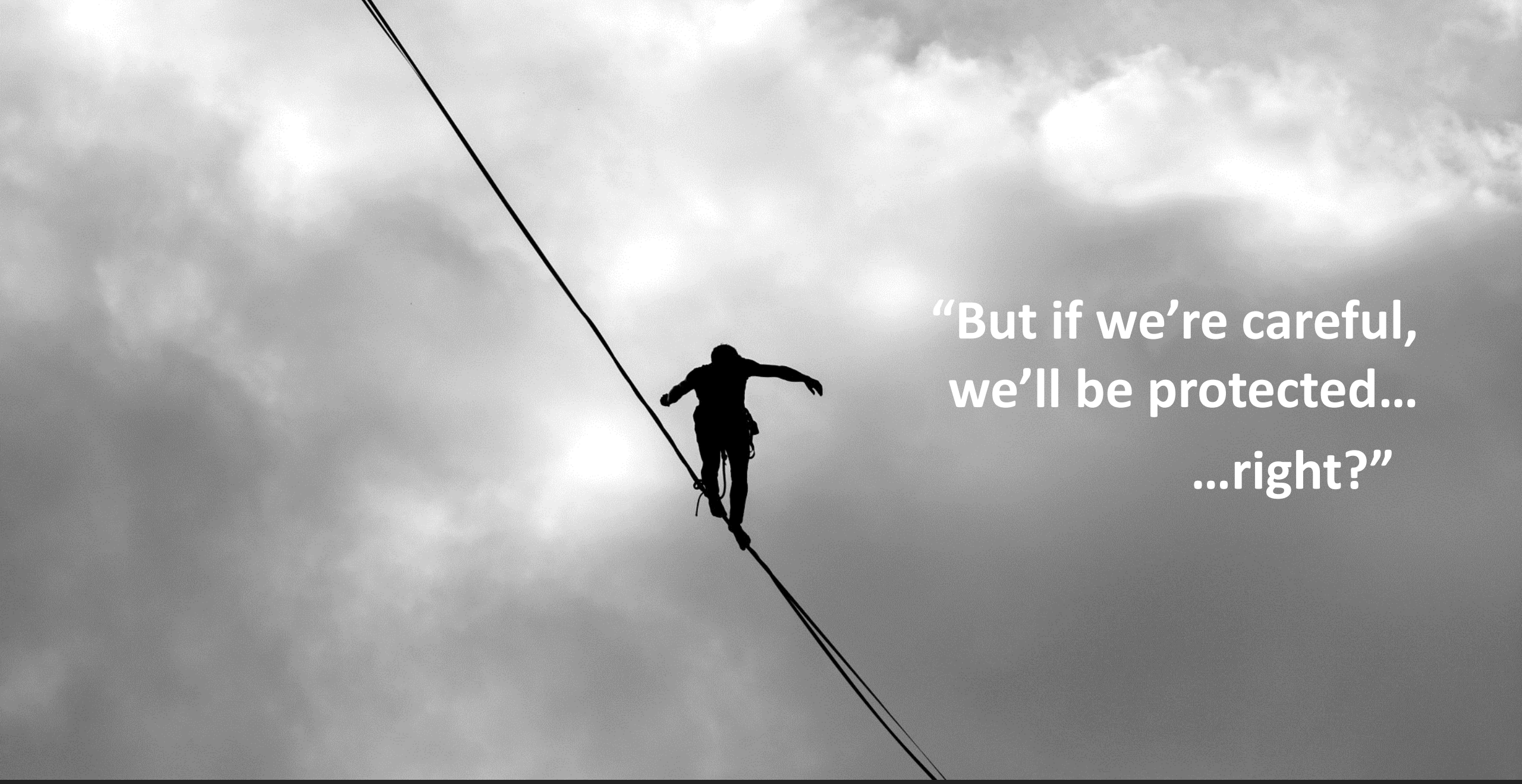
Of Michigan's **10 million** residents…

Many have mobile devices under active attack.

- Contain known malicious apps: **91,200**
- Are currently compromised: **56,000**

Others have mobile devices at serious risk.

- Vulnerable to freely downloadable exploits: **2,614,800**
- Installed apps with a high risk of data leakage: **4,600,000**
- Downloading from suspicious app stores: **634,520**


“But if we’re careful,
we’ll be protected…
…right?”

Local Public Entities are Under Attack

GCN The Technology that Drives Government IT

AI & Automation COVID-19 Cybersecurity Cloud Data & Analytics IoT Emerging Tech Public Safety State & Local

Cyberattacks on state, local government up 50%

BY STEPHANIE KANOWITZ | SEP 04, 2020

Many of the cyberattacks on state, local, tribal and territorial governments are not complicated and could be avoided through simple steps such as improved cyber hygiene and two-factor authentication, a new report states.

UpNorthLive NEWS WEATHER CORONAVIRUS DEALS - SPOTLIGHT CHIME IN WATCH

City of Mt. Pleasant falls victim to remote ransomware attack

by Devon Kessler | Monday, October 12th 2020 AA

The City of Mt. Pleasant said a remote ransomware attack was detected on city computers early Saturday morning. (WLUK image)

ISABELLA COUNTY, Mich., (WPBN/WGTU) -- The City of Mt. Pleasant has fallen victim to a ransomware attack, that is according to city officials.

According to a press release on the city site, a remote Ransomware attack was detected on the city's computer and phone systems on Saturday morning.

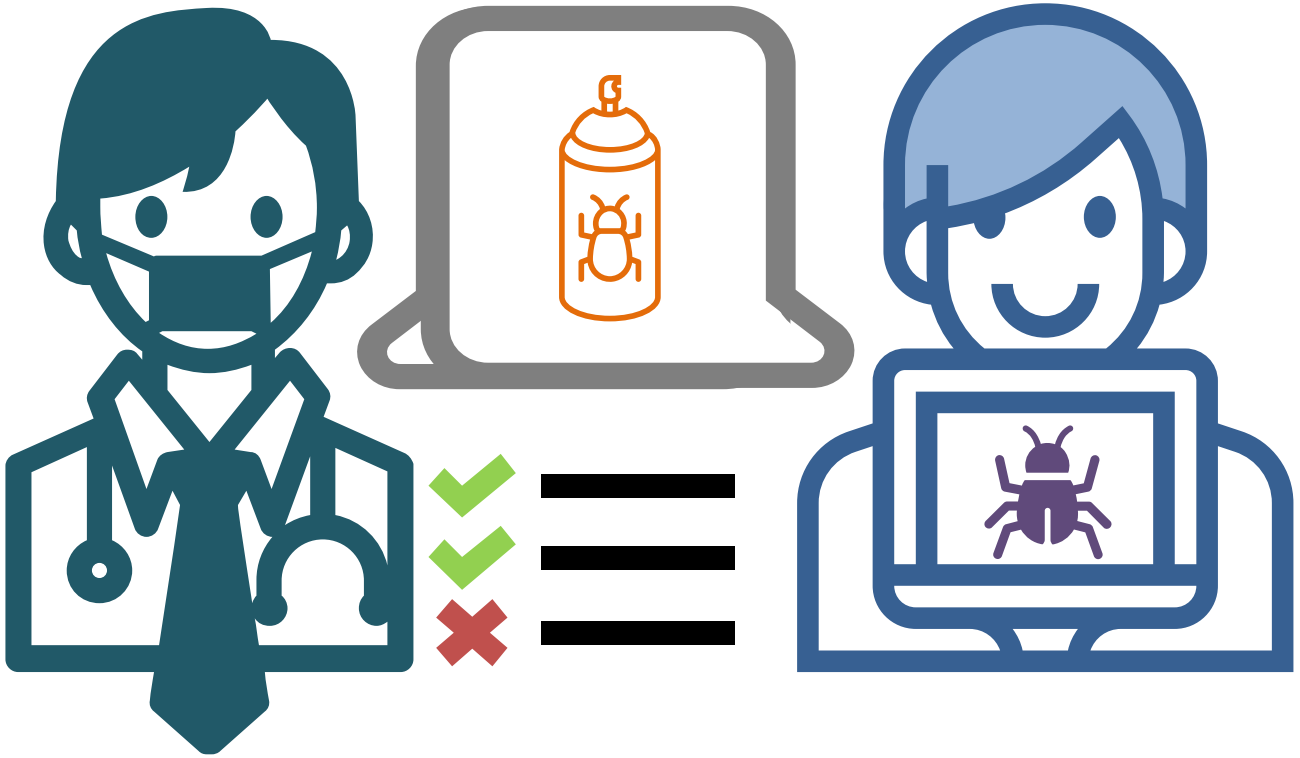
Officials said the city's firewall remained secure and they do not plan to pay a ransom.

The Michigan State Police is conducting an independent investigation of the cyberattack.

At this time, it is not believed any personal information has been breached.

Cybersecurity is Digital Public Health

- Prevent the spread of malware and threats through:
  - Developing cybersecurity policies and standards
  - Ensuring security of new and existing software and systems
  - Monitoring threats
  - Education on personal protection
  - Bulletins on emerging threats



How Can Organizations Stay Cyber Safe?

Don’t think, “It won't happen to me.” Do your part to protect yourself and others.

Be Careful What You Click
Beware of all links and attachments, particularly those from unsolicited emails or texts.

Back It Up
Use separate hardware or an online backup service to ensure a secure copy of your data is available in case of an incident

Practice Good Password Management
Never use the same password for multiple sites and implement multi-factor authentication when possible.

Install Updates on Your Devices
Keep your devices’ operating systems updated and patch vulnerabilities.

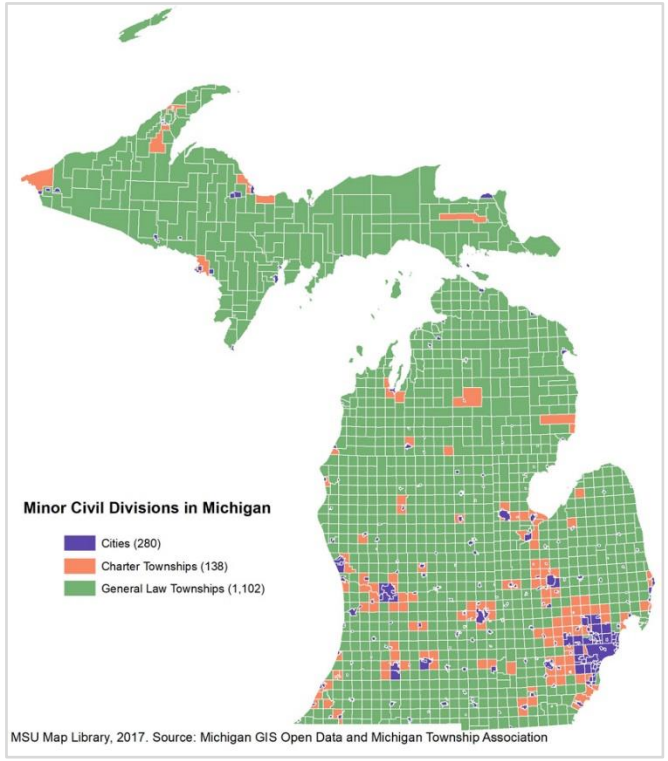
Use Mobile Devices Safely
Be wary of public wireless hot-spots and avoid storing or transmitting personal information on your device.

Stay Cautious on Social Media
Be careful what you share on social media, it can be used for phishing and social engineering.

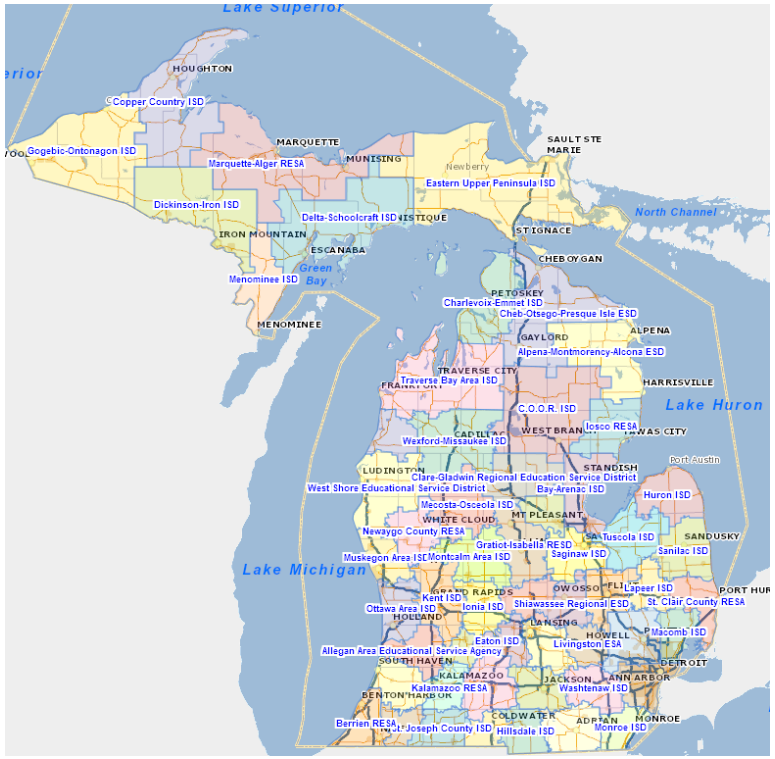
Statewide Engagement, Protection, and Response

Counties

Cities, Villages, Townships



School Districts



Cyber Partners

Prevention, Protection, & Mitigation

Cyber Readiness Service

Expert advice and support
- Assess
- Plan
- Coach

State of Michigan

Cyber Companies

Michigan Cyber Partners

- Learn
- Collaborate
- Share

State of Michigan

Local Government, Education, Authorities, Health Care

Response & Recovery

1-877-MI-CYBER
mc3@Michigan.gov

- Cyber 911

State of Michigan +MiC3

Federal Government

Cyber Companies

www.Michigan.gov/cyberpartners

MICHIGAN CYBER PARTNERS

Michigan Cyber Partners is a collaboration between various divisions at the State of Michigan, including Michigan Cyber Security and the Michigan State Police, and local public entities across Michigan to strengthen, improve, and promote cybersecurity resources and best practices.

JOIN MICHIGAN CYBER PARTNERS | MIDEAL CYBER ASSESSMENTS | REPORT A CYBER INCIDENT

CYBER PARTNERS HELPS YOU GET ORGANIZED AND CONNECTED

Prevent Cyber Attacks

Help prevent cyber attacks on local public entities in Michigan

Cyber Incident Response

Support an organized collective response to cyber incidents

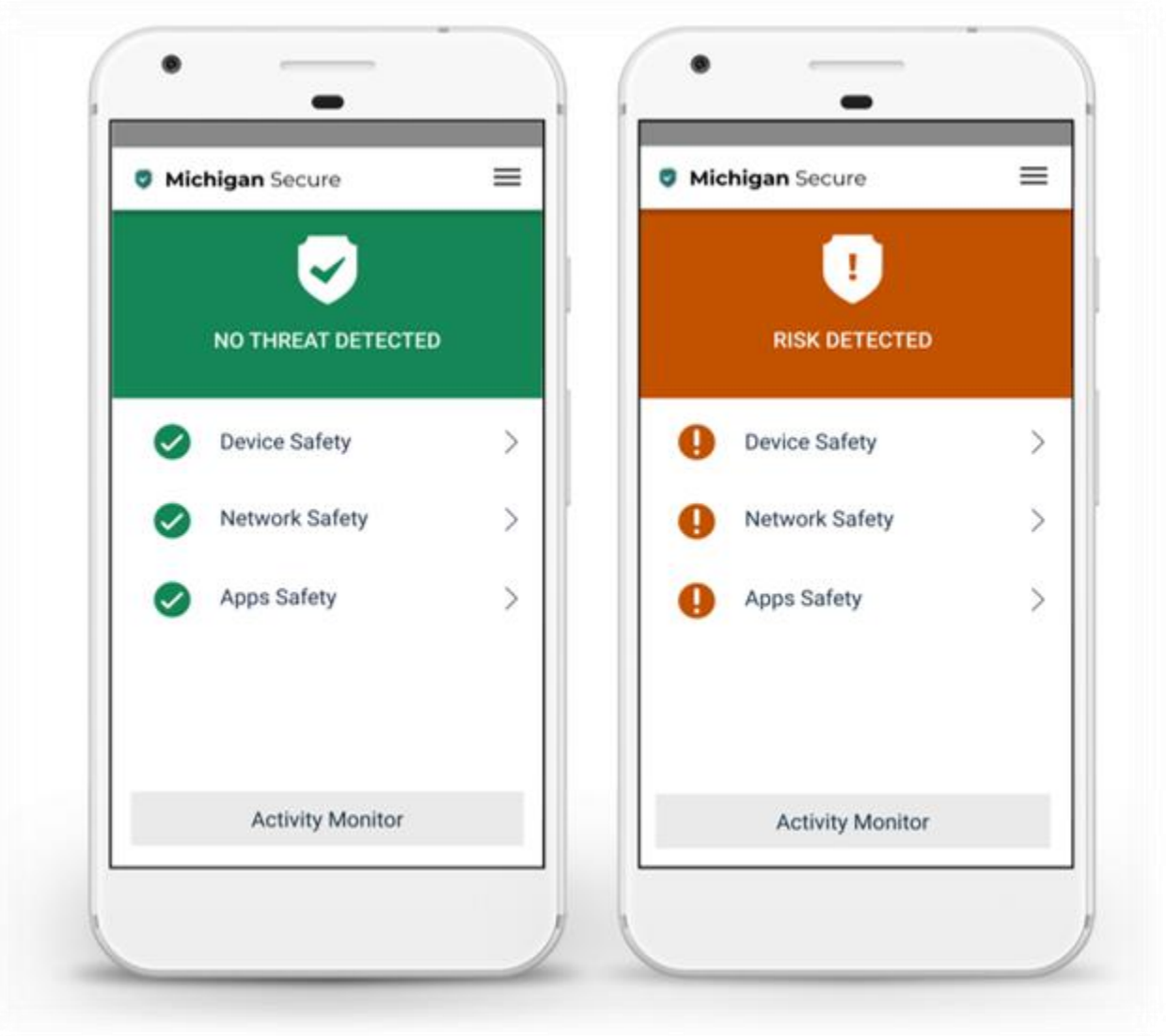
About Michigan Cyber Partners

Learn more about the program and how your organization can get involved

Michigan Cyber Civilian Corps (MiC3)

- Reserve corp. of cyber incident response professionals from across the State, available to respond to and mitigate cyber incidents.
- Able to respond to incidents and potentially imminent cybersecurity events, including hazardous vulnerabilities
- Assistance can be requested by requesting MiC3 through the Michigan State Police
- Over 80 MiC3 members from around the state.

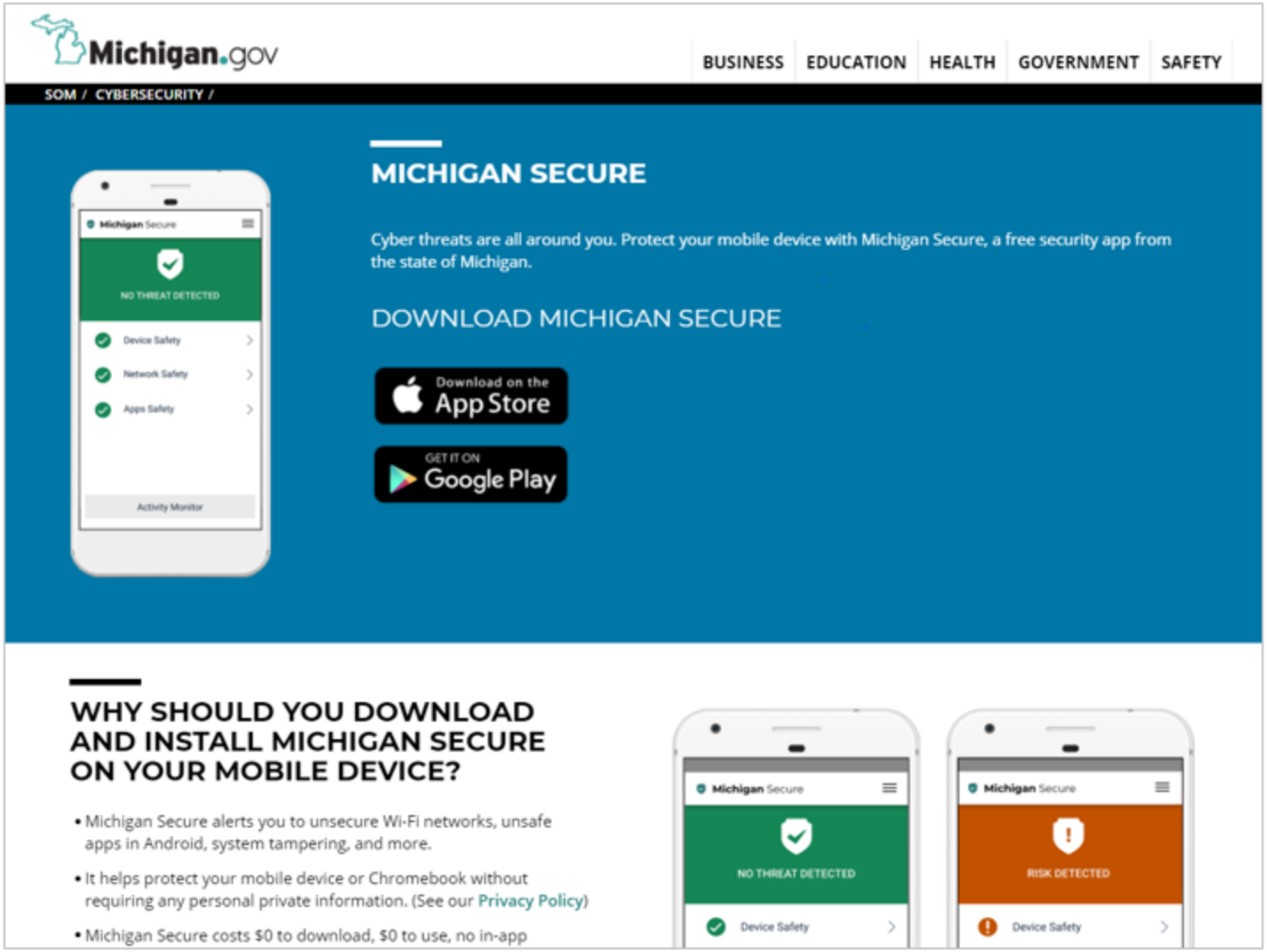
Michigan Secure Mobile Security App



A FREE mobile device protection app for Michigan residents that:

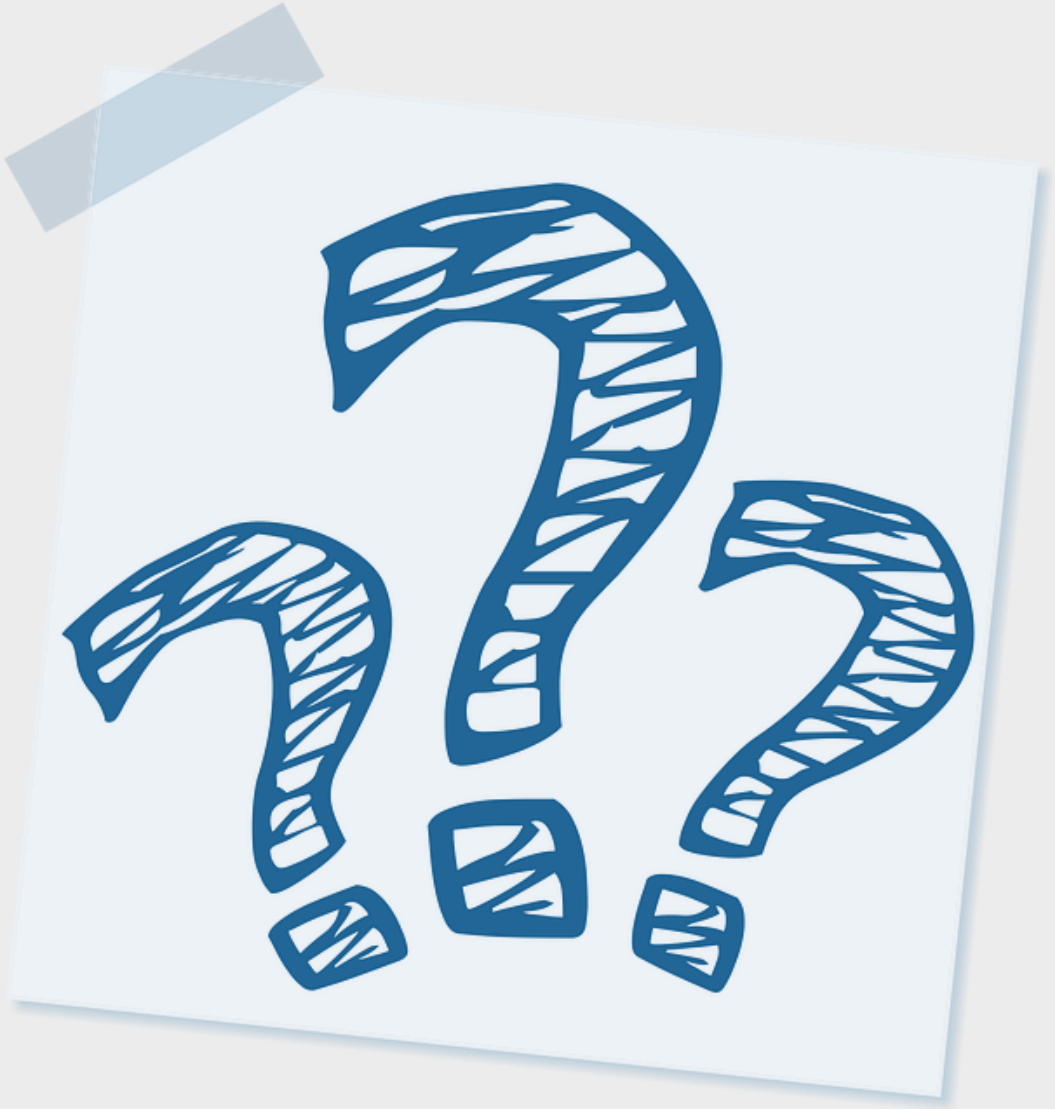
- Warns you when suspicious activity is detected on your device.
- Protects without collecting or transmitting any personal information.
- Was developed by a company specializing in mobile threat defense.

Michigan Secure Mobile Security App



Questions?

Questions



MAC
MICHIGAN ASSOCIATION OF COUNTIES

michigan municipal league

CRA™

Michigan Department of
TREASURY

MTA
MICHIGAN TOWNSHIPS ASSOCIATION