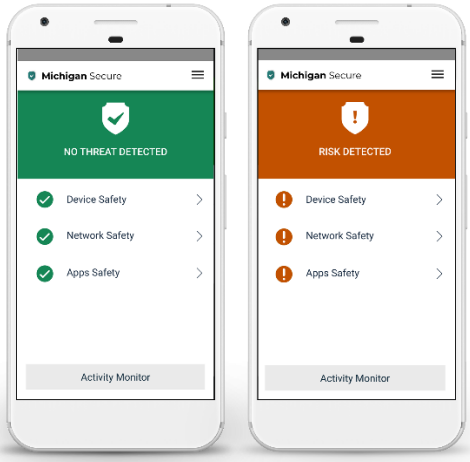
NASCIO State IT Recognition Award, Cybersecurity

Michigan Secure



Michigan Secure
State of Michigan
Department of Technology, Management, and Budget
February 2021 – Present

Contact:
Derek Larson
Acting Deputy Chief Security Officer
Chief of Staff, Cybersecurity and Infrastructure Protection
Department of Technology, Management, and Budget

DTMB | Cybersecurity & Infrastructure Protection

Introduction

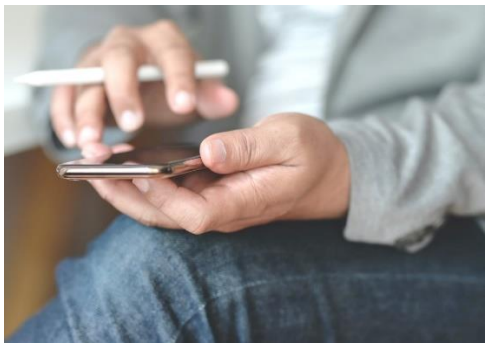
Almost every day, the news is filled with reports of malware attacks, data breaches, and ransomware campaigns targeting organizations of varying sizes and types. Whether it is hospitals, universities, government organizations, global corporations, or individual citizens, it seems no one is safe. In response to these threats, entities are investing record amounts of capital in cyber protections as the security industry seeks to stay one step ahead of ever-advancing malicious actors.

While security options for laptops and computers abound, there are fewer options for managing mobile device security. Although the number of security apps available to large entities has increased in recent years, everyday citizens have been largely left behind. This poses a threat to both residents and the State of Michigan (SOM) as the information stored on and traversing these devices is often used to engage and conduct business with the state. This makes the SOM vulnerable to significant levels of fraud, among other threats.

To combat the growing threat that mobile device insecurity poses to Michigan and its citizens, Michigan Cyber Security (MCS), a division of the Cybersecurity and Infrastructure Protection (CIP) branch of the Department of Technology, Management, and Budget (DTMB), authorized the development of a mobile security application that would identify threats on mobile devices, alert citizens of the threats in real-time, and, if the affected citizen so desired, report the threat to the State of Michigan.

Situation Analysis

As the entire digital ecosystem grapples with increasingly sophisticated cybersecurity threats, individual citizens have emerged as a major target for malicious cyber actors. While many citizens understand the need to protect their computers and laptops, the vulnerability and ubiquity of mobile devices has created a new attack vector that many people do not know how to defend against.



According to data from the Pew Research Center, 85% of Americans own smartphones and around 53% own tablets as of February 2021.[1] Further demonstrating the increased reliance on smart devices, 17% of US adults are smartphone only internet users, with lower income families with a high school diploma or less (26% of smartphone only users) and rural area adults (20% of smartphone only users) more likely to rely on a smart phone for internet access. Approximately 81% of online adults report they utilize potentially insecure public wi-fi networks,

[1] Pew Research Center: Demographics of Mobile Device Ownership and Adoption in the United States, 2021

with 32% expressing a preference for public wi-fi over cellular connections.[2] At the same time, 75% of Americans used some type of mobile banking in 2019, with studies of U.S. financial data indicating a 50 percent surge in mobile banking in the first half of 2020 as the COVID pandemic took hold.[3] In Michigan, the picture is no less concerning for its over 10 million residents:[4]

- Many are actively under attack, with 91,200 mobile devices containing known malicious applications, and approximately 56,000 devices currently compromised.
- Other threats Michigan's mobile devices are at risk from include:
    - 2,614,800 devices are currently vulnerable to freely downloadable exploits.
    - 4,600,000 devices have installed apps with a high risk of data leakage.

That attacks against mobile devices constitute a threat to state residents is clear, but an adequate response to the threat has been more difficult to determine. Governments have long addressed physical security through public safety services, like police and fire departments, as well as public health programs for sewage treatment and inoculation against infectious diseases. A growing number of government cybersecurity specialists believe that similar efforts should help citizens cope with cyberthreats.

Michiganders appreciate that they are at risk, but they currently lack the tools and understanding to better secure their digital lives. Providing the public with educational resources to reduce this risk is part of the solution, and some states have offered mobile security education programs to their residents. Nonetheless, providing an actual tool to help Michigan residents secure their digital lives creates better security results for both residents and the State.

> "We took a hacker to a café and, in **20 minutes**, he knew where everyone else was born, what schools they attended, and the last five things they googled."
>
> From a Medium.com article titled,
> **"Maybe Better If You Don't Read This Story on Public WiFi"**
> by Maurits Martijn

As the SOM examined the issue of mobile device security, a new application released in New York City came to its attention. Initially released in 2018, NYCSecure had already begun pioneering some of the mobile security technology in which Michigan was interested. After numerous meetings with the City of New York's digital operations teams, as well as meetings with cybersecurity leaders in Michigan across various levels of government and the private sector, Michigan began working with Zimperium, a U.S.-based global leader in mobile security and the developer behind NYCSecure, to build its own solution.

Michigan Secure

The result of the collaboration between the State of Michigan and Zimperium is the Michigan Secure mobile device security app. This is a low-resource demand, locally hosted app that

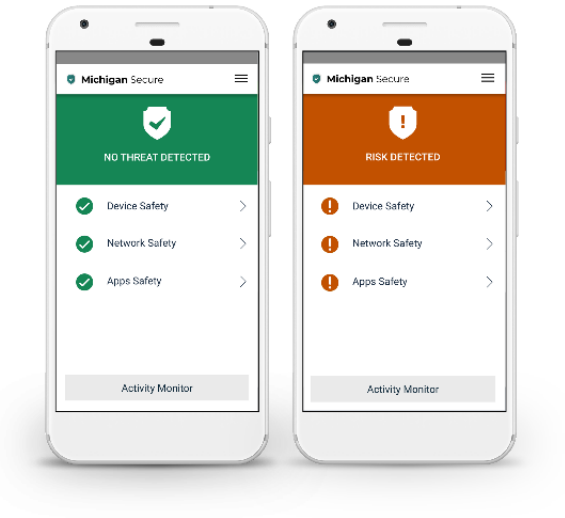
[2] One World Identity Labs, 2018
[3] Federal Bureau of Investigations: Increased Use of Mobile Banking Apps Could Lead to Exploitation, June 10, 2020
[4] Zimperium Threat Report, 2021

Michigan residents can install on their iOS and Android devices to provide security awareness and recommendations for protecting devices against identified threats.

Focusing on the biggest threat to mobile devices, Michigan Secure:

- Uses machine learning and a set of comprehensive threat patterns to:
  - Alert users to threats.
  - Offer recommendations to best address threats detected.
- Defends against rogue access points, phishing links, and malicious mobile applications.
- Protects without collecting or transmitting any personal information.

MCS understood that the app had to strike the balance between security and control. The app needed to notify users when they encountered security threats, but also enable users to accept the risk of a given action, such as connecting to a potentially risky WIFI hotspot, if they chose. MCS also knew that any government-sponsored cybersecurity tool would raise questions regarding user privacy, which was an important consideration as the suite of capabilities was determined.

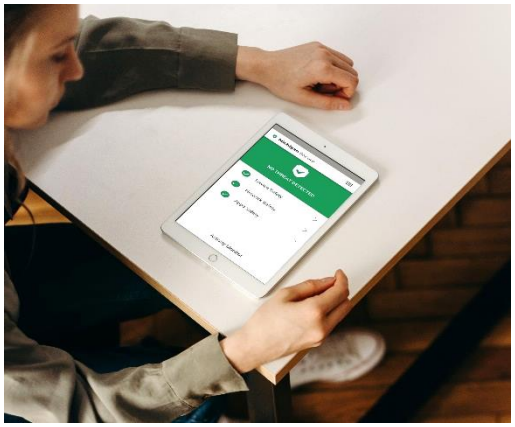


Throughout 2019 and 2020, the MCS and Zimperium teams worked collaboratively to create a product that would ensure greater security for Michiganders. The architectural and technical approach behind Michigan Secure is the perfect blend of security. Using the same core technology used by some of the most sophisticated security teams in the world, including the United States Department of Defense, Michigan Secure protects citizens against known and unknown mobile device compromises, malicious Wi-Fi networks, mobile phishing, and malicious apps. As the app offers unique on-device protection which does not require any personal information or off-device access to a cloud, Michigan Secure also protects citizen's privacy.

The digital defenses currently offered by Michigan Secure include:

- *Protecting Against Potentially Dangerous WIFI Connections*
  - A network threat is triggered when the device is connected to a rogue access point. An alert informs users there may be an issue with a Wi-Fi network they might otherwise be inclined to trust, so users can disconnect and take other precautionary actions.
  - The app monitors for and alerts in case of websites that may not be secure and could put users at risk of potential SSL stripping. For example, an attack may force users to visit webpages in HTTP instead of HTTPS. This will help an attacker to intercept the usernames and passwords in clear text. A network threat is reported if an attacker performs an SSL strip attack via a rogue or compromised access point.
- *Defense Against Phishing*

  - During installation, residents can enable “long press” actions for URLs. These actions can then send the URL to the Michigan Secure app for inspection prior to launching the website.
  - Malicious URLs are flagged, and the resident will be alerted not to follow the link.
- *Security from Malicious Apps*
  - Zimperium reports known malicious apps to the app stores for action – this is accomplished through the Enterprise product zIPS.
  - On device ML identifies malicious behaviors and alerts the resident.



While the SOM wanted to ensure strong protections for its residents, Michigan Secure also had to be designed to ensure that users’ data and personal information could not be accessed by either the application designer or the state. The local deployment and certain configuration safeguards ensure that information does not have to leave the device, in fact not even requiring an internet connection for real-time alerts. As a result, neither Zimperium nor Michigan officials can see or access any personally identifiable information (PII), including the user’s location, device serial number, phone number, text messages, pictures, emails, or any other information on your device.

Due to the privacy controls built into Michigan Secure, SOM personnel will not see anything and Zimperium can only see:

- Device ID: an anonymized, randomly generated number that can only identify how many people at any given time have downloaded Michigan Secure.
- Device Type: indicating whether the device ID is attached to an iOS or Android device.
- Version: whether the version of Michigan Secure running is the current one.

To ensure the Michigan Secure application delivered on its privacy and security goals, the source code was subjected to rigorous third-party assessment to validate that its design delivered on its promises.

Cost of Support to Michigan

An important element to the Michigan Secure proposal was that it should be free to Michigan residents downloading the application. In examining other technologies and other government voluntary enrollment programs, it was determined that, particularly early on in the release of the application, this could significantly increase adoption of the app. Increasing the digital security of Michigan residents is a component of the larger ecosystem security effort being led by DTMB, and investments in increasing use of the tool are seen as an essential part of this mission. There is also the more fundamental public service philosophy that security products developed by the State of Michigan should be available to residents regardless of their means. For now, this means DTMB is covering the costs associated with Michigan Secure's licensing and support. However, eventually the economic benefit of a more cyber secure state and the decreased risk of fraudulent activities facing the state will help to support the cost of these types of activities.

The State of Michigan invested $195,000 in the initial development of Michigan Secure and to cover its first year. A second investment of $200,000 was added as the app moved into production to cover licenses for up to 200,000 users. There was also a substantial investment of personnel resources, including security architects, project managers, and members of the CIP leadership team. Future expenditures include paid media advertising to ensure wider dissemination of the tool and, if needed, expanded license capacity.

The Impact

Much of the impact of Michigan Secure remains to be seen. However, the effort has already begun to galvanize groups in Michigan to start protecting their mobile devices. Shortly after the initial release of the application, DTMB Director and State of Michigan Chief Information Officer Brom Stibitz co-authored a letter with State Superintendent Dr. Michael Rice addressed to school administrators and technology officials calling attention to mobile device security and the threat it poses to students and their families, particularly with so many schools utilizing virtual means of engaging with students during the COVID-19 pandemic. The letter noted Michigan Secure as a trusted solution to the threat and encouraged them to reach out to their teachers, students, and parents to take preventative action.

Similar outreach and work have taken place with local government leaders. While tight budgets are a fact of life for most government units, local governments are perhaps the most squeezed for financial and human resources as it relates to IT and cybersecurity. Working through the Michigan Cyber Partners program, which shares cybersecurity-related information and best practices between local leaders and the State of Michigan, as well as other local government administrator and IT leader organizations, Michigan Secure has not only been adopted by many individuals for their personal use, but become the mobile device security solution for many of these governmental units. Often unable to afford their own solutions and unsure of how best to protect themselves, local government units have increasingly turned to Michigan Secure as a trusted name to protect the mobile devices on which they continue to rely more and more every day.

The rollout of Michigan Secure continues as the State of Michigan proceeds to engage with partners throughout the state. Even though the program is only now moving into wider distribution, the feedback from users, state and local leaders, and the technology and business communities has been overwhelmingly positive. The interconnectedness of the digital world has blurred, if not outright eliminated, the silos in which cybersecurity threats have been historically considered. As government cybersecurity units have expanded their digital defenses to better protect partners and infrastructure, Michigan Secure represents the vanguard of proactive defense of a state's citizenry.