



Michigan.gov

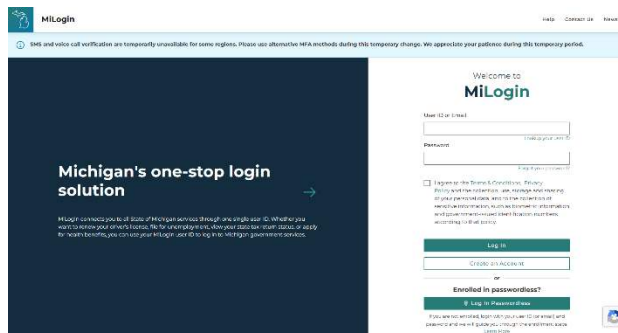
Securing Michiganders via MiLogin

Free cybersecurity awareness and training program

Award:	National Association of State Chief Information Officers (NASCIO) State IT Recognition Awards
Category:	Cybersecurity
State:	Michigan
Project Start:	September 2022
Project End:	December 2025
Contact:	Jamie Bennett Deputy Chief Security Officer State of Michigan Department of Technology, Management & Budget (DTMB) DTMB-CSO@michigan.gov

EXECUTIVE SUMMARY

Michigan's focus on whole of state cybersecurity has led to improvements in securing residents and their data. The Michigan Department of Technology, Management & Budget (DTMB) has taken multiple steps to enhance overall security modernization within its platforms while encouraging residents to strengthen their digital knowledge via the MiLogin platform.



MiLogin, Michigan's single sign on, provides access to government services with one single user ID. In 2025, MiLogin implemented identity proofing and fraud prevention to secure the enterprise identity, combat the proliferation of identity theft, and improve the user experience. To further protect residents, when signing on to MiLogin, Michiganders have access to free cybersecurity training. The training covers nine core cybersecurity topics over a series of nine videos to encourage residents to be secure in the ever-changing digital ecosystem.

IDEA

What problems or opportunities does the project address?

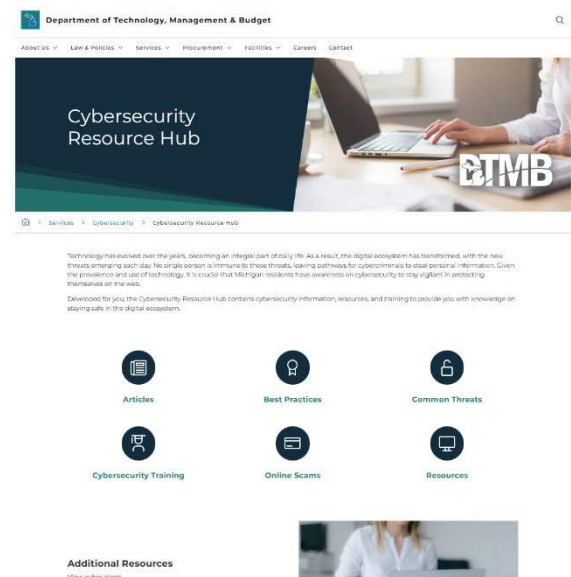
Fostering a secure digital ecosystem has long been a priority for Michigan. MiLogin has over 14 million public users accessing applications across various state agencies. This requires various security modernizations to fortify the enterprise identity single sign on platform while combating identity theft and enhancing the user experience.

Fraud prevention blocks high risk activity to protect Michiganders and their data, ensuring users are who they say they are. Identity proofing integrates an identity proofing tool with MiLogin to confirm a user's identity online by verifying user information against the Michigan Department of State's data. The identity verification process is triggered for certain scenarios, like if a user accesses State of Michigan services or if they update a previously verified name in account settings.

Cybersecurity training is free and accessible via MiLogin and aligns with the whole of state approach to government, offering residents the opportunity to strengthen their cybersecurity skills and better secure the digital ecosystem.

Why does it matter?

Implementing identity proofing and fraud prevention within MiLogin increases the public trust of Michigan's digital services, showing commitment to keeping data secure. While cases of identity theft are not new, the 2020 COVID-19 pandemic saw an exponential surge in cases, with the Federal Trade Commission (FTC) [reporting](#) a 2,920% increase in identity theft cases compared to the year before where personal information was used to apply or receive government benefits like unemployment. In 2024, the FTC received more than 1.1 million complaints of identity theft and 2.6 million complaints for fraud, resulting in a combined loss of more than \$12.5 billion.



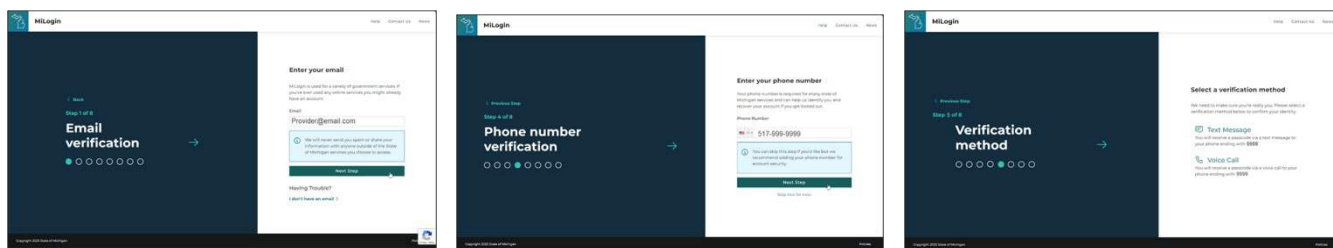
To protect residents from falling victim to identity theft and fraud, all MiLogin users have access to cybersecurity training. The training is free and designed for Michiganders of all ages, including tweens, teens, college students, those in the workforce, and senior citizens. There is an animated training series for tweens and teens, and an adult live action training for adults. The training covers nine cybersecurity topics, including popular threats, best practices, and what to do if you are hacked. Both training options include interactive elements and checkpoints to put knowledge learned to the test.



Images: (left) screenshot of youth cybersecurity course landing page, (center) main cybersecurity training page, and (right) adult cybersecurity trainings landing page.

Describe what makes the project innovative or distinct from similar initiatives.

Security modernizations are innovative, as they aim to protect residents from theft and data loss by introducing new ways of thinking. Fraud prevention shifts focus from detecting fraud to preventing it by ensuring a user is who they say they are. The simple steps implanted to verify a user still makes security easy for the user while making it hard for fraudsters. Not using a password is distinct from traditional login methods, which speeds up logging in while better securing the user.

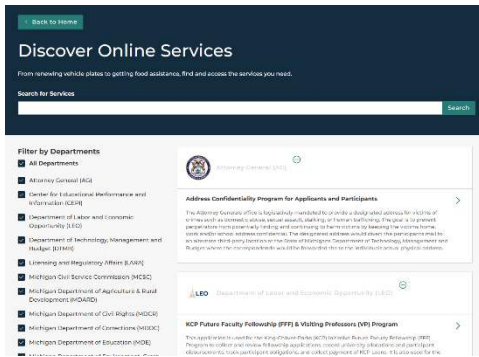


Images: (left) screenshot of MiLogin user email authentication setup, (center) screenshot of MiLogin user phone authentication setup, and (right) verification method for user account access.

Similarly, offering free cybersecurity training via MiLogin is innovative in that it is custom developed based on age demographic. Tweens and teens are offered an animated series about two cyber heroes to explain cybersecurity topics. Adults are offered a live action course that follows real-world scenarios and situations.

What makes it universal?

MiLogin is tied directly to two State CIO Top 10 Priorities: digital government/digital services and identity & access management. MiLogin provides access to hundreds of State of Michigan services, from vehicle renewal to food assistance to unemployment benefits, from a single log in portal. Because of this, it needs to provide a secure framework for digital services while being accessible. MiLogin also emphasizes the identity and access management priority, as it supports resident digital services, providing a secure single sign on log in method to authenticate users.



The cybersecurity training aligns with the State CIO Top 10 Priority of cybersecurity and risk management, as it is a training and awareness offering that follows the concept of whole of state cybersecurity. Whole of state is emphasized, as Michigan residents are directly engaged and provided with a tool to enhance their cybersecurity knowledge and awareness, strengthening Michigan's digital landscape.

Image: (left) screenshot of online services available to users after logging into MiLogin.

IMPLEMENTATION

What was the roadmap and how does this project fit into an enterprise view?

MiLogin being the single sign on for State of Michigan services requires it to be secure and updated to better serve users. MiLogin's .NEXT program began in September 2022, with the passwordless feature launching in June 2023. Passwordless was launched to improve security and user experience, as 51% of passwords are reused. Additionally, passwordless can reduce the average help desk labor cost of \$70 for a password reset.

Enterprise identity proofing began its sprint in February 2025 before it was successfully deployed in production in June 2025. The June 2025 release included the enterprise fraud analytics feature that monitors all incoming traffic to analyze a user's device and digital identity to determine if they are fraudulent, the user behavior analytics tool to monitor incoming traffic to analyze user behavior patterns like keystrokes and cursor movements to evaluate risk, and the enterprise identity proofing feature that confirms a user's identity by verifying information against the Michigan Department of State. Successful implementation includes reducing identity theft and increasing fraud protection. Implementing biometric and fraud prevention follows the security concept of zero trust, where users need to verify who they are. It acts as another layer of security to ensure a user is who they say they are, protecting critical personal data to prevent identity theft and fraud.

Cybersecurity training focuses on a whole of state approach to secure residents. It falls under DTMB's cybersecurity external engagements, which has evolved over the last seven years to include offerings for residents. The training is the latest external engagement offering designed to provide Michiganders with the knowledge they need to stay safe in the evolving digital ecosystem.

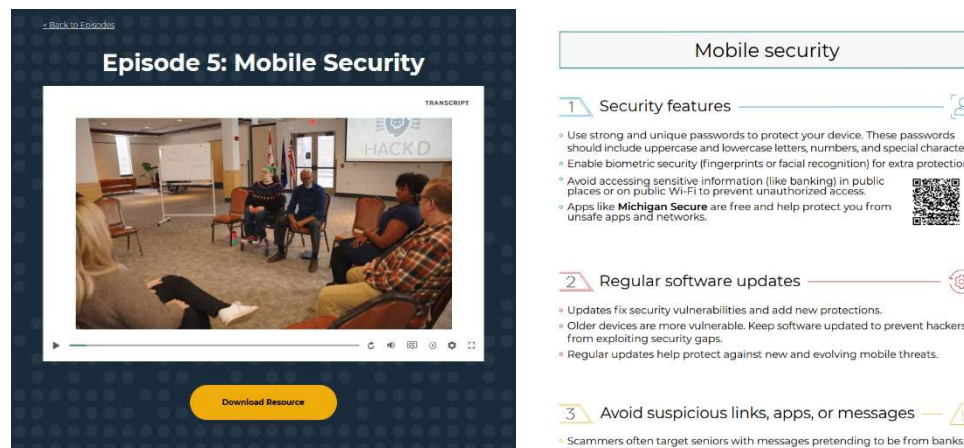


Image: (left) screenshot of the state's mobile security training video episodes and (right) screenshot of the supplemental cybersecurity training resource. These resources highlight the complexity of staying safe in a mobile and evolving digital ecosystem.

Following strategic direction to offer cybersecurity training to the residents of Michigan, a bid solicitation was sent out and implemented with DTMB IT project management methodology. Development of training materials involved reviewing scripts, descriptions, storyboards, several levels of video iterations, and interactive elements all while keeping a consistent feedback loop. Each piece had several levels of review and sign off by the State of Michigan to ensure the product met standards. Successful implementation of the training is determined by the number of users access points to the training. It also includes promotion of the training on social media and at events.

Who was involved?

The MiLogin project team worked to deliver a successful biometric and fraud proofing tool within the MiLogin platform. DTMB Agency Services partners were also involved to gain buy-in throughout the process and ensure agencies would have any questions or concerns answered. Deloitte team members supporting MiLogin were also involved in the implementation of biometric and fraud proofing to ensure rollout plans and communication materials were clear when distributed to agency partners. The MiLogin team also completed a case study for the industry group responsible for passkeys, FIDO Alliance, and was featured on the FIDO Alliance site. In October 2024, MiLogin was also celebrated for being the largest government implementation of passkeys in the world.



There was a cross functional team involved in the development of the training, which included DTMB’s cybersecurity external engagements, staff from business operations, the MiLogin team, DTMB communications team, input from DTMB’s diversity, equity, and inclusion officer, and staff running security awareness training for State of Michigan staff. Approval and buy-in were obtained, as the training aligned to Cybersecurity and Infrastructure Protection’s Four-Year Strategic Plan, which emphasizes the need to “make security easier for customers and harder for hackers.” The training was also promoted on DTMB social media and highlighted at the 2025 Michigan Cyber Summit.



Images: screenshots of DTMB social media posts promoting the State of Michigan’s cybersecurity trainings and the DTMB Cybersecurity Resource Hub.

How did you do it?

MiLogin’s .NEXT program began in September 2022, with the latest fraud prevention feature launching in summer 2025. These launched in various sprints, followed by QA, user acceptance testing, and certification testing before moving to production deployment. The MiLogin team worked closely with the DTMB Agency Services team throughout these launches to ensure agencies would not be adversely impacted by the new features. MiLogin’s passwordless enrollment cost \$400,000 and the enterprise identity proofing, enterprise fraud

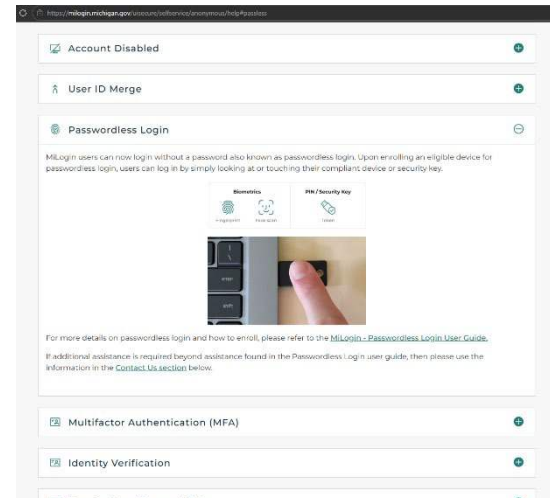
analytics, and user behavior analytics cost \$1.4 million. Both investments work to improve user experience and protect data while mitigating risks related to fake or stolen identities, enhance fraud protection, and improve identity verification to access State of Michigan services.

The cybersecurity training was implemented by selecting a vendor, MindSpring, to assist in development of the training and materials. The project began in October 2024 and officially launched in December 2025. A testing period was launched for stakeholders within State of Michigan government to test the training for functionality and content. The training is cloud-based, allowing for easy access, instant updates, and better management of the training platform. This also allowed it to be integrated with the MiLogin platform, making it easily accessible to Michigan residents.

IMPACT

What did the project make better?

Securing residents via MiLogin has improved overall security. Prior to fraud prevention, there was not a set identity verification in place across MiLogin's applications. The implementation of identity proofing and fraud prevention by thoroughly checking identity secures residents and protects personal data from being stolen. This empowers residents and gives them confidence in knowing the State of Michigan keeps resident data secure. Passwordless login is beneficial to users, as they don't need to remember a traditional password. Passwordless also reduces help desk calls related to password resets, saving a significant amount of time and money.



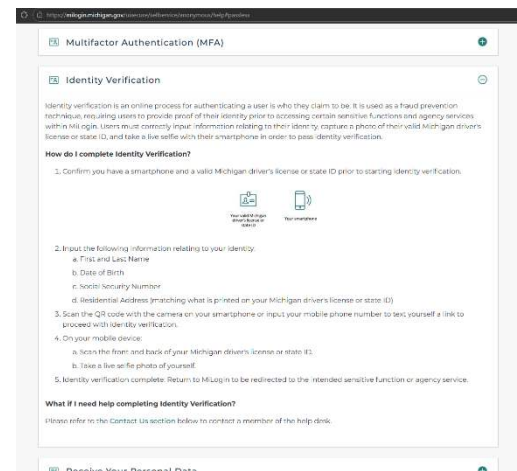
Customers are also more satisfied, as there are more security measures in place to prevent fraud and protect against identity theft. These enhancements mitigate risks related to fake or stolen identities, enhance fraud prevention capabilities, and streamline the identification of compromised accounts. They also allow MiLogin to review user behavior and transactions to seamlessly intercept and block suspicious activity.

Identity verification also improves user security and data, as while it adds some steps that need to be taken, they protect users to ensure only they are accessing their account. turn, this increases trust in the use of State of Michigan digital services, as Michiganders know there are security measures in place to protect their data.

Securing residents goes beyond the behind-the-scenes work of protecting data and systems. It also means empowering residents with tools and training to keep themselves secure. The training is free to all Michigan residents and covers several important topics, from basic concepts like simple best practices to more sophisticated topics like social engineering. Cybersecurity can be a complex topic, and the training provides key information in a simple, digestible, and easy to understand format for all ages. Cybersecurity training drives security awareness, instills best practices, and improves overall cyber hygiene across Michigan. It also provides a security training tool for local government entities across the state that cannot afford a security awareness program as a no cost option.

How do you know?

MiLogin identity proofing and fraud analytics has blocked high risk activity at a large scale. This includes more than 221,000 cloud hosted proxy risk signals and other major fraud indicators. Identity verification remains strong, with an 83.5% acceptance rate, a 15.2% rejection rate, and a 1.4% resubmission rate. Biometric passkey authentication, which is compatible with all make smart device providers and browser solutions, has over half a million enrollments on the public MiLogin portal. In 2024, MiLogin was recognized by the FIDO Alliance for their implementation of passkeys, as at that time, MiLogin was the largest government implementation of passkeys in the world.



Securing the cybersecurity landscape goes beyond the organization, extending to residents. Over 10 million Michiganders have access to cybersecurity training, with more than 2,400 active monthly endpoints taking the training. It is one of the primary applications users see when they access MiLogin, providing easy access to the free training.

What now?

MiLogin is moving toward future projects to further secure the platform. A usability study will be completed across its portals to help define further enhancements and improvements. Findings from the study will result in public portal self service upgrades to improve user experience and encourage further enrollment into passwordless authentication. MiLogin will also decommission on premise systems and continue migrations to the cloud for several appliances and the automated application onboarding app to improve overall platform scalability and reduce infrastructure costs. Additionally, MiLogin will ensure compliance with the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 to address session timeout alignment, support password intelligence, and enhance threat intelligence. Future enhancements to MiLogin will continue modernization and security innovations under the umbrella of the MiLogin .NEXT program

The free cybersecurity training will continue to be promoted on social media and at speaking engagements. As it is directly on the home screen of options when users log in to MiLogin, they don't need to search for it and request access and instead can take the training right when they log in. It is worthy of its initial investment because it keeps residents secure and teaches best practices. Providing Michiganders with tools and knowledge to stay secure helps keep the entire state secure, strengthening Michigan's digital ecosystem. More information is available at Michigan.gov/Cybersecurity.

