

FRAUD PREVENTION FRIDAY



Friday, October 16, 2026



Cybersecurity Awareness Month: DIFS Shares Tips to Help Michiganders Avoid Online Scams

Source: DIFS

October is Cybersecurity Awareness Month, and the Michigan Department of Insurance and Financial Services (DIFS) is sharing steps Michiganders can take to protect themselves from falling victim to scammers and cyberattacks.

"Cybersecurity Awareness Month serves as an important reminder for Michiganders to take necessary precautions to safeguard their information and money from constantly evolving cyberattacks and online scams," said DIFS Director Anita Fox. "As scams become more sophisticated, the most important step is simple but offers the most protection: never give out any personal information."

Here are some steps consumers can implement to protect their personal and financial information:

- NEVER provide any information to anyone calling, writing, emailing, texting, or messaging you on social media, even if caller ID or an email looks legitimate or the person contacting you says it's for "verification purposes."

(Click the heading link to read more.)

Top News

- [Cybersecurity Awareness Month: DIFS Shares Tips to Help Michiganders Avoid Online Scams](#)
- [Staying Ahead of Emerging Cybersecurity Risks in the Age of AI](#)
- [Securing Against AI Related Threats: Access Control and Privileged Access Management](#)
- [FinCEN Alert on Money Laundering Activity Associated with Digital Investment Scam Centers](#)
- [Cyber-Crime Prevention Strategy for Every Age Group](#)



Staying Ahead of Emerging Cybersecurity Risks in the Age of AI

Source: SHAZAM

Artificial intelligence is changing the way financial institutions operate, creating opportunities to improve efficiency, enhance customer experiences, and streamline decision-making. However, the same technology is also reshaping the threat landscape. As cybercriminals adopt AI-powered tools, financial institutions must prepare for attacks that are more sophisticated, personalized, and difficult to detect.

AI-powered social engineering is raising the stakes

Phishing remains one of the most common cyberattack methods, and artificial intelligence is making these attacks more convincing.

Modern phishing campaigns can use AI to create highly personalized messages that mimic legitimate communications from coworkers, vendors, or trusted institutions. Deepfake technology adds another layer of risk, enabling attackers to generate realistic audio and video content that can be used to impersonate executives, employees, or business partners.

At the same time, threat actors are increasingly automating reconnaissance efforts, collecting publicly available information about executives and privileged users before launching targeted social engineering attacks.

As these tactics evolve, organizations can no longer rely solely on traditional awareness training. Financial institutions need ongoing security education, testing, and validation to help employees recognize suspicious activity and respond appropriately.

(Click the heading link to read more.)



Securing Against AI Related Threats: Access Control and Privileged Access Management

Source: Office of Cybersecurity and Critical Infrastructure Protection

AI is increasing adversaries' ability to identify vulnerabilities, chain exploits, and escalate privileges, making strong access control and privileged access management (PAM) essential components of cyber defense. Robust identity-centric security limits unauthorized access to sensitive systems even when attackers leverage AI to accelerate exploitation and bypass traditional authentication mechanisms. Organizations should adopt a Zero Trust approach by implementing phishing-resistant multi-factor authentication, continuous identity validation, centralized identity management, just-in-time and least-privilege access, AI-enabled behavioral analytics, and automated identity governance. Together, these measures strengthen resilience against AI-enabled cyber threats while improving visibility, reducing unnecessary privileges, and ensuring only authorized users maintain access to critical resources.

As adversaries continue to leverage AI to enhance their capabilities for exploiting vulnerabilities and moving laterally through networks, access control and privileged access management (PAM) become vital to securing networks. Often, adversaries leverage misconfigured or missing access controls and PAM to expand their reach within a network and to access sensitive resources and areas. Even when malicious actors leverage AI to enhance their attack capabilities, strong access control practices can help minimize their success. Ensuring that access to resources is limited to those who are authorized to access them through proper authentication can help mitigate impacts from adversary attacks, especially those that leverage AI to not only identify vulnerabilities, but to also exploit them and bypass authentication systems.

(Click the heading link to read more.)



FinCEN Alert on Money Laundering Activity Associated with Digital Investment Scam Centers

Source: FinCEN

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Alert to urge financial institutions to be vigilant in detecting, identifying, and reporting suspicious activity connected to the operation of digital asset investment scam centers and the laundering of associated illicit proceeds. Transnational criminal organizations (TCOs), predominantly in Southeast Asia, operate these scam centers, which target individuals, including numerous Americans, with digital asset investment scams and other fraud schemes. A vast illicit ecosystem, which includes online marketplaces for cybercrime and money laundering-related services and artificial intelligence supported software platforms, enables scam centers' operations.

Fraud continues to be one of the largest sources of illicit proceeds in the United States, according to Treasury's 2026 National Money Laundering Risk Assessment. Fraud and cybercrime are two of FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities. On March 6, 2026, President Trump issued Executive Order 14390, Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens, declaring that it is the policy of the United States to protect Americans from, and harden our financial and digital systems against, these threats.

This Alert builds on ongoing efforts by Treasury, the Department of Justice's (DOJ) interagency Scam Center Strike Force, law enforcement, and other interagency partners to combat the threat of TCO-operated scam centers. This Alert supplements FinCEN's September 2023 Alert that provided behavioral, financial, and technical red flags associated with digital asset investment scams.

(Click the heading link to read more.)



Cyber-Crime Prevention Strategy for Every Age Group

Source: PCBB BID Daily Newsletter

It's clear that scammers are going after every population they can with an ever-evolving array of tactics. In general, they try different scams on different age groups. Effective detection and prevention can depend on connections with their customers, making CFIs and their strong customer relationships excellent partners in protection. A bank employee who notices a client suddenly beginning to send large wire transfers could save someone from a romance scam, for instance. Below are the four different age groups and tips to help protect them from fraud.

Baby Boomers: Trust and Connection

Boomers might get robo-calls, romance scams, email phishing, and sweepstakes scams. They're particularly vulnerable to scams that manipulate personal connections, whether it's a fake romance or an imitation of a grandchild needing bail money. People age 70 and older tend to lose more money per theft when they fall for scams, probably because their greater ages have given them time to amass savings. Boomers are most likely to remember positive, connection-oriented messages about stopping fraud, such as a reminder that they don't have to handle tech problems alone and can always reach out to their CFI. Traditional communication methods, such as in-branch material, personal conversations, and mailed information, work for this group. Older Americans are more likely than younger adults to open physical mail.

Gen X: The Generational Sandwich Filling

Gen X bank customers are often the people in the middle of three generations, guiding their children while protecting their parents. They are therefore interested in how CFIs can help keep entire families away from scammers.

(Click the heading link to read more.)