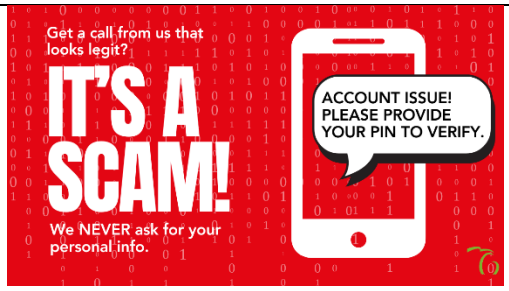
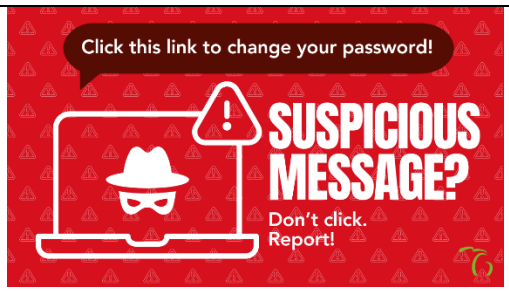
Spoofing: Toolkit

Social Media Toolkit

The Michigan Department of Insurance and Financial Services has created social media graphics and messaging to help stakeholders get the message out about spoofing. Please feel free to use or customize any of these as appropriate for your social media channels.

To download the graphics for posting, click on the Image Files folder or right-click the image, click "Save As Picture," and save the image to your computer.

Text for post	Image Preview
Got a call, text, or email from us saying there's a problem with your account? It may look legitimate, but it could be a scam! We will NEVER ask for personal or account information. #Spoofing (182char)	 *alt text: Phone with alert that reads, "Account issue! Please provide your pin to verify." Message reads, "Get a call from us that looks legit? It's a scam. We never ask for your personal info.
NEVER share sensitive information like PINs, passwords, or one-time codes over the phone, email, or text. If you receive an unsolicited call or message from your financial institution asking for sensitive information, NEVER provide it. Hang up. #Spoofing (256char)	 *alt text: Scared woman on phone with message that says, "Beware of phone scams: Caller ID can be spoofed."
If you get a call, text, or email from us about your account and are unsure if it's real or a scam, call the phone number on the back of your account statement or debit card to be sure you're safe! #Spoofing (225char)	 *alt text: Skull and cross bones in email with message that reads, "Phishy email? Don't get spoofed. Report it!"

You may have **NO FRAUD PROTECTION** or any way to recover lost funds if you give out personal or account information to scammers! Never share sensitive information like PINs, passwords, or one-time codes over the phone, email, or text. #Spoofing (241char)	 *alt text: Suspicious alert with message that reads, "Suspicious message? Don't click, report it."

Sample Newsletter Articles
The articles below are to help you communicate with your accountholders. Please feel free to use or modify as appropriate for your audiences.

Article #1:

Stay Safe, Protect Your Account, Avoid Scammers!

Rule Number One: We will NEVER call, text, or email you asking for your password or other personal information.

Scammers will do almost anything to get your money and your personal information.

Scammers can make calls, texts, and emails appear to come from us! If you receive suspicious outreach, for example, if someone calls claiming to be us stating there are issues with your account, **STOP and PAUSE.**

Scammers will try to create a sense of urgency, even claiming your account requires immediate action.

If you find yourself in this situation, **STOP**, hang up and call the phone number on your account statement or the back of your debit card – do not reply to an email or use a number given to you.

Worse yet, if you do give out personal or account information to a scammer, you may have **no fraud protection or other way to recover lost funds**! Be safe, protect your account, stay alert, and never give out your information -- hang up when in doubt.

Article #2:

Spoofing Victim? You may be out of luck.

Scammers constantly update their methods to steal personal information and your money, and to infect your devices with malware. Spoofing involves scammers faking caller id or an email and pretend to be a legitimate source, business, colleague, or other trusted contact, such as an employee of your financial institution.

If you give out account or personal information, you may have **no fraud protection or other way to recover lost funds,** but there are steps you can take to protect your personal information and data from future attacks.

- **Act quickly to protect your accounts.**
    - Contact the financial institution involved immediately at the number on your statement or the back of your debt card.
    - Ask about their policies regarding consumers who lose money due to scams. If you are a victim, you may not be able to get the money you lost back.
    - Change your passwords immediately if an online account was compromised.
    - Use strong, unique passwords for each account, and multifactor authentication whenever available.

- **Secure devices.**
    - If you need help figuring out technology, don't hesitate to ask a trusted friend or family member for help!
    - Consider uninstalling any unknown or suspicious apps you do not recognize.
    - Ensure your device operating system, software, and antivirus programs are up to date to protect against further attacks.

- **Spread awareness.**
    - Alert friends, family, and colleagues about the scam so they can avoid falling into the same trap. Share details on social media or consumer forums if comfortable.
    - Consumers can report the scam to consumer advocacy organizations to help raise awareness and possibly get advice on further actions.

Even after taking these actions, monitor your accounts and personal data for anything suspicious. Staying informed on new or updated scams helps you to recognize the warning signs and protects you in the future, so share the information with family and friends!

Possible Email to FIs with Best Practices:

Good morning/afternoon,

Scams are becoming increasingly common, and "spoofing" has emerged as a specific tactic that scammers are using to gain access to consumers accounts and personal information. To make sure Michiganders are aware of scams and are protecting themselves, the Department of Insurance and Financial Services is providing its tips to help inform and educate consumers on spoofing and how to recognize the signs of these scams.

- Explain spoofing as a method where scammers disguise themselves as legit sources, often using fake caller IDs, emails, or SMS messages that appear to be from the financial institution.
- Provide accountholders with information about what spoofing is and how it works.
- Highlight how spoofing can be used to acquire sensitive information like login credentials and account numbers.
- Institute multifactor authentication.

- Make it clear that your financial institution will **never** request passwords, PINs, Social Security numbers, or account details over the phone, or by text or email.
- Let accountholders know that your financial institution will not ask them to click on links or provide sensitive details via unsecured channels.
- Share red flags to watch out for, including:
    - Urgent language or threats (ex. “Your account will be locked”).
    - Requests for sensitive information, especially under pressure.
    - Odd-looking URLs or email addresses with slight misspellings.
    - Poor grammar or unusual formatting in emails or texts.
- Advise accountholders to verify suspicious calls, texts, or emails by contacting your financial institution directly using known contact information, such as the number on the back of their debit card or your official website.
- Provide clear instructions for reporting suspected spoofing attempts, including a dedicated email address or phone number where customers can report fraudulent messages and calls.
- Warn consumers that if they voluntarily give out their information – even to a scammer posing as your financial institution – they may not have fraud protection or any way to recover lost funds.

With these tips, your institution can provide additional security and peace of mind to your accountholders while helping them protect their personal information and finances. We encourage you to use this toolkit's content to educate your accountholders on how to recognize and avoid these scams.