FRAUD PREVENTION FRIDAY

Friday, June 14, 2024

Top News

DIFS Warns Consumers to Beware Scam Calls Impersonating Banks

The Michigan Department of Insurance and Financial Services (DIFS) is warning consumers about the rising frequency of scams where victims receive spoofed calls or texts from criminals posing as bank or credit union representatives in an attempt to access customer accounts and steal customers' money and information. In a spoofed call, the caller ID will make it look like the call is coming from the credit union or bank even though it is a scam.

"Spoofed call scams are becoming more sophisticated, and once they have you on the line, the caller will try to use fear and false urgency to pressure you to act immediately, putting you at risk of losing substantial amounts of money and disclosing your personal information," said DIFS Director Anita Fox. "Remember that your financial institution will never reach out to you requesting your password or other personal information to access your account. When in doubt, hang up with the caller and check with your bank or credit union directly using the phone number from your statement or card."

Your Smart Devices May Be an Invitation to Hackers

While you spend your time and energy guarding your community financial institution's (CFI's) central systems and technology against direct attacks by hackers, a back door into your systems may be vulnerable in ways you never imagined. Any device with an internet connection is potentially hackable. With the proliferation of smart devices, these back doors are multiplying.

The spread of smart devices has resulted in a host of new vulnerabilities. Often called the Internet of Things (IoT), these modern conveniences have been recognized as potential security problems. But those worries are often overlooked or downplayed. It's hard to imagine a fish tank as a security threat. There are actually quite a few seemingly harmless smart devices that pose a risk to your CFI if you haven't taken steps to secure them.

One of the top IoT device concerns at the moment is the office printer. Modern printers are far more advanced than earlier versions, offering myriad ways to print, scan, and copy, among other tasks. These multi-function printers are also typically connected to the internet, which can be a source of trouble: 61% of organizations dealt with data loss through their printers in 2023.

Impersonation Scams

Have you set up fraud alerts with fraud.org? Fraud.org is a project of the National Consumers League, a nonprofit advocacy organization based in Washington, D.C. Its mission is to promote the interests of consumers and workers in the US and abroad. Below is a recent fraud trend we should all be aware of and pass along to your account holders.

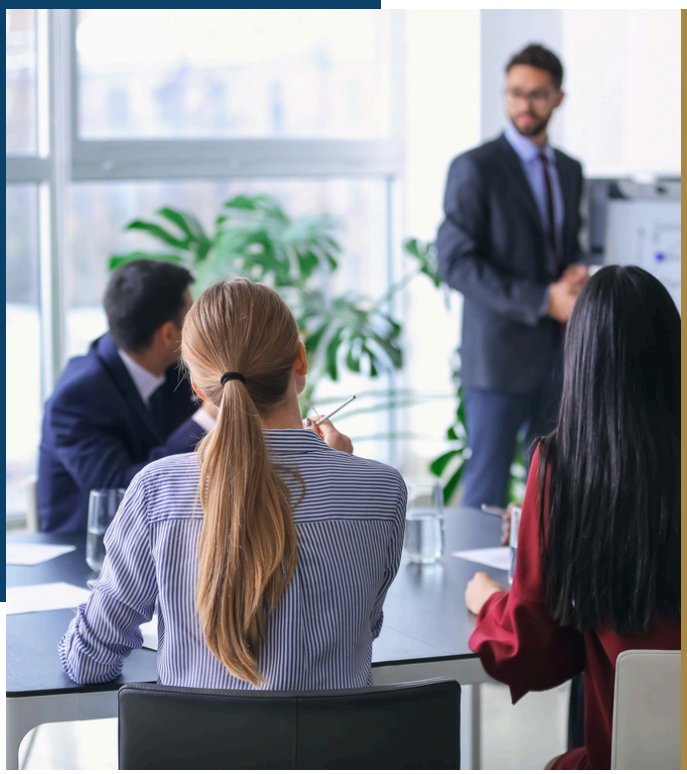
A number of government agencies have been warning consumers about a sharp rise in phishing attacks centered around fake toll charges. The FBI alone received over 2,000 complaints related to the surge in fake toll scams within a one-month period. Many state attorneys general and toll authorities have received similar spikes in reports as well.

The fraud hinges on impersonation, with the scammers posing as toll collectors and sending text messages claiming that the recipient owes money for unpaid tolls. Reported messages have said that the individual owes around $12 but can be hit with a $50 late fee. The texts then include a web link taking the target to what appears to be an authentic site for paying tolls.

Like other phishing attempts, this scam aims to deceive recipients into providing personal information to the fraudsters. Criminals can then use this data to commit identity theft and gain access to the individual's online accounts. Additionally, if the target responds to the phishing attempt, this signals the recipient's phone number is live, which can result in a greater number of scams targeted to that (now verified) number.

Keep the following tips in mind to protect yourself from these phishing attacks:

- Do not respond to the message or click on any links. Clicking on web links or attachments can make your device vulnerable to malware and jeopardize your personal data; in addition to signaling to scammers, there is a live target associated with the receiving phone number or email.
- Check your local toll operator's website. Impersonated authorities will often put a warning on their site with resources and methods to help consumers distinguish legitimate agencies from scammers. If you do owe a toll, this is where you would make a payment.
- Look for mistakes in the message. Some states, like Michigan, have toll bridges and tunnels but not toll roads. Scammers may also spell the names of toll collection agencies incorrectly. Inconsistencies like these are red flags that the message is not authentic.
- Report the message to law enforcement. The FBI, the FTC, and state attorneys general rely on reports of fraud to track trends, pursue the criminals, and compensate victims when possible.
- Report the message as junk to your phone carrier. This can be done with your phone's built-in "report junk" button. This allows your phone carrier to better detect and block fraudulent messages on its network. Using the built-in "report junk" button often deletes the message from your phone, so this should be done last.



Do Not Miss The CBM Risk Fraud Forum - 7.25.24

Take advantage of this forum and the opportunity to exchange ideas and build relationships with other risk and fraud management professionals across the Michigan community banking footprint. Attendees and subject matter experts will address the current fraud and technological issues affecting the financial industry, banking departments, and the supervisory process. Forum members will hear the latest cyber threats and technological advances available in the financial industry.

Steve Cree from ECCHO will be talking about Utilizing Warranties, Indemnities, and Exchange Rules to Reduce Losses. We will also have experts from the Michigan State Police and the FBI with us to provide updates on what they are seeing with fraud and how to stay vigilant.

What are some classic warning signs of possible fraud and scams?

Find ways to get these valuable tips to your accountholders to help educate them on fraud prevention.

Several signs indicate you might be dealing with a scammer, and you can take steps to protect yourself and others.

Criminals and con artists use many scams to target unsuspecting people—of all ages—who have access to money. Consumer scams happen on the phone, through the mail, e-mail, or over the internet. They can occur in person, at home, or at a business.

Warning signs include contact from someone:

- Claiming to be from the government, a bank, a business, or a family member, and asking you to pay money.
- Asking you to pay money or taxes upfront to receive a prize or a gift.
- Asking you to wire them money, send cryptocurrency, send money by courier, send money over a payment app, or put money on a prepaid card or gift card and send it to them or give them the numbers on the card.
- Asking for access to your money-such as your ATM cards, bank accounts, credit cards, cryptocurrency wallet keys or access codes, or investment accounts.
- Pressuring you to "act now" or else the deal will go away or trying hard to give you a "great deal" without time to answer your questions.
- Creating a sense of urgency or emergency to play on your emotions.

Here are some tips to protect yourself from scams:

- **Don't share numbers or passwords for accounts, credit cards, or Social Security.**
- **Never pay upfront for a promised prize.** It's a scam if you are told that you must pay fees or taxes to receive a prize or other financial windfall.
- **After hearing a sales pitch, take time to compare prices.** Ask for information in writing and read it carefully.
- **Too good to be true?** Ask yourself why someone is trying so hard to give you a "great deal." If it sounds too good to be true, it probably is.
- **Watch out for deals that are only "good today" and that pressure you to act quickly.** Walk away from high-pressure sales tactics that don't allow you time to read a contract or get legal advice before signing. Also, don't fall for the sales pitch that says you need to pay immediately, for example, by wiring the money, sending it by courier or over a payment app, or by sending cryptocurrency.
- **Beware when someone plays on your emotions or claims there's an urgent situation.** Advances in artificial intelligence make it easier for scammers to clone voices and alter images to make it seem like someone you know needs help. Contact the person yourself to verify the story. Use contact information you know is theirs. If you can't reach them, try to get in touch with them through another trusted person, like a family member or their friends.
- **Don't click on links or scan QR codes.** These can take you to scammers' malicious websites or give them access to your device.
- **Put your number on the National Do Not Call Registry.** Go to www.donotcall.gov or call (888) 382-1222.