

SIMPLYPUT

Retirement Savings Education, Simplified

Third Quarter 2021

10 Tips to Keep Your Finances Safe from Cybercriminals

Not to scare you, but your bank account, credit card, and even your retirement savings account may be at risk. Fraudsters are targeting retirement savings accounts more often due to account balances being higher than most checking or everyday savings accounts.

To protect your assets, you need to be diligent, educate yourself on how your information may be leaked, and take proactive measures to guard your data. Please review these 10 tips on how you can keep your financial assets safe, in addition to the steps that MO Deferred Comp is taking to protect your money.

1 Be aware of imposter websites.

This sounds easy, but cybercriminals make it extremely difficult to tell which websites are legit and which are phony. Check the spelling of each website URL, review the Privacy Policy, confirm the contact information is correct, and call the business when in doubt to ensure you are using the right website.

2 Before downloading that app...

Alongside websites, apps are another way hackers are targeting individuals. When downloading apps, stick to trusted app stores like Google Play™ or the App Store™ and read the reviews to ensure others have not mentioned any identity theft or leakage via the application. Malicious apps can be full of malware that can easily steal your personal information, account data, passwords, and more.

3 Don't go phishing.

If you do not know the sender, or even if you do, be wary of the links you click within emails, texts, social media messages, and so on. Phishing attempts are an easy way for hackers to gain access to your personal information. Identifying a phishing attempt can be tricky. Look for incorrect spelling or grammar, wrong numbers, misinformation, or a message that is out of character of the sender.

4 Beef up your passwords!

This tip should come as no surprise. You need to use complex passwords! Make sure your passwords are unique and use a variety of letters, numbers, and symbols. Experts recommend to avoid using your birthday, social security number, last name, children and pet names, and address.

5 Some things are better at home.

You may want to think again before using free WiFi or logging into your retirement or banking account from a public place. Public networks put you at risk for digital snooping and man-in-the-middle cyberattacks.



NEW NAME, SAME RECORDKEEPER

In June 2021, MO Deferred Comp's recordkeeper changed its name from ICMA-RC to MissionSquare Retirement. Rest assured this will not affect your retirement savings and there is nothing you need to do. If you have questions, do not hesitate to contact the deferred comp plan.

A CYBERATTACK IS ATTEMPTED EVERY 39 SECONDS!*

6 Set up your online account.

One of the easiest ways to monitor and protect your money is to set up an online account. It's much easier for a cybercriminal to take control of an "unclaimed" online account than one that has already been set up. Plus, when you create your online access, you can utilize online alerts, update your data easier, and monitor activity quicker.

7 Social media is a hacker's favorite tool.

Be cautious of who you friend on social media and the content you post. Your social pages are loaded with personal information hackers can use to break into your financial accounts. Your birth date, pet's name, mother's maiden name, high school, etc., are all pieces of information that could be used against you.



8 Check your accounts regularly!

Get into the habit of regularly checking your banking and investment accounts, apps that allow the transfer of money, and credit reports. By keeping a close eye on your accounts, you will be able to catch fraudulent activity quicker.

9 Use a shredder.

When it comes to any printed documents containing your personal information, shred them before disposing. Criminals are not above dumpster diving to get your data!

10 Embrace security features!

Security features may seem over-the-top and sometimes intrusive, but they are there for your benefit. Multifactor authentication, biometrics, and identity verification questions are just a few security barriers that can help keep hackers away from your personal data and money.

SECURITY IS A TOP PRIORITY FOR MO DEFERRED COMP

The MO Deferred Comp Plan and their recordkeeper, MissionSquare Retirement, take cybersecurity seriously. To ensure your data and investments are safe, we have adopted a hybrid of industry-standard security frameworks and layered a combination of security methods throughout our infrastructure. This includes, but is not limited to:

- Perimeter routers and next-generation firewalls
- Data loss detection and prevention services
- Secure web gateway
- Multifactor authentication for remote access
- Endpoint encryption and protection software and services
- Application security in the software development life cycle that includes static and dynamic code analysis
- Privileged access management
- Data encryption
- Network and application penetration testing
- Controls validation through audits
- Annual testing of the business continuity and disaster recovery plan

In addition, the deferred comp plan and MissionSquare Retirement apply levels of security to their participant services and call center to detect or prevent fraud, including:

- Multifactor authentication using a one-time passcode
- Disbursement controls that include bank account validation
- Use of the FraudShare service for IP addresses with reported fraud reputation
- Blanket disbursement holds, as needed, so no money moves out

If an incident were to occur, the MO Deferred Comp Plan and MissionSquare Retirement have implemented a robust response plan to quickly identify fraud and resolve the issues as soon as possible. This holistic approach allows the plan to protect the confidentiality, integrity, and availability of your personal data and assets.



NEARLY 86% OF ALL CYBERATTACKS IN 2020 WERE FINANCIALLY MOTIVATED*



Learn more at
www.modeferredcomp.org

VPN000-003-202109



* <https://cobalt.io/blog/cybersecurity-statistics-2021>