# Protecting Yourself from AI Scams

**06:19 Megan**
Financial wellness includes the ability to manage money in a way that gives you peace of mind and empowerment to make your own choices. At Golden 1, we're here to help with unbiased financial guidance. As a not- for- profit member owned credit union, our main goal is to help you reach financial well-being. Join us as we discuss why financial knowledge matters and how to apply it to your financial journey. Together, we can be golden!

Hello! Welcome to the Golden 1 Financial Wellness podcast. I'm Megan

**00:39 Daniela**

… and I'm Daniela and we are from Golden 1's Financial Education team!

**00:43 Megan**

Welcome and thank you for joining us today as we delve into the fascinating topic of Artificial Intelligence and its impact on our financial security. AI is revolutionizing the way we live, work, and conduct business, by enabling machines to perform tasks that were previously only possible through human intelligence, such as solving complex problems and making predictions. With the potential to transform multiple industries, including finance and healthcare, AI has already demonstrated impressive results in areas such as disease diagnosis, financial forecasting, autonomous driving, and language translation. This technology can identify patterns, automate repetitive tasks and perform them more efficiently and accurately than humans, saving time and money. Overall, AI has the potential to significantly enhance our quality of life and make our daily tasks easier, while also contributing to economic growth and innovation. However, its rapid development has also brought forth a host of concerns, particularly when it comes to issues of privacy and security.

**02:04 Daniela**

Many of us have experienced receiving robotic phone calls, emails, and messages and some of these are scams and identity thieves. But not all automated communications are malicious in nature. Some may simply be advertising or spam for a particular product or service. In this context, it's important to understand that artificial intelligence is a tool that can be used by anyone for a variety of intentions.

Look at Chat GPT, for example.  For those of you who may not be familiar with this app it's a web-based program developed by Open AI. It uses data from the internet, including books, articles, and websites, to generate natural responses to a wide range of questions and prompts. Since its launch in late November 2022, Chat GPT has gained a lot of popularity and proven to be incredibly effective at understanding lots of topics. With the help of this tool, users can avoid the hassle of sifting through lengthy text or navigating complex websites.  It's cutting-edge technology and has the potential to revolutionize the way we interact with and access information online.

**03:14 Megan**

I also use Chat GPT regularly and appreciate its usefulness. But, as AI technology continues to evolve and expand, scammers and fraudsters are using these types of tools to become more sophisticated in their tactics, further highlighting the need to remain vigilant in protecting our personal data from potential threats.

AI has the ability to process vast amounts of data, including personal information obtained from social media and other online sources, allowing scammers to create more targeted and convincing scams. These AI-powered bots can even replicate human behavior, making it harder to distinguish between genuine and fraudulent responses. This type of cybercrime is known as deepfake and it takes phishing scams to a whole new level. The aim of these scams is to obtain sensitive information like passwords, credit card numbers, and financial data by impersonating a trustworthy source. A notable example is a deepfake from last year where a billionaire businessman, Elon Musk, was used to promote a fraudulent cryptocurrency investment. The deepfake was so convincing due to its use of audio and video footage from someone with credibility in the field of wealth building. Unfortunately, many individuals were deceived by this scam, resulting in the loss of their confidential information and in some cases- their money.

**04:47 Daniela**

I remember that deepfake! These text-to-speech AI tools can simulate a person's voice based on just a three-second audio clip! Pair this with spoofing- a technique where fraudsters can change the phone number on your caller id- and you can start to understand how some of these scams are successful. Fraudsters aim at targeting who and what is important to us. They may exploit our desire for financial gain with schemes promising quick and easy riches, often using high-profile figures like Elon Musk to make their claims seem more credible. Or, they may use fear-based tactics such as posing as the IRS and threatening immediate arrest or legal action unless a payment is made. By preying on our emotions, scammers can increase the likelihood of their fraudulent schemes being successful.

When our emotions are involved, it can be easy to get wrapped up in the situation and not think clearly or make decisions that we may not have made otherwise. But there are some red flags that we can and should be aware of to spot a scam or an attempt at stealing our identity. Scammers will often use urgent or emotionally charged language to pressure us into taking immediate action without giving it proper thought. They may also request payment through untraceable methods like purchasing gift cards, using pay apps, or exchanging cryptocurrency, in order to avoid detection.

If you receive this type of heightened situation call or message - ask yourself if the situation being described is even plausible? Is it too good to be true? Or can you verify the story?  If, for example, your grandson claims to be calling from another part of the world, can you phone his parents to verify the story? If you can't confirm the story, hang up immediately. Don't give the scammer time to keep you on the phone and convince you that they are your loved one in a tough situation. Remember, scammers are professionals and know the right things to say to convince you to send them money or divulge your personal information. By being vigilant and recognizing these red flags, we can protect ourselves and our loved ones from falling victim to these deceitful tactics.

**07:00 Megan**

In my family we have developed a layer of security that AI may not be aware of. We have a family password or a pre-arranged safe word. For example, if my child is approached by someone claiming to be a family friend or relative, they can ask for the safe word or password to confirm the person's identity before going with them or responding to their message or phone call. This strategy can be particularly helpful in cases where the imposter is using AI technology to clone a loved one's voice.

**07:32 Daniela**

What a great idea! It's always wise to take proactive steps to protect ourselves and our loved ones from potential threats, and having a family password or safe word is an excellent example of such a measure. Two-factor authentication can also provide an extra layer of security as well as using strong unique passwords. Keeping your operating system, antivirus software, and other applications up to date will also ensure that you have the latest security available to protect you from scammers and identity thieves. As a reminder, it's also a best practice to not click on links in emails or messages from unknown sources, be mindful of the personal information you are posting on social media, check your bank and credit card statements regularly for any unauthorized transactions, set up alerts for suspicious activity on your accounts, and check your credit report at least once a year for signs of identity theft.

Reporting scams and fraud is also an important action step in combating these criminal activities. If you are a victim of a scam or similar incident, report it to your local police and file a report with the Federal Trade Commission at Reportfraud.ftc.gov.

In addition, staying up to date on the latest types of fraud, scams, and identity theft, and how to prevent and handle such situations is important. The Federal Communications Commission maintains a common fraud and scam list that is regularly updated on their website at www.fcc.gov. By staying informed and taking proactive measures, we can protect ourselves and our loved ones from falling victim to scams and fraudulent activities.

**09:12 Megan**

Don't miss out on even more financial tips and insights by subscribing to the Golden 1 Financial Wellness podcast, available on Apple, Google, and Spotify. Our podcast episodes "Staying Safe on Public Wi-Fi" and "Identity Theft," are packed with invaluable advice to help you protect yourself from scammers and thieves too.

But that's not all – the "Financial Wellness" tab at Golden 1.com is a treasure trove of resources. You can explore engaging videos, interactive modules, and enlightening webcasts, all designed to enhance your financial knowledge. Make the most of our Learning Lab, where you can access our comprehensive Identity Theft Risk tool to ensure you're taking all the necessary precautions to safeguard yourself against fraudsters and scammers. And for further guidance, our vast collection of articles, videos, and the Identity Theft Course in the Learning Lab are exceptional resources to boost your financial security and wellness.

**10:15 Daniela**

Thank you so much for joining us today. This has been Daniela

**10:18 Megan**

And Megan. Wishing you financial health and happiness — and, as always, reminding you to …

**10:23 Daniela and Megan:**

… stay golden!

**10:26 Megan**

Golden 1 Credit Union is insured by NCUA