Rising of Deepfake Scams Targeting Consumers

Deepfake technology, once used primarily in entertainment and education, is now being weaponized to exploit consumers, posing significant risks to personal security and financial well-being. Leveraging artificial intelligence (AI), deepfakes can produce eerily realistic images, videos or audio recordings that blur the lines between reality and manipulation.

According to a report by Signicat, AI-powered fraud attempts now account for 42.5% of all detected fraud, with nearly one-third successfully executed. Deepfake fraud has skyrocketed by an astonishing 2,137% over the past three years, underscoring the urgent need for awareness and vigilance as this technology becomes increasingly accessible.

Deepfake scams often involve impersonating trusted individuals – such as family members, friends or financial advisors – to gain access to personal or financial information. Scammers have used this technology to clone voices, manipulate video calls and even create fake social media accounts to target unsuspecting victims.

To help protect yourself and your family, follow these key steps:

- **Educate yourself and your family –** Understanding what deepfakes are and how they're misused is the first step to staying safe. Teach loved ones to look for unusual distortions in videos or images, examine content for signs of manipulation and avoid acting on sensational or "too-good-to-be-true" information without verification.
- **Limit your online footprint –** Be mindful of what you share online. Personal photos, voice clips and even casual posts can be used to create convincing deepfakes. Adjust privacy settings on social media to limit who can see and share your content and consider using watermarks on photos to discourage unauthorized use.
- **Monitor your name and likeness –** Set up alerts for your name or image to quickly identify unauthorized use. Identity monitoring tools can also help you track and address misuse.
- **Leverage advanced security measures –** Stay ahead of evolving threats by using technologies such as facial recognition with additional verification steps or identity monitoring software. These tools can help detect and mitigate fraud attempts involving deepfakes.

These tips are provided by the Iowa Bankers Association.