

BE FRAUD SMART Stay alert. Stay informed. Stay protected.

Online Fraud in the Age of AI

Online fraud can impact anyone—regardless of age.

As Artificial Intelligence (AI) advances, the threat of identity theft and online fraud continues to escalate.

AI's rapid advancement isn't just a boon for innovation—it's also a powerful tool for scammers, making their schemes more sophisticated and harder to spot.

For example, the use of AI has led to a staggering surge in malicious emails, between 2022 and 2023 alone.

While many believe that older adults are more susceptible to ID theft and online scams, the reality is that internet fraud can impact anyone—regardless of age (see graph).

The key to safeguarding your personal and financial information lies in awareness. Understanding the tactics scammers use will help your entire family master the art of detection and fortify their defenses against these digital threats.

Here's a closer look at some current AI-driven scams, along with some practical tips to stay one step ahead.

VOICE CLONING: THE FAMILIAR VOICE OF FRAUD

Imagine receiving a distress call from a family member, their voice unmistakable, pleading for immediate financial help. It may sound like science fiction, but fraudsters can now use AI to replicate the voice of someone you trust. Social media is a goldmine for voice samples, feeding the technology needed to execute these scams.

If you get a phone call from a loved one urgently requesting money, hang up and reach out directly to the family member in question, or another trusted relative to verify the claim.

Remember, urgency is the scammer's ally.

DEEPFAKE DECEPTION: SEEING ISN'T ALWAYS BELIEVING

Deepfakes use AI to add realistic images onto existing videos, creating fake videos that are convincingly real. These videos can be weaponized to impersonate real people to trick you into falling victim to fraudulent scenarios.

So how can you know if a video is real or fake?

Watch for unnatural movements, inconsistent lighting (including shadows around the eyes), and out-of-character behaviors—like not blinking, or using strange word choices.

Most importantly, remember that verification remains your best defense. Directly contact the person being impersonated to confirm the authenticity of the message, especially if it involves a financial transaction.

THE DOUBLE-EDGED SWORD OF AI CHATBOTS

Many websites feature chatbots, a pop-up chat feature that makes it easy for users to ask questions and receive immediate answers.

While chatbots are great tools, they can also be used by online scammers to engage victims with seemingly legitimate

customer support interactions—like sending an unsolicited email or text message claiming that your account has been blocked, or some other error.

Here are some common red flags to watch out for, and how you should react to them:

Unverified Payment Requests

Legitimate organizations will NEVER solicit sensitive information or payments through unverified channels, so be skeptical of unsolicited links—especially if they demand money. Always double-check the source before sending payments.

Subtle Inconsistencies

Whether it's a cloned voice, a deepfake video, or a chatbot, look for anomalies—like unnatural language, odd behaviors, or anything that just feels "off."

Urgent Demands

Pressure tactics are a big red flag, so take a moment to confirm a request before sending money. Consider asking a friend or trusted family member for help.

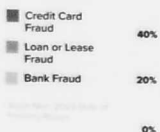
OTHER COMMON SCAMS TO WATCH OUT FOR

TECH SUPPORT SCAMS

Never call a number or click on a link from an unexpected pop-up claiming there's an issue with your device. Odds are, it's malware trying to lure you into a scam.

Legitimate companies won't contact you out of the blue for tech support. They also won't pressure you to use payment methods that are hard to reverse, like wire transfers, gift cards, prepaid cards, or cash reload cards. Another major warning sign is when a request is made to gain remote access to your computer.

THREE COMMON ID THEFT TYPES BY AGE GROUP



NEVER SHARE Legitimate organizations

If you genuinely suspect an issue with your device, contact tech support from an official source.

FAKE PRIZE SCAMS

"You've won a prize!" Scammers know that excitement over winning a prize can be enough to cloud anyone's judgment. A big red flag: watch out for is being asked to pay taxes, fees, or processing before awarding you the prize.

A legitimate prize promotion will never charge you money or request personal/financial data. If you receive a major prize, they'll have clear protocols to validate you as the winner without charging you fees first.

VISIT UCCU.COM/FRAUDSM

A free resource created to help keep entire families educated and informed on current online frauds and scams, and what to do if you should fall victim.

Stay vigilant, stay informed, and together we can combat online fraud in the