

The Federal Trade Commission reported that fraud losses last year in the U.S. topped \$23.7 billion, though some estimate that number could be as high as \$158 billion.



How to Protect Yourself

- Create a secret word or phrase with family members to easily verify identity.
- Trust your gut – if it seems too good to be true, it probably is.
- #BanksNeverAskThat – don't fall for messages that appear to be coming from your bank.
- Verify before you act – contact your bank directly before taking action over the phone or clicking suspicious links.
- Limit your online content – scammers use social media to impersonate victims.
- Add a trusted contact to your bank account for fraud protection.

Trust Your Local Banker

- Before clicking, sending money, or sharing information – call your local banker!
- If you suspect fraud, contact your bank immediately – acting fast improves the chances of recovering losses.
- Bankers see fraud every day and know what to look for. If they contact you about potential fraud – take the time to investigate and verify.
- Bankers are your best resource for preventing financial scams!

Stay Informed and Report Fraud

- **FTC:** consumer.ftc.gov
- **IC3 (FBI Internet Crime Center):** ic3.gov
- **CFPB:** consumerfinance.gov
- **FDIC:** fdic.gov
- **#BanksNeverAskThat Quiz:** banksneveraskthat.com/scam-quiz
- **IBA Fraud Resources** iowabankers.com

Fraud Prevention Guide

Fraud Trends to Watch For



Romance scams



Fake prize scams



Check fraud



Government imposter scams



Fake distress



Payment app fraud

Cyber Fraud Trends

- **Account compromise/takeover:** For example, someone getting your bank account password or other login credentials.
- **Identity theft:** Criminals get enough of your personal information to take out loans on your credit, impersonate you, and apply for credit cards, mortgages, car loans, etc.
- **E-commerce scams:** Tricking you into giving away your credit card information, which is then used to purchase goods, leaving you the bill
- **Installation of malware:** Criminals install bad programs on your computer that steal your data, or lock you out of your system, then charge you to restore data or access. Your computer can even be used by cybercriminals to attack others.
- **Text/social media fraud:** Fake delivery notices, bank alerts, or investment scams

For more information on fraud trends, visit iowabankers.com.

Be Aware of the Use of AI

- Criminals use AI to create incredibly sophisticated scams. AI is used to voice clone and create falsified information making the scam seem even more real.



IOWA BANKERS
ASSOCIATION