FIDUCIARY™ TRUST

Staying Secure in a Changing Digital World

Information Security Insights

Key Takeways

- Cyber threats are becoming more sophisticated, targeted, and difficult to detect, especially with the use of artificial intelligence
- High-net-worth individuals and families are particularly attractive targets due to the scale and complexity of their assets
- A combination of disciplined habits, technical safeguards, and verification protocols can significantly reduce risk
- If a breach occurs, acting quickly can help limit financial loss and protect your long-term financial plan

Why is Cybersecurity Risk Increasing for Individuals and Families?

Cybercrime is no longer opportunistic; it is increasingly organized, targeted, and driven by technology. High-net-worth individuals are especially vulnerable because of their financial visibility, digital footprint, and reliance on multiple advisors and platforms.

Learn More:

For more insights or information on Fiduciary Trust visit:

www.FidTrustCo.com

or contact:

Sid Queler
queler@fiduciary-trust.com
617-397-7181

Perhaps the most significant emerging risk is the ability to impersonate trusted individuals, including family members, advisors, or executives

At the same time, the scale of digital fraud continues to grow. According to the Federal Trade Commission, reported fraud losses in 2024 reached $12.5 billion in the United States alone, which represented a 25% increase over the previous year.[1]

One of the most important shifts is the role of artificial intelligence. AI is enabling cybercriminals to:

- Create highly convincing phishing messages
- Automate large-scale attacks
- Personalize scams using publicly available information
- Mimic trusted individuals or institutions

These developments are transforming cybercrime from a "numbers game" into a trust-based attack strategy.

How is Artificial Intelligence Changing the Threat Landscape?

Perhaps the most significant emerging risk is the ability to impersonate trusted individuals, including family members, advisors, or executives. AI-powered tools can now generate:

- Voice clones that sound like a spouse, child, or advisor
- Deepfake videos that appear to show a real person making a request
- Real-time impersonation during video calls or phone conversations

For individuals and families, this creates a new reality: familiar voices and faces can no longer be relied upon as proof of authenticity.

What Steps Can You Take to Reduce Your Risk?

There is no single solution, but a layered approach can significantly improve security:

1. Strengthen Account Security

- Use unique, complex passwords for each account
- Enable multi-factor authentication (preferably app-based or hardware-based rather than a text message)
- Regularly monitor financial and email accounts

2. Establish Verification Protocols

- Confirm all financial transactions, especially wire requests, through a secondary channel
- Create family-wide protocols for verifying urgent or unusual requests
- Be cautious of any communication that creates urgency or secrecy

3. Limit Your Digital Footprint

- Be thoughtful about what is shared publicly

- Review privacy settings on social media and online platforms
- Minimize exposure of travel, family, or financial details

4. Secure Devices and Networks

- Keep software and devices updated
- Avoid public Wi-Fi for financial activity
- Consider using a dedicated device for sensitive transactions

5. Educate Family Members and Staff

- Ensure that all family members understand common risks
- Provide guidance for household staff or assistants who may handle communications
- Reinforce consistent practices across all participants

For many families, the most significant vulnerabilities arise not from technology, but from human behavior. There are a number of additional steps you can take to help protect yourself against fraud-related identity theft:

- Obtain and carefully review your credit reports
- Set up your My Social Security Account, in part to prevent someone else from doing so (https://www.ssa.gov/myaccount/)
- Guard your social security number
- Freeze your credit
- Consider credit monitoring services
- Be leery of unsolicited mail
- Review your bank, credit card, and investment statements regularly
- Shred sensitive information
- Delete questionable emails and texts
- Let phone calls from unknown parties go to voicemail

For many families, the most significant vulnerabilities arise not from technology, but from human behavior

FIDUCIARY™ TRUST

Author

Puneet Nevatia
Chief Operating Officer

Let's discuss what's important to you

Contact Sid Queler
queler@fiduciary-trust.com
617-397-7181

What Should You Do If You Suspect Your Identity Has Been Compromised?

Even strong safeguards cannot eliminate risk entirely. If something appears suspicious, speed is critical. If you suspect fraud, we recommend taking the following immediate actions:

- Initiate a fraud alert on your credit file
- Review your credit reports
- File an Identity Theft Report at https://www.identitytheft.gov
- Change your passwords and access credentials across key platforms
- Contact creditors, banks, and other organizations
- Consider filing a police report
- File tax returns as soon as possible
- Document all activity and communications

A Closing Perspective

Technology has created extraordinary convenience, but also new forms of vulnerability. As cyber threats become more personalized and sophisticated, maintaining a healthy level of skepticism is essential.

At Fiduciary, we view cybersecurity as an important aspect of helping clients safeguard their financial lives, not only by managing assets, but by helping families navigate the evolving risks that surround them. If we can be of assistance to help you with your wealth planning, including cybersecurity recommendations, please reach out to your Fiduciary Trust officer or Sid Queler at queler@fiduciary-trust.com. ■