resolution
Your Identity at Risk, Our Solutions at Work™

Let's take a brief look at the 3 fastest growing trends and categories for Identity Theft

- ### Account Takeover (ATO) Fraud

  This happens when criminals gain control of existing accounts—banking, email, shopping, healthcare, or social media—using stolen passwords, phishing, SIM swaps, or malware. Once inside, they change passwords, transfer money, or impersonate victims. Industry and law-enforcement reporting shows strong growth in these attacks during 2025.

- ### Synthetic Identity Fraud

  Synthetic identity fraud involves combining **real data**—often a Social Security number—with **fake names, addresses, or identities** to create a new "person." Criminals then open credit lines, loans, or accounts and build fake credit histories before cashing out. Fraud experts increasingly identify this as a major 2025 growth area.

- ### AI-Driven Impersonation and Deepfake Fraud

  AI has accelerated identity crime by making fake voices, emails, texts, and videos more convincing. Reports show sharp increases in impersonation scams and concern over voice-cloning and deepfake fraud.

Why this matters for individuals !

Traditional identity theft focused on events such as **stolen credit cards or opening accounts**. The newer trend is **taking over digital identities and using AI to bypass trust and security systems**—making fraud faster, harder to detect, and more personalized.

5 Warning Signs Your Identity or Online Accounts may be Compromised

1. Unexpected Security Alerts or Password Changes

You receive notifications about password resets, two-factor authentication codes, or login attempts that you did not request. Locked accounts or unfamiliar devices appearing in your account settings are strong indicators of unauthorized access.

2. Unrecognized Charges or Financial Activity

You notice small "test" transactions, unfamiliar purchases, withdrawals, wire transfers, or new payees on your bank or credit card statements. Criminals often start with small amounts before attempting larger fraud.

3. New Accounts or Credit Inquiries You Don't Recognize

You receive credit card offers, loan denials, or alerts about hard credit inquiries you did not authorize. A sudden change in your credit score may indicate someone has opened accounts using your information.

4. Missing Mail or Unexpected Bills and Collection Notices

Bills stop arriving, or you receive statements, tax documents, medical bills, or debt collection notices for accounts or services you never opened or used.

5. Friends, Family, or Colleagues Receive Suspicious Messages From You

Contacts report strange emails, texts, direct messages, or social media posts that appear to come from your accounts. Criminals frequently use compromised accounts to spread scams or phishing links.

Think you might have a problem?

Call us at 877 308 9169

Learn more at our website:

https://idresolution.net/

resolution
Your Identity at Risk, Our Solutions at Work™