Protecting Yourself from Scams and Identity Theft

~~~ Bill Schretter, CFP, CFCS ~~~

Table of Contents

What is Identity Theft

Identity theft occurs when someone fraudulently obtains and uses another person's personal information, such as their Social Security number, credit card number, or other identifying information. The goal is usually to commit fraud or other crimes under the victim's identity. Identity theft cost US citizens and businesses about $56 billion annually[i]. AARP research in 2023 indicated $43 billion was stolen from US citizens[ii].

Common Methods of Identity Theft

- **Phishing**: Fraudulent emails, texts, or calls that trick people into sharing personal data.
- **Skimming**: Hidden devices at ATMs or gas pumps capture card information.
- **Data Breaches**: Hackers target databases of companies to steal large amounts of customer data.
- **Mail Theft**: Thieves intercept mail to obtain credit cards, checks, or other sensitive information.
- **Social Engineering**: Manipulating people into divulging confidential information by impersonating trusted individuals.

Strategies for Protection

- **Strong, Unique Passwords**: Use different passwords for each account and consider a password manager. It is important to realize that a password that is used
~~~

on one account my later be known and attempted on another account, so do not use the same passwords or password template on different accounts.

- **Two-Factor Authentication (2FA)**: Enables an additional layer of security by requiring a second form of verification.
- **Limit Social Media Sharing**: Avoid sharing personal information like birthdates, addresses, or other sensitive data online.
- **Shred Documents**: Shred any documents containing personal information before disposal.
- **Secure Wi-Fi Connections**: Use a secure network, particularly when conducting financial transactions.
- **Review Financial Statements**: Regularly check credit card, bank, and other financial statements for unusual activity.
- If you maintain a list of accounts or passwords (paper or electronic), keep in a safe place so that cleaning service, vendors, contractors, guests, customers, or employees cannot view or steal the information easily.
- In office environments, keep personal and financial information in locked drawers. Have signs that cameras monitor file rooms. Use security methods like passcodes and ID Badges to prevent individuals from unauthorized access of office space or systems.

How to Monitor for Identity Theft

- **Credit Monitoring**: Services that monitor your credit report for any changes or inquiries.
- **Fraud Alerts**: Place a fraud alert on your credit file with the major credit bureaus.
- **Credit Freeze**: Freezing your credit report prevents creditors from accessing your credit, making it harder for thieves to open accounts in your name.
- **Annual Credit Report Review**: Review credit reports from all three bureaus (Equifax, Experian, and TransUnion) yearly at AnnualCreditReport.com.

Reporting Identity Theft

- **Contact Financial Institutions**: Notify banks and credit card companies immediately if you detect unauthorized activity.
- **File a Report with the FTC**: The Federal Trade Commission (FTC) allows victims to report identity theft through their website IdentityTheft.gov.
- **Report to Law Enforcement**: Some instances may require filing a police report, especially if local crime is involved.
- **Notify the Credit Bureaus**: Contact the three major credit bureaus to place a fraud alert or credit freeze on your file.

Protecting Yourself from Scams and Identity Theft

~~~ Bill Schretter, CFP, CFCS ~~~

Types of Phishing Attempts

Phishing is a common method used by cybercriminals to trick individuals into sharing sensitive information such as passwords, credit card numbers, or Social Security numbers. Phishing usually happens via email, but it can also occur through text messages (smishing), phone calls (vishing), and fake websites.

- **Email Phishing**: The most common form where attackers send fraudulent emails that look legitimate, often impersonating trusted organizations like banks, delivery services, or government agencies. These emails contain links to fake websites or attachments with malware.
- **Spear Phishing**: A targeted form of phishing aimed at specific individuals, often containing personal information to make the message seem more convincing.
- **Smishing**: Phishing through text messages. Smishing attempts may include links to fake websites or request that the user replies with personal information.
- **Vishing**: Phishing through phone calls. Attackers might impersonate support representatives, bank officials, or government agents to convince the victim to reveal information or make payments.
- **Clone Phishing**: Cybercriminals copy a legitimate email and replace any links or attachments with malicious versions, then send it to the victim, often appearing to come from a known contact.

How to Recognize Phishing Attempts

- **Suspicious Sender Information**: Look closely at the sender's email address/Header. Phishers often use addresses that look similar but may contain slight misspellings or extra characters. They may also be sending from a public email provider like Gmail, Yahoo, or Outlook. The Social Security Administration, the IRS, the US Postal Service, Amazon, Microsoft, Bank of America, etc. do not use Gmail, Yahoo, or Outlook email domains to send emails to customers.
- **Urgent or Threatening Language**: Many phishing attempts include urgent language, like "Your account will be suspended" or "Immediate action required," to provoke a quick response.
- **Poor Grammar and Spelling**: Many phishing emails contain spelling errors, awkward grammar, or unusual phrasing.
- **Unusual Links or Attachments**: Hover over links without clicking to see the actual URL. Avoid clicking links that do not direct you to the official website. Often, they direct you to cloud files in Google accounts or Yahoo or an unknown service provider, sometimes referenced in a foreign language.
- **Requests for Sensitive Information**: Legitimate companies will never ask for personal details like passwords or Social Security numbers over email or text.
~~~

Protecting Yourself from Scams and Identity Theft

~~~ Bill Schretter, CFP, CFCS ~~~

What to Do if You Encounter a Phishing Attempt

- **Do Not Click Links or Open Attachments**: Avoid engaging with any content in a suspicious message.
- **Report the Phishing Attempt**: Most email providers have options to report phishing emails. You can also report phishing emails to the Anti-Phishing Working Group (APWG) at reportphishing@apwg.org or directly to companies being impersonated.
- **Delete the Message**: After reporting, delete the message immediately.
- **Stay Updated**: Use reputable antivirus software, and ensure your system and applications are up to date to guard against malware that may accompany phishing attempts.

Preventing Phishing Attempts

- **Enable Multi-Factor Authentication**: This adds an extra layer of security.
- **Educate Yourself and Others**: Being aware of phishing tactics helps to identify these scams.
- **Use Spam Filters**: Many email providers filter out potential phishing emails, which reduces the chances of these attempts reaching your inbox.

Other Types of Common Scams

1. **Romance scams**- scammers may ask for financial help for a variety of reasons, including:

    - Travel expenses to visit you.
    - Medical expenses for themselves or a family member
    - Emergency money
    - Paying off debts
    - In exchange for intimate photos, they may ask you to send personal information.
    - They may pose as a military member and ask for money to cover military-related expenses.
    - They may ask you to verify your Tinder account through an email or text

2. **Tax & Credit Scams- Threaten police involvement if money owed is not repaid.**

    - Phone calls from fake IRS agents.
    - Emails that steal personal information
    - False tax returns to steal your refund.
    - False charities that ask for donations
    - False tax preparers who pose as legitimate professionals
    - Offers to move money offshore.
    - Promises of a larger tax refund than you are due.
    - Phishing emails that ask you to verify information
    - Claiming your SSN has been suspended.
~~~

- Receiving emails requesting additional tax forms
- Fake IRS messages
- Gift card scams, where scammers call or leave a voicemail claiming you owe federal taxes.

3. **Employment Scams -** Request information such as Social Security card, birthday, and back account information for the purpose of onboarding you as an employee.
    - Pretend to hire you for a position and require information for background checks or actual payroll setup.
    - Offer unusually high salaries or remote location work to encourage you to believe that the job is legitimate.
    - Request that you travel to a specific location for training. This is a dangerous element of the scam because they may attempt kidnapping or enslavement, especially if they are able to seize and keep your Passport in a foreign country.

4. **Delivery Scams –** A message from Amazon, USPS, US Customs, or UPS sent via email or text that indicates there is a problem with a delivery, additional information is needed or there is an unpaid invoice that is still outstanding
    - These scams do not know if you have such an account or pending delivery, they are phishing for information. They will ask you to verify your identity via name, address, birthdate, SSA, bank account, credit card info, and even PIN.
    - They will ask you to log into a site that looks real, but is a fake site where you type in all your information.
    - The scammers will seek to download virus software to collect even more data from your phone or computer, including location data and other data files.

Value of Stolen Information on the Black Market

Stolen personal information has significant value on the black market, especially for organized criminal syndicates that specialize in identity theft and fraud. The value varies depending on the type of information, its quality, and demand. Personal data can remain valuable for years because the criminal creates a profile on their victim, collects data from multiple sources, and analyzes the data for patterns in passwords or potential interests that can be exploited. Criminals will use the information, images, and professional credentials to target both the person and potentially their employer to gain access to personal and business systems. Criminals might bide their time and use stolen data after a delay to avoid detection. If the criminal is unable to use the data, t the data may become more valuable to them by selling to another criminal.

Here is a look at the worth of various stolen data and what criminals typically do with it:

- **Credit Card Numbers**: $5 to $110 per card, depending on factors like the card's limit, associated bank, and whether it includes CVV and other identifying information.
- **Social Security Numbers (SSNs)**: $1 to $10; however, if bundled with other personal information in a "fullz" (a full set of personal details), prices increase significantly.
- **Bank Account Information**: $25 to $500, influenced by the account's balance and status.
- **Medical Records**: $1 to $1,000 per record. Medical data is highly valuable due to its detailed personal information and potential for insurance fraud.
- **Driver's Licenses and Passports**: $50 to $1,000, often used for identity theft and forgery.
- **Login Credentials**: The price varies widely, from $5 for social media accounts to several hundred dollars for corporate emails.

What Criminals Do with Stolen Data

- **Financial Fraud**: Stolen credit card or bank information is used for unauthorized purchases, wire transfers, or reselling online.
- **Synthetic Identity Fraud**: Criminals create new identities by combining real and fake information, which they use to open fraudulent accounts or secure loans.
- **Account Takeover**: With login credentials, attackers gain access to email, social media, or bank accounts, often using them for scams or to target contacts.
- **Medical Fraud**: Medical data is used to fraudulently bill insurance for medical services, drugs, or equipment. This can also lead to inaccurate medical records for the victim.
- **Tax Refund Fraud**: Criminals file fake tax returns to claim refunds using stolen SSNs and other personal information.
- **Resale of Information**: Data is often sold multiple times across the dark web to different buyers, who may then exploit it in various ways.
- **Long-Term Exploitation and Extortion:** Some criminal organizations use stolen data for prolonged exploitation.: If sensitive personal information is obtained, criminals may threaten to release it unless the victim pays a ransom.
- **Personification -** Present themselves a s a family member or friend to request emergency money for bail or medical needs. Often requesting to be paid via gift card, bank wire, or credit card transfer. A strategy to help prevent this is to maintain a "security password" within your family or friend circle that is used to verify your identity.

Larger Operations by Syndicates

In some cases, criminal syndicates take stolen information to a larger scale:

- **Social Engineering and Targeted Attacks**: Organizations may use the data to carry out large-scale phishing campaigns, pretexting attacks, or "man-in-the-middle" schemes.
- **Corporate Espionage**: Information about employees, systems, and clients can help in launching attacks on organizations, potentially leading to further profitable breaches.
- The stolen data is a high-value commodity that organized crime syndicates manipulate for profit, often using it to fuel ongoing fraud and criminal operations.

Important Tips to Protect Yourself

Never purposely or for compensation do any of the following. If so, you may be assisting a criminal enterprise in facilitating their strategy to victimize people or conduct money laundering operations.

- Use another person's bank account or credit card number for a transaction.
- Deposit money into your own account only to then transfer to another account under the request of a third party.
- Have a mail package delivered to your home for the purposes of redirecting to another location.
- Not report packages being delivered on a regular basis to your home, and then being picked up by a third-party claiming, "it was delivered to the wrong address."

If you are the victim of or suspect fraudulent transactions on your credit card, bank accounts, credit report, or medical transactions, report these transactions to the respective organization. If the crimes are not reported, then they can not be investigated and the perpetrators stopped and convicted.

Do not get into a conversation or email exchange with a scam artist or syndicate. Do not inform them that you have/ will report them. Such individuals can be dangerous, and they have local mules (syndicate members) who may threaten you. You can be targeted for increased identity theft efforts. Report any concerns to local Police.

Additional Sources for Information and Research

1. US Justice Dept – What to do if your Identity is Stolen
2. US Department of Health - The Financial and Psychological Impact of Identity Theft Among Older Adults
3. US Justice Department - **Identity Theft Recovery Plan**

Important Disclosure About This Article

This primer is for educational purposes only. The information is a compilation of articles from trusted public domain sources and government agencies. The information included is believed accurate, but not guaranteed and subject to change without notice. This article was compiled by Bill Schretter, CFP, CFCS, EA. This primer is not to be considered financial, tax, or legal advice.

---

[i] https://www.idx.us/knowledge-center/the-real-cost-of-identity-theft-to-employees-businesses
[ii] https://www.aarp.org/money/scams-fraud/info-2024/identity-fraud-report.html#:~:text=American%20adults%20lost%20a%20total%20of%20%2443%20billion,in%202022%20%28when%20the%20number%20was%2015.4%20million%29.?msockid=379c386aec8e66b207fc2a60ed0367f0