Preventing Identity Theft

About Financial Knowledge Network

Financial Knowledge Network (FKN), founded in 1989, is a nationwide provider of on-site and web-based employee financial education courses. FKN continually reviews and updates our material to stay current during changing laws and markets. Participants will gain the information, knowledge, and skills to make educated financial decisions.

Workbooks and Course Content

The information contained in this workbook and presented during the course is for educational purposes only. FKN does not recommend any financial products nor render financial/legal advice. Students should seek guidance from a tax advisor, attorney, or other financial professionals for counsel on their specific issues.

The material contained herein is believed to be accurate at the time of printing, but is subject to change. All information provided is of a general nature and is not intended to address the circumstances of any particular individual or entity. Any examples included herein are for illustrative purposes only; *no implications should be inferred*.

Instructors

Our instructors have a minimum of 10-15 years of experience in the financial services industry. Their backgrounds include previous associations with banks, brokerage houses, mortgage lending, insurance, and financial planning firms. Many of the instructors have previous teaching experience as adjunct faculty members with institutions of higher education and community colleges.

In addition to a college degree, many of the instructors also maintain a CFP® (Certified Financial Planner) credential or are currently enrolled in the CFP® Professional Education Program. Our certified instructors are required to meet annual continuing education requirements in the financial planning field.

Financial Knowledge Network, LLC
P.O. Box 8756
San Jose, CA 95155-8756
www.financialknowledge.com

Authorized IACET Provider

Financial Knowledge has received authorization by the International Association for Continuing Education and Training to award CEU credit for its courses. Individuals may earn CEU credits for attending Financial Knowledge courses. Financial Knowledge provides over 75 conflict-free financial education classes to the workplace.

IACET is an internationally-recognized organization with standards and authorization for continuing education. Financial Knowledge courses are in compliance with IACET's high quality standards in the areas of learning environment, learning outcomes, instruction, course content, assessment, and support services.

In order to obtain CEU credits for attending this Financial Knowledge course, we need to receive confirmation that you've attended. This can be in the form of your printed name (first and last), email address, and your handwritten signature for live classes and through the electronic report from the online meeting center used for webcast classes. Please note your full name and email is required upon login for webcast classes to give you proper credit for attending. If you have any questions about this process, please call 408-414-5050 or email info@financialknowledge.com.

Privacy Policy Information

Financial Knowledge respects your privacy and recognizes the need to protect your personal information. We do not sell any financial products or personal financial advisory services. In addition, we do not request or collect any personal financial information from visitors to our site. Financial Knowledge's mission is to provide conflict-free financial education courses to students based on identified needs and which satisfy the ANSI/IACET standard to award ANSI/IACET CEU's.

Your personal information is used only within Financial Knowledge for maintaining a permanent student record. This student record shows the classes you attended, online follow up assessments that were successfully completed, the number of CEU's awarded (based upon the total contact hours), as well as your permission to send you emails about upcoming Financial Knowledge classes. If you no longer wish to receive emails about future Financial Knowledge classes, simply select the notifications preference box under Edit My Student Profile under My Account.

Your permanent student record is accessible only to you or authorized individuals at your employer. Other than authorized individuals at your employer, your permanent student record may be released only with your permission and notification.

Course Description

Participants will learn how to define identity theft, employ steps to avoid identity theft, develop awareness of specific identity theft crimes, and learn exactly what to do should they find themselves a victim of identity theft. Interactive exercises and thought-provoking questions will stimulate participants to adopt and maintain habits to improve the security of their personal finances.

Audience

Recommended for those who want to learn solid methods of preventing identity theft and want to learn exactly what to do should they find themselves a victim. This course is especially valuable to those who bank, pay bills, and make purchases online, or anyone who has assets/ credit they want to protect.

Learning Outcomes

- Define identity theft, who commits the crime, its victims, and its cost to consumers
- Identify types and methods of identity theft, including "phishing", and other scams
- Minimize risk of becoming a victim of identity theft by employing simple and effective security habits
- Interpret government legislation and understand what government agencies are doing to help
- Develop awareness about areas left open to identity thieves
- Learn how to question those who may request private information about you
- Design a plan and know exactly what to do and who to contact should you find yourself a victim of identity theft
- Evaluate whether you should buy insurance or sign up for other services designed to protect against identity theft

Table of Contents

Test Your Awareness

Before getting into the details of the course, see if your current actions and behaviors may be leaving you susceptible to identity theft.

✓ EXERCISE

1. **I check my credit report:**
   A. Two or more times a year
   B. Once a year
   C. Every few years
   D. Never
2. **I pay for credit cards and other bills by:**
   A. Mailing payments at the post office or official collections box
   B. Putting paid bills in the home mailbox for pickup
   C. Using online banking or bill pay
3. **The information printed on my personal checks includes:**
   A. Full name, personal address, and phone number
   B. Full name and personal address
   C. First initial, last name, and home address
   D. First initial, last name, and P.O. Box, or work address
4. **I am at the doctor's office and the receptionist asks for my Social Security number for account identification. I:**
   A. Give the receptionist my Social Security number
   B. Whisper it, making sure no one else can hear me
   C. Ask why they are using my Social Security number to identify me and if there is some other method they could use
5. **I review my bank and credit statements:**
   A. Online at least two times each month
   B. Within the first 15 days of receipt
   C. 15-30 days after receipt
   D. Occasionally, but usually after 30 days
   E. Never
6. **Do you own a shredder and use it?**
   A. No (or yes, but rarely)
   B. Yes, and I use it occasionally, but not consistently
   C. Yes, I use it to shred any sensitive documents

7. **My password is:**
   A. Something easy to remember, such as my birthday, mother's maiden name, or child's birthday
   B. Something obscure that others would have a difficult time figuring out
   C. Something obscure that others would have a tough time figuring out, and I change it frequently
   D. So complicated that I need a password manager to keep track of it
8. **The way I use antivirus and firewall software on my computer is:**
   A. I don't have antivirus software or a firewall on my home computer
   B. I run antivirus software, but the subscription has expired
   C. I have updated antivirus software running in the background automatically
   D. I have updated antivirus and firewall software running automatically
   E. I have updated antivirus, antimalware, and firewall software running
9. **The way I use social networks and blogs is:**
   A. I never or rarely visit them; If I do, I don't comment on anything
   B. I have a few favorites, but if I comment, I do it anonymously with a different email address (not my primary one)
   C. I visit regularly, comment occasionally, and use my email address and name
   D. I spend a lot of time on social networks and blogs, and others know me there
10. **My wallet contains:**
   A. Social Security card
   B. The bare essentials: some credit cards and a driver's license
   C. The bare essentials with a copy of sensitive information stored in a separate location in case my wallet is stolen

Tally Your Score

Tally up the points based on your answers, then discover what your score means in the Appendix on Page 32. Revisit the quiz in 30 days to see how much you've improved!

	A	B	C	D	E
1.	10	8	4	0	
2.	4	3	5		
3.	0	1	3	5	
4.	0	3	6		
5.	6	5	4	3	0
6.	0	2	5		
7.	0	3	5	10	
8.	0	1	2	5	8
9.	5	4	1	0	
10.	-5	3	6		

Identity Theft

What Is Identity Theft?

Identity theft occurs when personal information, like a name or Social Security number, is used without permission by a thief to impersonate a victim and commit fraud. Thieves use this personal information to open new accounts, obtain credit, buy merchandise and services, or commit other fraud.

Identity theft has proliferated for many reasons:

- The use of credit (especially "instant" credit) has become increasingly popular.
- It has become easier to gain access to personal information.
- The rapid growth of the Internet and consumer databases has exposed Social Security numbers to potential thieves.
- Many police departments aren't trained to deal with this growing problem.
- Many state and federal agencies will not prosecute cases if the stolen amount is less than $25,000 or $50,000.
- It is a low-risk, high-return venture for thieves since few are ever convicted.

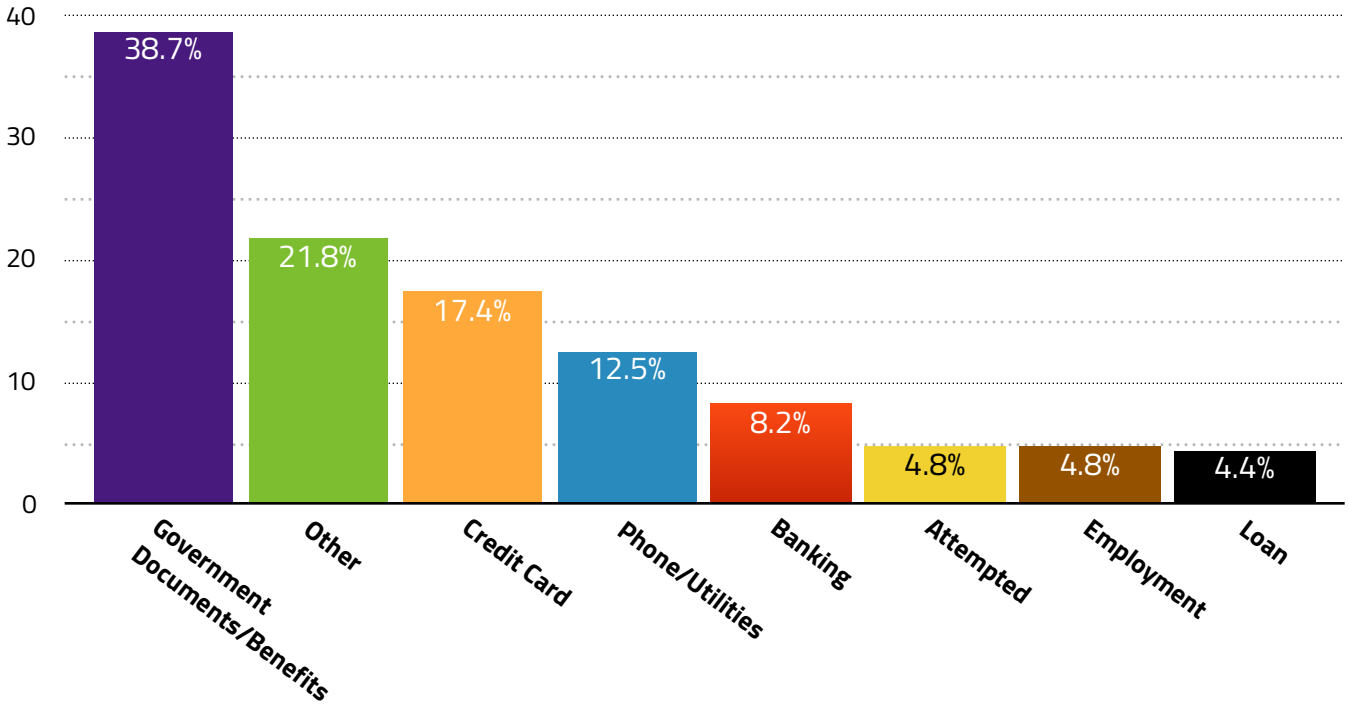
Although identity theft has become more common, you can protect yourself using the techniques outlined in this course and by staying informed about emerging threats to the safety and security of your personal information.

Impact on Victims

Identity theft can damage your lifelong good credit rating, as well as setting you back financially. It is estimated that 7% of the U.S. population were victims of identity theft in 2014. On average, approximately $4,500 was stolen from those victims (plus out-of-pocket expenses to clean up the mess). However, there can also be a considerable emotional toll. As with other crimes, victims often feel violated.

Unlike other forms of stealing, the damage from identity theft can last for years. Even if you repair your credit, it can be attacked again. Once an identity thief has your Social Security number, it can be abused again at any time.

Types of Fraud



Graph: *Of reported identity theft, what type of fraud is committed with the information?*[1]

An identity thief, armed with personal data, can:

- Obtain credit cards or loans in the victim's name
- Siphon money from bank accounts and other investments
- Acquire life insurance in the victim's name (and make themselves the beneficiary)
- Receive medical care using the stolen identity
- Steal the victim's disability, Social Security, or unemployment benefits
- Obtain the victim's tax refunds
- File bankruptcy in the victim's name

Being aware of the common types of fraud can help you protect your identity.

Credit Card Fraud

Many people believe that the greatest risk of credit card theft is through online stores. While your credit card numbers used online do need to be secured, this is not the only way for thieves to access your information. One trick is the "skimmer," a physical device that can read the card's information embedded in the magnetic strip on the back. These devices have been found everywhere a card could possibly swiped, from gas stations, to ATMs, to gadgets concealed in the clothing of a dishonest restaurant waiter!

Another common way thieves access sensitive credit card and personal information is when you apply for a loan or other credit. An employee at the lending company can copy personal information and use it for their own financial gain or sell it to others.

---

[1] Source: https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf

Employment ID Theft

A thief with someone else's personal information can use that person's business background and credentials to secure employment or receive employment benefits. This is often done in a different region or state than where the victim lives. You may have no idea it's happening for months or even years.

Medical or Tax ID Theft

If a thief has your Social Security number, they can secure medical coverage or obtain benefits under your name. They can also file a tax return immediately on January 1st and collect a fraudulent rebate check before you even file your legitimate taxes.

In the summer of 2015, the IRS discovered their poorly-designed website for retrieving tax filing information made it simple to steal the identity of several hundred Americans[1]. Because the login relied on trivial security questions that could be researched elsewhere, the information was not actually secure and the IRS removed the site. But before the breach was discovered and closed, an estimated 334,000 had personal information stolen from the site.

Child Identity Theft

Although your child may be too young to have a credit card, that doesn't necessarily stop someone from stealing their identity. With your child's social security number on school, insurance, and medical forms, they are just as susceptible to identity theft as an adult. A child receiving social security benefits might have them directed into someone else's account, someone could claim your child as their dependent, or you could receive bills or notices in your child's name.

If you suspect suspicious activity in your child's name, contact the three credit bureaus listed later in this workbook. Request a manual search under your child's name and SSN, since a normal online request would fail because of their date of birth. The search should come back empty while your child is a minor.

For other steps you can take to protect your child, visit the FTC's website on child identity theft: **www.consumer.ftc.gov/articles/0040-child-identity-theft**.

Synthetic ID Theft

An emerging form of identity fraud, **Synthetic ID Theft** takes information from several legitimate consumers and combines it into a new, fake identity. For example, a criminal might take the birthdate of Jane, the SSN of George, the address of Diane, and the phone number of Mitchell. Since any one person is only a piece of the fraud, this can be extremely hard to detect and clean up. Not every credit database has the sophisticated checks necessary to verify that all the given information on an account fits together.

Along with the normal steps you take to prevent identity theft, pay particular attention to your annual Social Security statement. If your SSN has been used to apply for another job, your wages will appear inflated, and you should pull your full credit report[2].

---

[1] http://www.pressherald.com/2015/08/17/irs-identifies-more-potential-victims-of-website-breach/

[2] https://www.protectmyid.com/identity-theft-protection-resources/types-of-fraud/synthetic-identities.aspx

Banking Scams

Not all banking scams begin with withdrawals. Thieves can deposit counterfeit checks into a victim's bank account, then write checks from that account before the original fraudulent checks are discovered. This form of identity theft could cost a victim thousands of dollars. In some reported cases, the bank first considered the victim as either the perpetrator of the crime or an accomplice to it.

Identity Theft to Avoid Prosecution

People go to great lengths to avoid the law, including committing identity theft. Identity thieves often give false names when arrested. The victim might not know anything about the crime until he or she is arrested from a bench warrant. Further, many people don't know that a large percentage of identity theft fraud is perpetrated by someone they know: a friend, an acquaintance, a family member, or someone who has ongoing access to a residence, such as a housekeeper or maintenance worker.

Who May Be An Identity Thief?

It is important to realize that 68% of identity thefts are committed offline (i.e. not via the Internet or some other electronic information source), according to Javelin Strategy & Research. While the identity thief is often portrayed as a criminal who steals mail or a computer hacker who accesses online databases, family members and workplace insiders often commit identity theft.

Family Members

Identity theft committed on and by family members is more common than most realize. Javelin Research & Strategy's 2014 Identity Fraud Report concluded that 847,000 identity theft victims knew the thief[1]. Family members can be easy targets:

- The thief knows that the family member will be less likely to press charges
- It is easy for the thief to get access to a family member's personal information.

Workplace Insiders

Many identity thefts are conducted by employees within companies such as cell phone providers. Whenever a Social Security number, date of birth, and an address are provided to initiate an account, your information is at risk. Personal information is usually shared with other parts of the organization, introducing the potential for someone to steal data. Criminals have been known to work for temp agencies to gain access to confidential information.

[1] https://www.javelinstrategy.com/brochure/314

Methods of Identity Theft

Identity thieves require little more than a name and Social Security number (plus perhaps the date of birth) to assume another person's identity. They use a combination of old-fashioned misdirection and high-tech ways of obtaining personal data online. Remember that thieves dream up new methods as quickly as we can uncover them.

Here are some common methods of identity theft:

Mail Theft

Before online shopping took off, many identity thefts occurred by intercepting your mail. Thieves would steal incoming and outgoing mail from home mailboxes. Favorite pieces of mail include credit card offers, credit card and bank statements, ATM cards, and check orders delivered from your bank.

Call from "Security"

The caller says they are from the security or fraud department of Visa or MasterCard. They ask if you purchased some random expensive item. After denying you made the purchase, the caller offers to credit the account and begin a fraud investigation. They ask you to verify that you have the card in your possession by reading off the last three numbers on the back of the card, which is the unique "card verification number".

Many consumers are fooled by this scam because the caller never asks for the credit card number. That's because they already have the credit card number from another theft, perhaps from skimming. They need the card verification number to make online and phone purchases. Your credit card company already has all of your information, so If they need to verify anything, they will read the information to you

If you ever get a call like this, hang up and call the phone number on the back of your card to verify the authenticity of the caller. If the initial call was fake, reporting that phone number to your credit card company may help them track down the scammers.

ATM or Credit Card Skimming Devices

Identity thieves can steal customer information by setting up skimming devices at Automated Teller Machines (ATMs). They alter ATM machines to swipe your credit card information while you swipe the card and complete your transaction. It is also possible for wait staff or retail store employees to steal credit card information with a skimmer.

Before using an ATM machine, make sure it appears to be functioning normally. If the machine looks like it has been altered or there is a sign that asks you to swipe your card in another location first, do not use it. Try to use the same few ATMs when you withdraw cash so you will notice any change that's made to them.

When handing over a credit card, keep the card in sight at all times. This is not easy to do in many restaurants, so use a credit card to limit your liability.

"Free" Credit Report Emails

Ignore these emails. Most, if not all, "free credit report" emails are scams. The aim is usually to obtain Social Security numbers. (Note: even the legitimate "free credit reports" charge you for the service at a later time unless you remember to cancel the subscription in a timely manner.) You are entitled to a free credit report from each of the three credit reporting agencies (Equifax, Experian, and TransUnion) once per year. Just complete the form at **www.AnnualCreditReport.com**.

Phony Identity Theft Protection

This is the same tactic as the free credit report email scam. In this ironic tactic, thieves convince unsuspecting consumers to give up their personal information by offering to provide identity theft protection.

Questions from a "Friend"

If you use social media or blogs, do not divulge personal details or history that can be used against you, even if it seems harmless. In this scam, thieves monitor social media for personal details. They start a social media account that duplicates the pictures and information from someone you know and they request to add you as a friend. If they contact you, they may be evasive with their information but ask you for personal information that can be used to guess other passwords, such as where you were born, your mother's maiden name, your birthday, etc.

Under no circumstances should you respond to questions like this online. Even if you think you are giving away harmless information or speaking to your friend, you may inadvertently give away information that could be used against you. If it really is someone you know, there are other ways to contact them and verify who's chatting.

In-Store Security Scams

A person representing themselves as in-store security asks for your help to catch a dishonest employee. He asks your to fill out a credit application and give it to the alleged-dishonest employee. If you are ever approached in a store, make sure that any employee who approaches you has proper identification. Do not use paper forms in a store to apply for credit under any circumstance.

Job Advertisement Scams

Never provide a Social Security number to a phone interviewer found through a classified ad without an in-person interview unless you have verified the legitimacy of the company and interviewer. If the ad looks suspicious or provides inconsistent information, be careful.

For example: "Project Manager at ABC Systems, email Tom at tsmith43@gmail.com." Why is this person using a Gmail account and not an ABC Systems email account?

Call the company directly using a phone number found on their website and ask for the interviewer. You may find that there is no Tom Smith at ABC Systems. If the company doesn't have a website, call the Better Business Bureau or state attorney general to make sure the company is legitimate. Report the scam if the company is not legitimate.

Don't give out any personal information until the source is independently verified.

Other Money Scams

There are other kinds of scams that don't involve identity theft directly but can lead to problems down the road. All of these scams share one thing in common: they rely on the victim's naïveté or greed. Here are just a few examples:

Nigerian 419 Scam/ African Email Scam/ Lottery Scams	These scams have been around for as long as the USPS has been delivering mail. The story goes that the sender must transport a large sum of money and needs your help, for which they offer a financial reward or cut of the money. You're asked to contact the sender to express interest. Once you respond, they may ask for a "transfer fee" or perhaps your financial information to wire payment to you. As time passes and you are waiting for your "reward," they ask for additional sums of money to expedite the process. These letters originally mentioned Nigeria or some other African nation. Now they can come from anywhere, usually an exotic-sounding locale. These letters can also take the form of a lottery from a foreign nation. The same principles apply: you have won millions of dollars, give us a call and it is yours. Except when you call, you have to hand over a "transfer fee" to get the money or all of your personal information to complete a "tax form."
"You Have Won A Free Gift" Scam	You receive a phone call or email about a free gift or prize. Just provide the caller with your credit card or banking information and the gift is on its way! Many of these companies will then send you some cheap item that is worth far less than the shipping cost (if you receive anything at all) and rack up other fraudulent charges or worse.
Email Chain Letters/ Pyramid Schemes	These are pyramid scams and are usually illegal. Many say that you will receive money from each person who comes after you in the chain. Follow the instructions and your financial rewards will come to you. Just send cash. Do not respond to or forward these emails. At best, you will annoy your friends and family. At worst, you will lose money.

Phishing

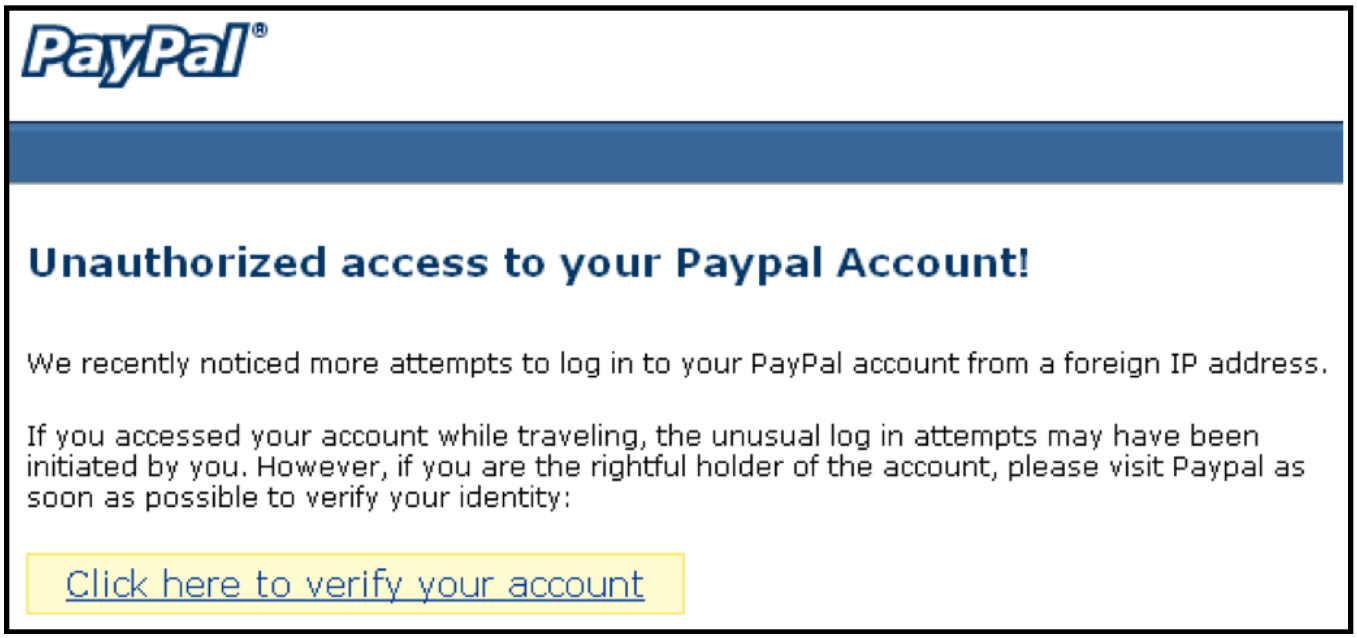
Phishing (and more destructive flavors like spearphishing) is today's fastest growing identity scam. It deserves special mention because it is so common.

Phishing is the slang term for fake email messages that appear to come from a legitimate source, perhaps a company with which you do regular business, but are actually sent by criminals attempting to steal your information. These thieves "fish" for information from thousands of potential victims using emails designed to trick you into divulging personal information, such as passwords or credit card numbers. These deceptive emails may also ask you to verify account information and Social Security numbers. Phishers will often steal a financial institution's email or website design and trick you into accessing bogus banking and e-commerce websites.

Many scammers send an "important message from the system administrator" requiring immediate attention to your account. Almost every well-known company has had its name used by phishers in their quest for personal data.

Typical Phishing Scam Process

Many of these emails contain an institution's logos, colors, and other design elements, and include a legitimate link to the company or bank's website somewhere in the message. The subject line of many of these emails reads like an urgent message. Some messages ask you to reply to the message with personal information to safeguard the account or to click on a link to reset your password. Some emails will threaten to suspend your account if you don't act soon. An example from a fraudulent PayPal email:



The link may look legitimate, but the text in the link can say anything! It is where the link actually goes that matters. When you access the site through the link in the phishing email, the site looks like the PayPal site, but it actually belongs to the phisher. The only indication that this email is not legitimate is if you had hovered over the link to reveal the site it will actually take you to. In this case, it would be something random like **http://moneygrampay.pl/password** instead of **www.paypal.com**.

Clues You Caught a Phish

Deceptive websites can come in many forms.[1] You must hover your mouse over any links in the email to see where they will take you. If you click on the link, you can also take a look at the address in your browser, but your computer may have sent a message to the spammers that your email address is correct, inviting even more spam messages!

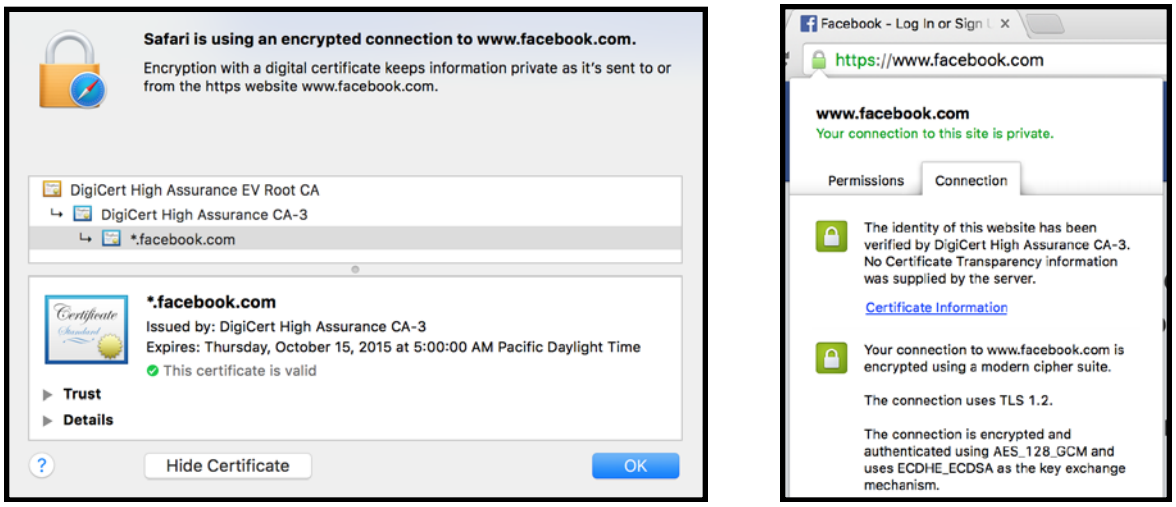
Some things to look for in the hyperlink include:

- A different suffix (i.e. instead of the legitimate address such as **abcbank.com**, the scammers use abcbank.net or .tv, .ru, .pl, etc.)
- A deliberately misspelled name (i.e. **abcbanc.com**)
- Extra words in the company name (i.e. **abcbankaccountinfo.com**)
- It can be extremely hard to notice, but sometimes an address may use letter substitutions that blend in. For example, capital "i" instead of a lowercase "l"
- Using foreign domain names in creative ways (**abcba.nk**)

Confirm You're On a Legitimate Site

If you do click on a link, make sure that the site is the actual address of the company. Anything else is probably a fraud. The notification email and official website URL will never have any misspellings. Fraudulent emails and sites frequently have typos, bad grammar, or odd phrasing. They may contain the word "urgent" or rush you in some way.

On any page requesting personal information or a login, the official URL should begin with the prefix "https," which denotes a secure connection. A secure site will also use a certificate from VeriSign, Digi-Sign, or another well-known company that issues security certificates to websites. Most modern web browsers will display a lock icon in your address bar when you have a secure connection, and clicking that should provide more information about the certificate that was issued.



Examples from Safari and Chrome.

Most importantly, it is very unlikely that a legitimate organization will solicit personal information in an email because they don't want their customers to confuse a phishing email with a genuine communication.

[1] Some guidance from **http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx**

How to Respond to Phishing

If you receive a suspicious email, don't access any websites provided in the email. Instead, visit the company or bank website directly through a major search engine, a bookmark you created previously, or a URL you know to be correct. This will prevent you from inadvertently logging into the fake website.

If you receive a suspicious phone call, hang up and contact the firm directly using the number on the back of your card or another contact number on the bank's website. Ask the customer service representative if the call you got was legitimate.

Although they can't fight back directly, companies may request a copy of the email for their own research or to help warn customers if the phishing becomes widespread. Customer service may be able to give you an address to forward those messages to. Don't copy-paste the content of an email into a new email because that removes valuable information that can help a company track where spam is coming from.

The Cost of Identity Theft

Clearing up your identity once it has been stolen costs time and money. Financial liability for charges made to accounts can be limited if issues are reported quickly.

Credit Cards

For credit cards, the maximum amount you can be penalized is $50 per card. If the credit card is reported lost or stolen before it is used, you will not be held responsible for any unauthorized charges on the account.

ATM and Debit Cards

Be very careful with ATM and debit cards. They do not carry the same level of security as credit cards. If unauthorized charges are not reported within a timely manner, you could be held liable for the charges. And since the card ties directly to your checking account, crucial money you would need to pay bills could be frozen while the fraud is investigated. Here is a summary of the rules governing reporting and potential losses:

If You Report the Theft or Loss:	Your Liability Is:
Before the Card is Used	No charge
Within Two Business Days	$50 maximum liability
Between Two and 60 Days	$500 maximum liability
After 60 Days	All the money taken out of an account

Although this is how the law is written, it's extremely unusual for you to be liable for any more than $50 in fraudulent transactions. Visa and MasterCard extend traditional fraud protection and guarantees to debit cards, so you shouldn't be liable at all.

Stolen Checks

Banks are responsible for losses from forged checks in most states. But if the bank is not notified of stolen checks in a timely manner, you could be held liable for any losses.

✓ EXERCISE

Match the scam or potential identity theft with the corresponding letter below.

1. **You get an urgent email from your bank asking you to update your account.**
   A B C D E F G
2. **You get a message from an old friend asking for personal information.**
   A B C D E F G
3. **The fraud department of ABC Bank calls and asks for your Social Security number.**
   A B C D E F G
4. **You receive a credit card you didn't order and some bank statements are missing.**
   A B C D E F G
5. **Your credit card information is taken by an employee or altered ATM.**
   A B C D E F G
6. **You reply to a help-wanted ad and they ask for your Social Security number.**
   A B C D E F G
7. **You receive a free credit report offer via email.**
   A B C D E F G

	Scam or Potential Identity Theft
A	**Call from "Security":** Hang up and call the institution directly.
B	**Mail Theft:** Get a P.O. Box for your mail. Put sensitive mail directly into a post office collection slot. Consider online bill payment options.
C	**"Free" Credit Report:** Contact the credit bureau directly. Ignore these emails.
D	**Phishing:** Go directly to the company website or call the number on your card.
E	**Job Advertisement Scam:** Don't provide any sensitive information until you've had a personal interview to verify the company's legitimacy.
F	**Questions From a "Friend":** Don't share personal information with anyone online.
G	**Skimming:** Don't use ATMs that appear tampered with.

Answers can be found on page 32.

Identity Theft Legislation

The federal government has taken action to combat the increasing problem of identity theft. The FTC is constantly working with financial institutions to draft guidelines and legislation to protect and inform consumers.

The Fair & Accurate Credit Transactions Act

The Fair and Accurate Credit Transactions (FACT) Act was passed in December 2003. It took strides to address the problem of identity theft. Specific accomplishments include:

- Retailers may print no more than the last five digits on credit card receipts.
- Consumers may obtain one free credit report a year from each of the three credit reporting agencies and may dispute information on their credit reports.
- Businesses are required to provide victims with fraudulent transaction records.
- Companies are not allowed to ignore any fraud alert.
- Improvements in 2008 also require banks/credit unions to be more proactive in preventing, detecting, and reacting to identity theft, known as the Red Flags Rule[1].

Identity Theft Penalty Enhancement Act

The Identity Theft Penalty Enhancement Act of 2004 adds two years to prison sentences when criminals use stolen personal data or credit card numbers to commit crimes[2]. The act was designed to dissuade criminals from ever attempting the crime, but has had little impact on the rate of identity theft.

Identity Theft Enforcement and Restitution Act

First passed in 2008, this act and amendments clarified that the victim's time spent cleaning up the mess left by identity theft can be included in restitution amounts. It also makes identity theft a federal offense, even if both the perpetrator and victim live in the same state. Previously, state lines had to have been crossed for federal prosecution.

State Financial Information Privacy Laws

Some states have enacted their own financial privacy laws. Check with your state authorities for up-to-date information about local laws or visit the FindLaw listing for your state: **statelaws.findlaw.com/criminal-laws/identity-theft.html.**

Still Cause for Concern

According to many consumer groups, while new federal and state laws are a step in the right direction, identity theft crimes will still be committed. The reasons for this include:

- Law enforcement's resources are already stretched thin. They don't have enough resources to go after identity thieves.
- Identity theft is increasingly becoming an international, organized crime, with gangsters setting up spambots and websites in countries like Russia, China, and India. In these areas, prosecution is difficult and governments aren't equipped to deal with the problem.

Prevent Identity Theft

[1] https://en.wikipedia.org/wiki/Red_Flags_Rule

[2] http://www.identityguard.com/identity-theft-resources/articles/punishments-for-id-theft/

There are many simple and effective steps you can take to avoid becoming a victim of identity theft. Here are some essential preventative measures.

Check Your Credit Report Annually

The most important action you can take to prevent identity theft is to check your credit report once a year, at a minimum. If you monitor your credit report regularly, you will be able to notice any sudden changes in your credit or payment history. In addition, check your credit several months prior to applying for a loan since it can take a while for any errors to be corrected, impacting your credit score.

You can get a free annual credit report from all three credit reporting agencies through **AnnualCreditReport.com**. If you find an error in your report, call the credit agency to report the error. Be sure to keep notes on any conversations you have with the agency.

Credit reporting agencies offer "credit monitoring" services for a small annual fee. The agency will notify you of any negative credit reports they receive to your credit file. If you decide to sign up for this service, make sure it covers all three credit reporting agencies.

Review Monthly Statements

It is important to review your monthly bank and credit card statements and look for any unauthorized activity. Report and resolve unrecognized charges as soon as possible.

Read and Respond to Privacy Notices

Many companies, especially credit cards, are required to issue annual privacy notices. These notices usually contain information on how to opt-out of the financial institution sharing information about you with their other companies or even 3rd parties.

While banks and other large financial services companies view sharing information (particularly throughout different parts of the company) as a positive thing for consumers, some consumer advocates are concerned this information could fall into the wrong hands. You have the right to stop financial services companies from sharing information through these opt-out forms.

Privacy policies are sometimes difficult to decipher. Look for the phrase "affiliated companies" and specifically communicate that you do NOT want your private information shared with anyone, including any "affiliated companies."

Protect Your Credit Cards

There are several actions you can take to reduce credit card fraud:

Configure and Use Apple Pay

Modern Apple devices offer to securely store your credit cards in a digital wallet. This information is never stored in the cloud and provides a unique, one-time-use code for each transaction you make. Your actual card number is never shared during the transaction, making it an extremely secure way to purchase items.

Use Apple Pay any time you have the opportunity to do so since, even if that card number is stolen, it's a virtual card number which can't be used again. If fraud occurs to your credit card number through another source, Apple Pay will often update with the new card number before it arrives in the mail. You may also receive notifications on your device after a transaction, even with your physical card, reminding you the cable bill just got paid or warning you that your spouse just bought some expensive concert tickets.

Note about Android Pay: Some Android phones offer a similar feature called Android Pay. However, this service stores your card number in the cloud and authenticates with as little as a pin code rather than a fingerprint. If you choose to set up Android Pay, consider the privacy implications of the service and use a complex password.

Use Chip and Signature for Transactions

Although they've been a fixture overseas for nearly two decades, EMV-chipped debit and credit cards only recently became common in the U.S. Since October 2015, retailers are now more liable for fraudulent card transactions if they've failed to install credit card terminals that accept chipped cards.

Like Apple Pay, a chipped credit card transaction relies on a one-time-use code rather than your normal credit card number. Instead of swiping your card, you place the chipped-end of the card into a slot at the base of the card terminal. Then you enter your pin or sign to complete the transaction as you normally would.

Use the chip-and-signature option wherever you have the chance so the retailer can't "misplace" your credit card number and expose you to possible fraud down the road.

Reduce Mail Fraud

- Ask your credit card company to stop sending blank, promotional checks.
- Opt-out of pre-approved credit offers. In addition to filling your mailbox, they are an easy target for thieves. Credit bureaus offer a toll-free number or website to opt out of all offers in just minutes. Visit **www.optoutprescreen.com** or call (888) 567-8688.
- If your credit card offers it, add your photo to the card.

Watch Your Wallet

Make photocopies or record the information from all credit, bank, and ID cards that you keep in your wallet. If your wallet is stolen, it will make it much easier to know what is missing and report it more rapidly. Keep this information in a secure (and separate) location. Carry only items in your wallet that you really need. Never carry your Social Security card in your wallet.

If you travel, pack a list of 800 numbers for all of the bank and credit cards you are holding. Do not place this list in your wallet or purse; keep it in a secure location.

Use Personal Checks Safely

Remove your full name from the face of personal checks. Only include your first and middle initials such as "J.B. Fletcher." Identity thieves won't be able to tell if the account belongs to a man or woman or prove that they are an owner of the account. They also won't know whether your signature includes your full name or just your initials.

The only information on your checks should be:

- Post office box or business address
- Cell phone or work number

Your checks should not have the following information printed on them:

- Home address
- Home phone number
- Social Security number
- Driver's license number

When making purchases, consider using a credit or debit card to speed up the transaction and provide additional security. Reserve checks for mailed payments or other unavoidable transactions like paying loans, rent, or a small business. Consider using online bill pay services through your bank to mail checks for you.

Shred Documents

Experts say that thieves are more likely to steal your personal identity by going through your trash than through the Internet. For as low as $50, buy a cross-cut shredder and use it. Shred any sensitive documents before disposing of them. In particular, be sure to shred pre-approved credit card offers you receive in the mail so that thieves cannot steal them out of your trash. Don't forget to shred deposit slips, too, as they have your account number on them.

Secure Your Mail

Get a P.O. Box and use it for all your incoming mail. This will prevent your mail from being stolen by a passer-by. Send outgoing mail containing checks and other sensitive information directly at a U.S. Post Office using a mail slot that deposits inside the building. Don't leave them in your mail box or sticking out of a mail slot.

Protect Your Private Information

Never give out information to someone who telephones you. Ask for the name of the organization that needs the information and call them back at a number you have looked up yourself (not one given to you by the person who just called you). For example, if your bank calls asking for your Social Security number, ask what the call is regarding and call them back at the phone number listed on the card or statement.

Many institutions are backing away from using Social Security numbers for identification purposes. Ask providers that are still using your Social Security number to stop using it, and ask for a new identification number from the company.

Medical Information

The medical community trails financial institutions in safeguarding your security, as evidenced by several massive breaches and disclosures from insurance companies. Social Security numbers are often still used as a means of identifying patients so these breaches can be particularly devastating. You can improve your awareness of these problems and reduce your personal exposure by following some basic steps:

- Read all privacy notices before receiving any medical care
- Refuse to allow your Social Security number to be visible in uncontrolled places, such as on wristbands or unmonitored medical charts
- Ask that your name and condition not be released if you are hospitalized
- Review and copy your medical records
- Ask providers to correct any errors, although they aren't required to make changes
- Ask for a list of medical information that has been distributed to third parties
- Don't verbally provide confidential information if it might be overheard by others

Do Not Call Registry

Sign up for the National Do Not Call Registry at **www.donotcall.gov**. This will prevent most telemarketers from calling you. It takes three months for the calls to cease. If you receive a call that you think is from a telemarketer after that time, file a complaint with the government on the website.

Some institutions are still allowed to call, including:

- Charities and research surveys
- Political campaigns

The Direct Marketing Association operates the Mail Preference Service to opt-out of a variety of junk mail and catalogs. See their web site for details: **www.dmachoice.org**.

Request a Security Freeze

One of the most effective ways to eliminate identity theft is called a security freeze (a.k.a credit freeze or credit lockdown). Nearly every state has instituted a law allowing it. All three credit reporting agencies—Experian, TransUnion, and Equifax—allow you to freeze your reports online, regardless of state law, although you must contact each separately.

The security freeze allows you to prevent others from accessing your credit reports without your permission. When you freeze your file, nobody—not even you—can use it to open new credit accounts. This prevents a thief from gaining credit in your name since no one can check your history. The only way to gain access to a frozen credit file is to call the credit bureau and supply a PIN code.

Remember, freezing your credit freezes it regardless of who asks for the information, impacting your ability to intentionally apply for new credit. It will hamper or delay applications for mortgages, rentals, credit cards, cell phones, utility services, as well as some job applications.

To freeze your credit file, visit the Experian, Equifax, and TransUnion websites. Most state laws allow for a small fee to freeze or unfreeze your file, but the procedures are different in every state. Read much more about security freezes at **www.creditcards.com/credit-card-news/credit-report-freeze-1282.php**.

Safeguard Your Computer

Virus Protection

Install and regularly update virus protection, anti-spyware, and firewall software. This will help keep personal information stored on your computer safe from online thieves.

While newer versions of Windows (8.1 and higher) include antivirus software already, this only provides basic protection against malware and other advanced threats. Consider purchasing a complete internet security suite from reputable companies like Norton, McAfee, or Kaspersky. Your ISP may also offer an internet security subscription for free with your monthly service. Visit their website to investigate this option.

Email Attachments

Be extremely cautious about opening attachments in emails. A popular way of infecting your computer is a combination of spam/phishing emails with a file attachment claiming to be an account statement or other information. Discard these immediately.

Data Storage

File Storage

Password protect any file that contains sensitive data. While a password on a Microsoft Office document provides minimal security, it will prevent someone from casually snooping through your files. Investigate using encrypted disk images on your Mac or encrypted zip files on your PC to securely protect files you place inside. These are a better way to protect financial documents.

Disk Encryption

Disk Encryption protects data at rest. That means the files stored on your computer are protected if it were stolen or physically tampered with. This doesn't improve your security when transferring the data over the internet, but it is an important step to take on laptops, especially for business travelers who are constantly taking their laptop to different cities and countries.

If you have a modern PC running Windows Professional or a Mac running newer versions of Mac OS, drive encryption is available to you for free with very little impact on the performance of your computer. PC users should look for more information on BitLocker, while Mac OS users should investigate FileVault.

If you encrypt your drive, you will be given some type of recovery key to enter in case you lose or forget the password to unlock the drive. This is the only way to ever unlock the data on your drive, so be sure to keep that information in a safe place like your password manager or a safe deposit box.

Computer Disposal

When it's time to dispose of your computer, make sure all the information on your hard drive is permanently erased. You can bring it to a recycling facility to have it physically destroyed for a small fee. The facility will provide a certificate of destruction confirming your data is no longer accessible. If you are more tech-savvy, a bootable program like Darick's Boot and Nuke (DBAN) will completely overwrite the data on your drive one or more times, preventing it from being accessed again. Visit **www.dban.org** to download.

Ad Blockers and Secure Connections

Advertisements are so common you may already tune them out. But what started with relatively tame but annoying pop-up ads has blossomed into something much worse, and even possibly malicious. In addition to being a distraction and tracking your activity, ad networks are becoming a way to distribute viruses to your computer.

You may have had the experience of searching for a particular item over the course of several days, only to have that item start appearing in ads on different websites. Those ads may all be powered by one ad network and a tracking cookie on your computer is monitoring what websites you visit and what you do on those sites.

As if the privacy problems weren't disconcerting enough, thieves and bad actors have latched onto the fact that ads are everywhere and powered by only a few different networks. They can buy a "normal" ad on the network and later change the ad to install software on your computer through a security hole. Now you have a virus from an ad!

Consider running an ad blocking plugin in your web browser to prevent these ads, both malicious and legitimate, from ever loading or tracking you. Most web browsers will offer one or more of the following popular blockers:

- Ghostery: **www.ghostery.com/en/try-us/download-add-on**
- uBlock Origin: **https://github.com/gorhill/uBlock**
- Adblock: **www.getadblock.com**

Secure Browsing With the Electronic Frontier Foundation

The **Electronic Frontier Foundation (EFF)** is a nonprofit committed to civil liberties in the age of the internet. In addition to creating, exposing, and fighting legislation through court proceedings and lobbying, they also offer tools to stay safe online.

Privacy Badger
www.eff.org/privacybadger
Working hand-in-hand with your ad blocker, privacy badger prevents third-party trackers from monitoring your activity on websites. You can click on the icon when you visit a website to see how many trackers were stopped.

HTTPS Everywhere
www.eff.org/https-everywhere
While most websites now offer a secure connection, not all of those websites are great at directing you to the secure version. The HTTPS Everywhere plugin automatically requests a secure connection on websites that have it available. This protects your pasword from being casually sniffed while browsing on public networks.

Some of the ad blockers and EFF tools listed above are also available on mobile devices. If you have an Apple device, make sure you're running iOS 9 or greater, which adds support for content blockers. Search the web or your app store to see what options are available for your device.

Create & Store Passwords

If there is one behavior almost everyone needs improvement on, it's creating and managing secure passwords across various websites. Simply put, there is almost no way to create a unique password that is memorable to you, unique to every website, and difficult for a hacker to exploit. Many resort to storing passwords on sticky notes or using the same password everywhere, but these habits put your personal information in jeopardy. You should understand what makes a "good" password to create a few you'll need to memorize, then select a password manager to do all of the hard work for you.

What Makes Passwords Secure

The formula for deciding what makes a great password is simple:

Length × Complexity = Security

You've likely heard every combination of truth and misinformation about what should be in your password. Symbols! Numbers! Upper and Lower Case! Who can fit all of these into a password they can remember? We'll provide a formula you can use to generate your own complex passwords and then explain why you should use those sparingly.

Responsible password requirements increase constantly, but there are some goals to keep in mind when building a complex password today:

- The single-most-important feature of a password is length. Create a password that is at least 16 characters, but try to get above 20 for additional security.
- Since length is more important than complexity, a full sentence is more secure than a short phrase full of symbols. Compare "MyVoiceIsMyPassword" to "$3Cur#." Which seems more secure?
- Don't incorporate any numbers of personal significance (birthday, anniversary, PIN, birthday of child, etc.).
- It's not an issue if you follow the direction of this workbook, but certainly never use any of the worst-possible, most-common passwords. Common offenders include "123456" and "password." One such list can be found at **splashdata.com/splashid/worst-passwords/**.
- **Never use the same password on another website; Each website should have its own unique password.** This is because when one website is hacked, the attackers will often use those account passwords to try to access other websites. If you've used the same password on multiple sites, thieves could access those accounts.

Example Secure Password Formula

The only memorable passwords you need to create are the passwords to unlock your password manager (discussed later) and passwords you may need to enter while the manager is unavailable, such as unlocking your phone or logging into email.

For these passwords, you'll want to incorporate all of the factors mentioned above but still have a password you can remember easily. How it this possible? You can rely on a password formula to create memorable bits and phrases you put together to create a password. We've developed two example formulas for you to try out to improve your own passwords. Experiment with the ideas presented and add your own twist.

Example 1: Secure, Memorable, Salted

In computer science, a **Salt** is a word, phrase, or code added to your password while it is stored on a company's server. This increases the length of the password, improving the security when it is encrypted on the site. We'll use salts to build complex, memorable passwords you can use on the accounts you absolutely must remember passwords for. Combine the following factors to build a secure password:

1. A symbol
2. Your initials, lowercased
3. The site or service this password is used for, capitalized
4. A code word only you would know. Try to avoid things like childhood nicknames and focus on a memorable, but random, word
5. Some additional numbers, but never anything like your birthdate or anniversary

Here are some examples of the types of password this formula would create:

- !jsCHASEbutterfly9521
- *msPG&Edaisy1076
- &dmEBAYjupiter2936

This may seem intimidating, but keep in mind that the only portion changing is the company name, underlined in the examples above. The rest of your password would remain the same for each website you use it on. This allows you to make very long passwords that are still memorable because you can remember each piece of it.

Example 2: WordsWordsWords

Remember that real security comes from length rather than complexity. With that in mind, a password composed of little more than a sentence is much more secure than a short, complex one[1]. Consider using a memorable phrase, capitalizing each word, and removing the spaces. You may need to substitute a symbol for each space to satisfy password requirements on websites that are trying to protect you from yourself!

- TheSkyIsSoBlue
- EarlyToBed$Early$To$Rise

Two-Factor Authentication

Two-Factor Authentication (2FA) means that when you try to login to a website with your username and password, you'll also need to provide a code the website sends to you, usually by email or text. This code is your "second factor," meaning that a criminal would need both your password and your email account or cell phone to successfully break into your account. This dramatically improves the security of your account, so consider enabling it on every website that offers it.

Rather than sending a text message or email to authenticate you, some companies also support a physical 2nd factor called a Yubikey. Think of this just like a normal key you would use to open a physical lock, but this one helps you unlock websites you visit. You need your password AND the key to login. Learn more at **www.yubico.com.**

For a list of websites with 2FA support, visit **www.twofactorauth.org.**

[1] https://xkcd.com/936/

Password Managers

The key to securing accounts online is a password management app that creates and stores complex passwords you couldn't possibly remember. These programs can generate infinitely-complex passwords and can often audit them in case a hacker breaches a website. Those passwords are stored in a secure, encrypted vault you unlock with one final password, the only one you need to remember in the future. Important accounts like those for your bank or healthcare should be completely random; they should be so secure you don't even know the password yourself!

Here are some popular apps to consider, all at a very low cost:

1Password by Agilebits
www.agilebits.com/onepassword
Store passwords, secure notes, software licenses, credit cards, and more in a secure vault on your computer, Dropbox, or iCloud. Their Watchtower service will alert you to passwords that have been compromised. Also supports two-factor authentication tokens.

LastPass
www.lastpass.com
Free to use on just one device, LastPass stores your passwords and other information in a secure file on their servers. Their $12/year premium service allows you to sync this information across all of your devices. They partner with some websites to allow you to automatically change your passwords in the event of a breach or on a regular schedule.

KeePass
www.keepass.info
Recommended only for advanced users, this free and open-source program offers basic password management and secure note storage without the user interface or support of the other two programs. You are responsible for storing your vault on your computer or network drive.

While it is a good practice to have a memorable password for your phone and the cloud account you would need to login to restore your password vault, consider making all of your other passwords random and stored in a password manager.

✓ EXERCISE

For each ID theft prevention strategy, decide which attacks it protects against. Some strategies may have multiple answers since they protect against various attacks.

1. **Get a P.O. Box**
   A B C D E F G H I
2. **Opt-out of junk mail like pre-approved credit cards and catalogs**
   A B C D E F G H I
3. **Use only official collection boxes or the Post Office for sensitive mail**
   A B C D E F G H I
4. **Check your credit report regularly**
   A B C D E F G H I
5. **Shred sensitive documents**
   A B C D E F G H I
6. **Use secure passwords**
   A B C D E F G H I
7. **Record the contents of your wallet**
   A B C D E F G H I
8. **Use internet security software with an active subscription**
   A B C D E F G H I
9. **Don't divulge personal information in chat or email**
   A B C D E F G H I
10. **Don't reveal personal information in public areas where it could be heard**
    A B C D E F G H I

	Protects Against
A	Mail theft
B	A thief figuring out or cracking your passwords and PIN codes
C	A thief going through the trash and finding information
D	Employees or eavesdroppers overhearing your Social Security number
E	Hackers accessing your computer and personal information
F	Being confused about what's missing if your wallet is lost or stolen
G	Unwanted accounts being opened in your name
H	Someone gaining sensitive information about you
I	Large volumes of sensitive mail that could be stolen

Answers can be found on page 32.

Are You a Victim?

What should you do if you suspect your identity has been stolen, despite your best efforts to prevent it?

Warning Signs

It can be difficult to detect when you have become an identity theft victim. Keep an eye out for some common warning signs:

- You are denied credit even though you've been responsible with your money
- You receive a letter that you are approved or denied credit for something you didn't apply for
- You are no longer receiving your bank or credit card statements
- Some of your mail is missing
- Your credit card has been maxed out and shut down
- You find charges on your credit card for items you never purchased
- A collection agency contacts you about an account you never opened
- Your money disappears from a savings or checking account

Was an Online Account Compromised?

There's a good chance that one of the accounts you created on a website has already been compromised as part of an attack by hackers. But if you don't follow the news or get notified by a company, how would you know your password may no longer be safe? That's why it's so important to never use the same password for more than one website.

To see if your information may have been compromised in the past, enter your email addresses at **haveibeenpwned.com**. This site is managed by a well-respected security researcher and relies on data that was already publicly-available from hackers. If you see an account has been compromised, make that the first password you change!

What to Do If Your Identity is Stolen

When a person first realizes they are the victim of identity theft, their first reaction is usually panic. However, the best reaction is to act quickly and stay on the offensive. If the theft is not reported in a timely manner, credit card and other companies may make it harder to dispute unauthorized charges.

Contact Credit Card Company or Bank Where Problem Occurred

First, contact the company involved in the incident. Let them know about any fraudulent account activity and make it clear you were not involved in the transactions. Review the account with the company for any evidence of other unauthorized charges. Make sure the account holder information is correct, especially the address on record and other contact information. If any problems are found, the account may need to be closed.

Contact the Federal Trade Commission (FTC)

The FTC is committed to finding and preventing identity theft. Follow their checklist at **www.identitytheft.gov** to take steps towards reporting the problem and cleaning up the mess. These steps include completing an ID Theft Affidavit as soon as possible.

Place a Fraud Alert on Your Credit Report

To place a fraud alert on all of your credit histories, you need only contact one of the three major credit bureaus. That agency will contact the other two for you[1].

Equifax
(800) 685-5000
www.equifax.com

Experian
(888) 397-3742
www.experian.com

TransUnion
(877) 322-8228
www.transunion.com

Ask that a fraud alert be placed on your file and that no new credit be issued in your name without your approval. A fraud alert requires that creditors contact you before making modifications to existing accounts or opening new ones. Also request a copy of your credit report to see if a thief has opened up any new accounts in your name.

Contact the Authorities

File a police report for identity theft, now recognized as a crime in most states and municipalities. The police report shows future creditors and employers what happened and may help if documentation is required to help your claim. The police are busy and often understaffed, so they may be reluctant to file the report. While always being polite, insist that they do so.

Also contact your state's attorney general. Some proactive offices will assist identity theft victims in dealing with the police and filing appropriate reports.

Contact Check Verification Companies

If someone has either opened a bank account in your name or forged/stolen checks, call the major check verification companies. Request that they notify retailers using their databases not to accept the lost or stolen checks, or ask your bank to notify the check verification service it does business with.

- **ChexSystems** - (800) 328-5121, **www.consumerdebit.com**
- **CrossCheck** - (800) 552-1900, **www.cross-check.com/forgery**
- **TeleCheck** - (800) 366-2425, **http://www.firstdata.com/telecheck/**

If you know which retailer was involved, find out which company they used.

1 http://www.consumer.ftc.gov/articles/0275-place-fraud-alert

Cleaning Up The Mess

If the perpetrator has been arrested, one way to clear up your identity is to have the police compare your fingerprints to the fingerprints taken during the arrest. When they don't match, the police will issue a "letter of clearance." This document may be vital when applying for a job or in case of future problems. This type of identity theft can linger for a long time unless it is addressed aggressively.

Internal Revenue Service

Contact the IRS at **http://www.irs.gov/Individuals/Identity-Protection** if you suspect the improper use of your identification in connection with tax violations.

Post Office

If you think someone has tampered with your mail by rerouting your mail through a change of address form or is stealing your mail, contact the Postal Inspection Service **http://postalinspectors.uspis.gov**.

Department of Motor Vehicles

Contact your state's department of motor vehicles and investigate whether any new identification cards or duplicate cards have been issued in your name.

Document Everything

So much of the recovery process requires creating a paper trail to prove your identity and that you have taken steps to repair the damage done. Be sure to document:

- Names of representatives you talk to
- Contact numbers
- Department names
- Dates/times of contact
- Time spent on calls
- Response from representatives

Any written correspondence should be sent by certified mail with a return receipt required. Record the amount of time spent documenting identity theft along with the amount of time at work that was lost. A few lucky victims have been reimbursed for their lost time after the thief was caught.

Credit Protection Services

There are several services available that claim to help prevent identity theft:

Credit Card Registry Services

These firms, which include some credit card companies, offer to register your credit or debit cards and notify all registered card companies if any cards are lost or stolen. Some credit card companies can even provide an emergency passport and/or an emergency driver's license in certain states.

Credit Monitoring Services

Credit monitoring services can alert you of any unusual or suspicious changes in your accounts. They often cover the cost of straightening out your financial records. The cost for these services typically ranges from $50 to $100 per year.

Many of these services offer little more than what you could do on your own for free. Other companies offer services beyond the reach of most consumers like constant 24-hour credit monitoring. These more-advanced services may be convenient if you have been a victim of identity theft in the past, and are often paid for by the institution where the breach occurred.

However, savvy thieves have been known to "sit on" stolen information for the one to three years these free monitoring services are typically offered after a breach.

Credit Repair Scams

Credit repair companies claim they can improve or erase negative information from your credit file so you can qualify for loans or a new job. According to the Federal Trade Commission, many of these companies engage in illegal business practices and violate federal and state consumer's rights laws.

It takes time and effort to repair credit history, and a firm can't provide any additional benefits beyond what you can do on your own.

Telemarketing Scams

Since liability is limited to $50 as a result of credit card fraud, beware of calls from telemarketers selling "loss protection" insurance. Some telemarketers may falsely claim that you will be responsible for all unauthorized charges made against your account if your credit card is stolen. Just hang up the phone.

Identity Theft Insurance

Identity theft insurance covers the costs incurred while cleaning up your identity. While this may include a protection service, insurance often doesn't cover the money stolen from bank accounts or fraudulent charges to credit cards.

The cost for identity insurance is relatively low. Most companies charge $25 per year, and some insurers may include this service as part of a homeowner's or renter's policy. In addition, some employers are offering identity theft insurance as a benefit.

Who Should Buy Identity Theft Insurance?

Of course, no one buys insurance expecting to have a loss. Most people buy insurance for peace of mind, which is difficult to quantify. Proponents of identity theft insurance argue that having this type of insurance helps victims cope with the ordeal. Moreover, consumers in high-risk categories might consider purchasing identity theft insurance. This includes those who:

- Travel internationally on a regular basis
- Have significant assets in savings and checking accounts
- Don't check accounts frequently

Tips for Buying Identity Theft Insurance

The following are tips to keep in mind when shopping for identity theft insurance:

You May Already Be Covered: Check your homeowner's or renter's insurance policy to see if identity theft insurance is already covered. Several major insurers include it; Others offer it as a rider on existing policies.

Seek A Low Coverage/Low Deductible Policy: Identity theft policies are generally very affordable since most people don't have to worry about high coverage amounts. Therefore, consider a low-deductible policy for your identity theft protection needs.

Coverage Provisions: Find out exactly what the policy covers. Some insurance companies are including personal counseling services to help identity theft victims get their lives back. These counselors are experienced and know the steps you need to take to start rebuilding.

Exclusions: Are there exclusions if the thief turns out to be a relative? Family members and relatives are frequent perpetrators of identity theft since they have easy access to your personal information.

Choosing Identity-Theft-Aware Banks

While many banks have made significant strides to help their customers prevent and detect fraud, some are doing a better job than others. Javelin Strategy and Research recently conducted a study of the 40-largest retail banks and their online identity theft detection and resolution services. The top-rated banks deliver email alerts to customers when changes are made to their account information, such as change of address. Most, however, do not offer email alerts when unusual account activities have occurred, such as a request for a change in PIN or phone number.

What You Should Look For in a Bank

- 24/7 account shut-off services
- Option of not receiving paper checking account statements (preventing criminals from stealing this account information out of your mailbox)
- Secure, online transaction services
- Email or text message alerts when significant changes are made to your accounts

Financial Products That Minimize or Eliminate Identity Theft

Some larger banks have introduced virtual debit cards that are designed to tie into your checking accounts and regular debit cards. These virtual debit cards are a piece of paper with an account number, expiration date, and verification code for making purchases online, over the phone, or via mail-order. You can set a maximum daily spending limit on the virtual debit card.

If an identity thief obtains the virtual debit card number, they would only have access to the daily limit amount. Many times these cards are bundled with identity theft reimbursement insurance and debit card rewards programs.

✓ EXERCISE

Test your identity theft knowledge. Some questions may have multiple answers.

1. **You discover unauthorized charges on your credit card. What should you do first?**
   A. Call the card company
   B. Order a copy of your credit report
   C. Call the FTC
2. **If there were just one step you could take to defend against identity theft, which would have the largest impact on your safety?**
   A. Mail all bills from a post office or official collection box
   B. Order a credit report on yourself at least once a year
   C. Stop using a debit card
   D. Buy identity theft insurance
3. **You receive an urgent email from your bank asking you to update your information. What should you do next?**
   A. Click the link in the email and login to your account
   B. Call the phone number on the email to ask for more information
   C. Call the phone number on the card belonging to that account
   D. Reply to the email
   E. On your own, go to the company's website to find their contact information
   F. C and E
4. **You get an email saying you won the lottery in London and should call immediately regarding your winnings. You decide to:**
   A. Delete the email; you never played the London Lotto
   B. Call the number listed and pay a small transfer fee for the winnings
   C. Respond to the email to ask for more information
5. **Who are potential identity thieves?**
   A. Scam artists
   B. Family members
   C. Rogue employees
   D. All of the above
6. **You have 30 minutes to devote to identity theft protection tonight. Of all the possible actions, which three should you take first?**
   A. Order your credit report
   B. Copy your wallet and take out anything you don't need
   C. Order identity theft insurance
   D. Get a P.O. Box
   E. Buy a shredder
   F. Review your bank and credit card statements

Answers can be found on page 32.

Suggested Action Items

The following are suggestions only. Whether you wish to take action should be based on your own individual situation and circumstances.

1. Order at least one free credit report from **www.annualcreditreport.com**
2. Select and use a password manager to create and store complex passwords for all of your online accounts. If the program offers it, store your credit card information and contact numbers there as well
3. Shred any sensitive information; If you don't own a shredder, purchase one
4. Opt-out of unwanted mail solicitations at **www.dmachoice.org**
5. Opt-out of credit card offers at **www.optoutprescreen.com**
6. Start carrying only essential items in your purse/wallet
7. Make a front and back copy of everything in your purse/wallet, and store it securely
8. Install an ad blocker on your computer and mobile device

Appendix

Answers to Workbook Exercises

Page 1-2:

Total Points	Your Identity Theft Awareness
35+	**EXPERT:** You are very well-protected against identity theft! Use this guide to continue to protect yourself because new scams happen every day. share your strategies with others who don't protect themselves as well.
25-34	**NEAR EXPERT:** You are doing well! With a few changes, you will become an expert. You should find several tips in this workbook you didn't consider.
16-25	**TRAINEE:** You have some good identity theft prevention habits, but you could improve in some areas. This workbook can help you.
15 or Less	**NEWBIE:** Don't fret, you're in good company! Most people need to make significant changes to the way they protect their identity. This workbook will really help you improve your habits.

Page 13:

1. D
2. F
3. A
4. B
5. G
6. E
7. C

Page 24:

1. A, H, I
2. A, H, I
3. A
4. G, H
5. C, G, H
6. B, E, H
7. F
8. B, E, G, H
9. B, D, E, G, H
10. D, H

Page 30:

1. A
2. B
3. F
4. A
5. D
6. A, B, (E), F

Organizations & Websites

Annual Credit Report www.annualcreditreport.com	*This site allows you to request a free credit report every 12 months from each of the three major credit bureaus.*
Call for Action www.callforaction.org	*An international non-profit network of consumer hotlines. Provides a list of identity theft resources.*
DMA Choice www.dmachoice.org	*The Direct Magazine Association is a group representing companies who send catalogs and other solicitations in the mail. DMAChoice allows you to stop these mailings.*
Electronic Privacy Information Center (EPIC) www.epic.org	*This website contains information on how to stay safe on the internet, news about the latest security breaches, and any new legislation on these issues.*
FTC's ID Theft Home Page www.consumer.gov/idtheft	*A national resource for identity theft information.*
IdentityTheft.gov www.identitytheft.gov	*A checklist with links to resources on what to do if you become the victim of identity theft.*
Identity Theft Resource Center (ITRC) www.idtheftcenter.org	*A non-profit, nationally-respected program dedicated to identity theft. It provides consumer and victim support and advises governmental agencies about this growing crime.*
National Do Not Call Registry www.donotcall.gov	*Add your phone number to a list that stops telemarketers from contacting you (except in a few cases).*
OnGuardOnline www.onguardonline.gov	*Information about avoiding email scams, securing your computer, and protecting your children online.*
Privacy Rights Clearinghouse www.privacyrights.org	*A non-profit consumer organization dedicated to consumer information and advocacy.*
Social Security Fraud Info www.ssa.gov/antifraudfacts	*Provides information about reporting fraud, waste, and abuse within the Social Security program.*

Glossary

419 Scam: A type of fraud or scam where you are promised a portion of a large sum of money in exchange for helping the recipient transfer the money past some difficulty. At some point during the process, you'll be asked to provide bank account details or payment for a transfer fee, which goes through, but no money reaches your account.

BitLocker: Drive encryption software included in Enterprise or Professional editions of modern Windows operating systems. BitLocker pairs your hard drive encryption with a chip inside your computer so that the drive can't be accessed from another computer.

Certificate: A small file issued by one of only a few authorities that guarantees the security of a network connection. If a valid, secure certificate is presented in a connection, you can be confident you are communicating with the website you expect to and no third party is "listening in" between you and the website.

Data Breach: A massive leak of information, usually when a hacker infiltrates the computer system of a company. Data breaches can include information as impersonal as credit card numbers to as critical as Social Security numbers. A data breach is usually large enough that, when discovered, there will be news reports about the event and you should receive a notice from the company if you were a customer.

DBAN: A free bootable utility which allows you to erase all of the information from a hard drive. DBAN works by copying empty or garbage data to a hard drive over and over again to eliminate any trace of the original information. This process may take a long time, but is essential before recycling or selling your computer.

EMV: Short for Europay, MasterCard, Visa, EMV is the technical standard for credit cards which have an embedded security chip. This chip can issue one-time-use codes for credit card transactions rather than using the credit card number. EMV has been popular in Europe for almost two decades but has only recently appeared in the U.S.

Encryption: The process of protecting information by jumbling it up based on a particular formula which can only be cracked using a specific key or password. An encryption key allows the data to be decrypted, or have the security removed, so that it can be read normally by the computer. Without the key, there is typically no way to read or access the information that has been protected.

FileVault: Drive encryption software included in every modern OS X computer system. File Vault encrypts the data on your Mac and unlocks it each time you start up using your normal login password. If your computer was lost or stolen, the data is safe.

Fraud Alert: This is a notice you issue to one of the Credit Bureaus when there has been a known data breach or identity theft on your credit report. That bureau will contact the other two to place fraud alerts on those reports as well. A fraud alert flags your credit report for additional scrutiny when new credit is requested.

Internet Service Provider (ISP): This is the company providing your internet service to your computer. Most commonly your ISP will be Comcast, AT&T, Time Warner, Cox, or Verizon. Your internet service may include a free subscription to antivirus software.

Malware: Malicious software which is installed on your computer without notice or permission to manipulate data or steal your personal information. Malware can steal passwords, install ads on your computer, delete your files, or slow down your work.

Phishing: A malicious email designed to look like it came from a legitimate business, often requesting a password or other personal information. While the company logo and other features of the email might seem legitimate, any links or addresses in the email will lead you to someone else trying to steal your personal information.

Privacy Notice: A federally-mandated communication from some entities like banks and credit unions which you will receive once a year. This notice will reveal the ways a company plans to use your information and your opportunities to restrict that use. The notice will require you to reply back to prevent your data from being shared.

Pyramid Scheme: A business enterprise where money from new investors or customers is used to pay the gains of previous investors. No actual business or product exists since the money is being funneled elsewhere. The scam can persist as long as new money is coming in because without that, there are no earnings to share with the old investors. *Also known as a Ponzi Scheme.*

Salt: An extra bit of data or information attached to other information, like a password, to increase its length and change the result after encryption. A salt changes the data stored on a server, making it harder for a criminal to guess a password because the result of any guess will be garbage without knowing what the salt is.

Security Freeze: A request on your credit report which prevents any new credit from being issued. You must request a security freeze from each individual credit bureau and there many be a small fee. If you freeze your credit, you will be issued a PIN in case you need to unlock it for a legitimate credit inquiry.

Skimming: Stealing credit card information by physically swiping a credit card in some apparatus. This can be as large as a reader inside of an ATM machine or as small as something in the pocket of a waiter. Skimming works because the data on the magnetic strip of your credit card is not encrypted, but it does not include your PIN number or the 3-4 digit security code on the back of the card. Criminals may use other tactics to find those numbers and increase the value of their stolen card numbers.

Smishing: Similar to phishing but by text message rather than email. The name comes from SMS, the technical term for a text message on your cell phone. These texts may claim to be from a relative, the phone company, or some other entity, but are a clear scam because they will request personal information or money transfers.

Spyware: Software installed on your computer without your knowledge or consent which seeks to track you or show additional advertising. The most common form of spyware is browser toolbars but some spyware is almost invisible. Be sure to protect your computer with a current subscription to internet security software.

Synthetic Identity Theft: A form of identity theft where bits of data from several different people are combined to create a new, false person. This makes the theft very difficult to trace or detect, since each individual victim will only have a small clue of a problem. The best protection against Synthetic Identity Theft is to constantly monitor your credit reports and also request your annual statement of social security benefits to make sure their data matches your earned income.

Two-Factor Authentication (2FA): The ability to request a second factor, a short numeric code, which you use to login to a website, along with your password. Enabling 2FA means just stealing your password isn't enough to allow someone to steal your account.

Send Us Feedback