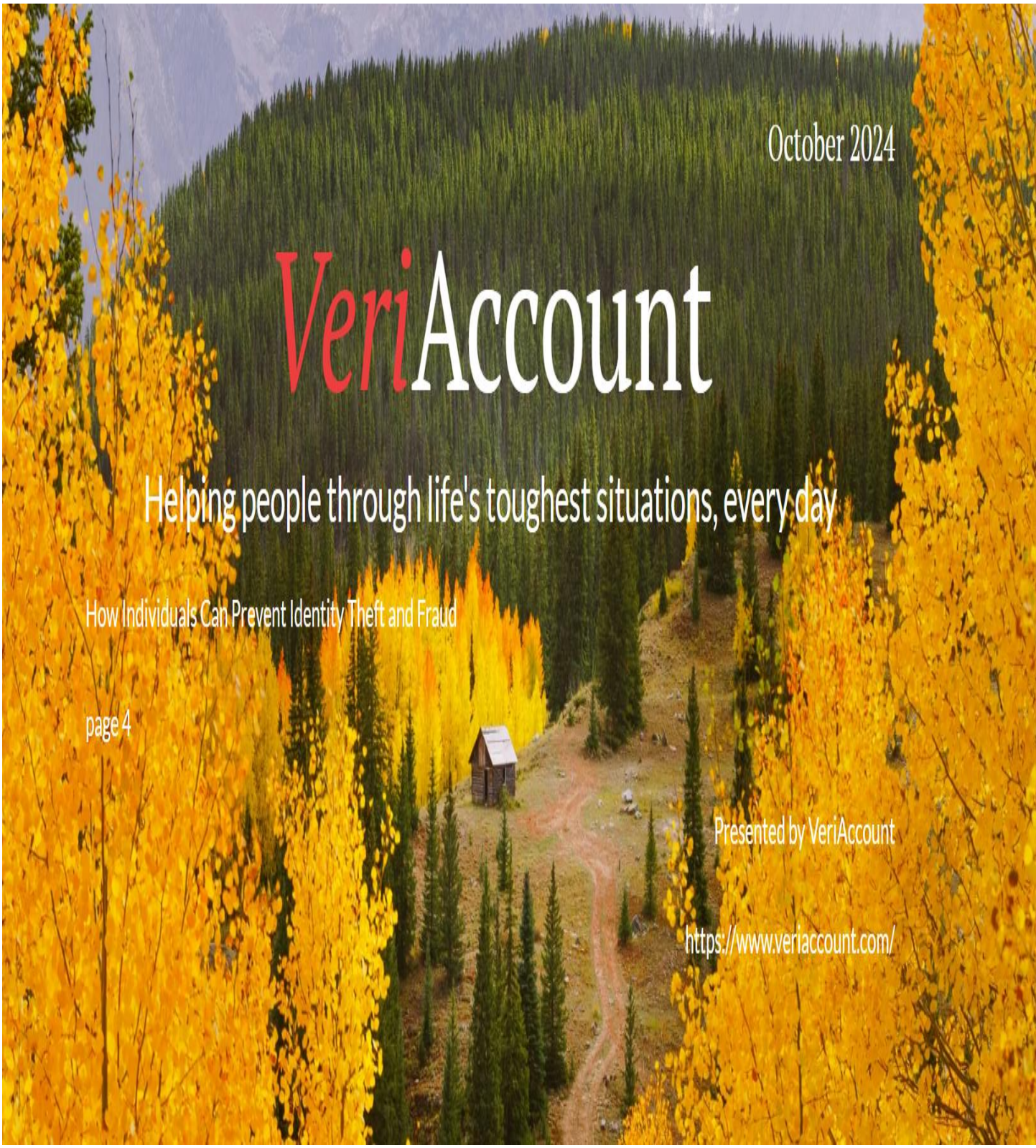

October 2024
VeriAccount
Helping people through life's toughest situations, every day
How Individuals Can Prevent Identity Theft and Fraud
page 4
Presented by VeriAccount
https://www.veriaccount.com/

Table of Contents

How much do you know about identity theft and identity fraud?

1. How can you know whether or not someone wrongfully used your credit card to make purchases?

A if you see unauthorized transactions on your monthly statement

B if you see authorized transactions on your credit report

C if you see constant billing for a subscription that you did not sign up for

D A and C

2. How can you tell if Social Security card identity theft has occurred?

A when someone transcribed your SSN number when you read it aloud to someone on the phone

B when they got it in a data breach

C when someone stole your SSN number

D all of the above

3. How can you tell if Social Security identity fraud has occurred?

A if you find a fake ID card with your name, date of birth, and a new Social Security number on the internet

B if someone created a new bank account in your name

C if someone created a synthetic identity in your name

D all of the above

4. What is synthetic identity theft?

A when someone merges parts of your personal information to create a real identity

B when someone merges parts of your personal information to create a fictitious identity

C when someone merges parts of your personal information with one or more victims to create a fictitious identity

D all of the above

5. How can you tell if a company sent you a spam email?

A if it asks you to pay to finalize the hiring process

B if it asks you to give them your date of birth in the job application

C Both A and B

D if it does not get back to you after you submit your job application

6. What kind of identity fraud involves leveraging security flaws in people's internet-connected devices to go after their personal data?

A credit card fraud

B Internet of Things fraud

C debit card fraud

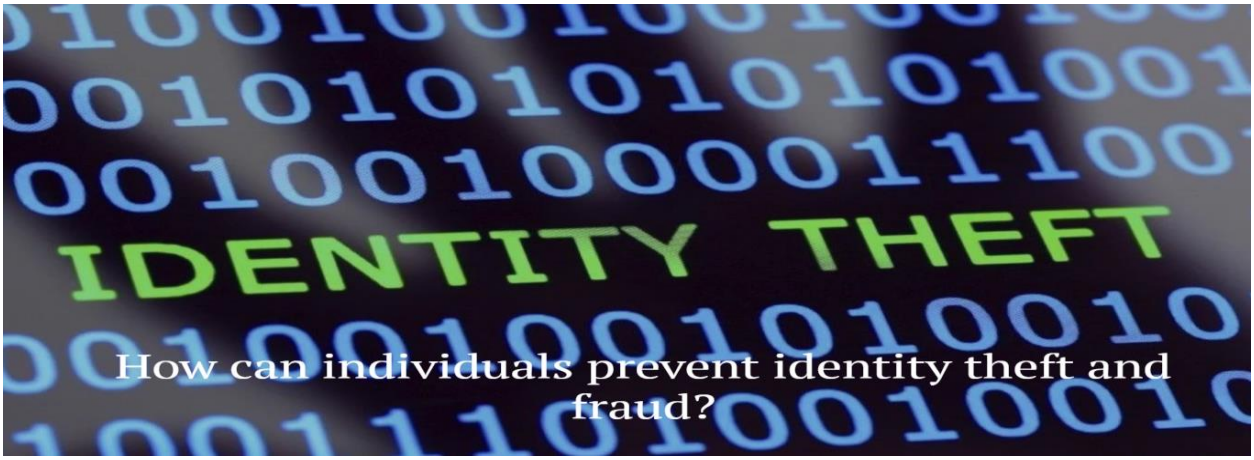
D all of the above

QUIZ RESULTS

1-2 Q's right	3-4 Q's right	5-6 Q's right
You need a lot of help protecting your personal information. Luckily, VeriAccount can help you do that with the utmost integrity!	You know what you're doing in some areas of handling identity theft and fraud but need help in some areas.	You know what you're doing when handling most to all instances of identity theft and fraud. Congratulations!

QUIZ ANSWERS

1. D	2. D	3. D
4. C	5. C	6. B



Identity theft and fraud are inevitable considering that anyone can access people's personal information. Common examples of personal information that people steal are usernames and passwords, credit card information, email addresses, and phone numbers. It is imperative that individuals know how to prevent identity theft and fraud so they can protect and secure their personal identities and take charge of their finances.

What is the difference between identity theft and identity fraud?

There is a fine line between identity theft and identity fraud since they are both crimes that involve a person's personal information being used for unethical purposes. Identity theft is when someone takes somebody's personal information while identity fraud is when someone uses a somebody's personal information to open accounts, such as bank accounts. Individuals who partake in identity theft and identity fraud crimes are called hackers and fraudsters. Examples of data hackers and fraudsters obtain include names, addresses, credit card numbers, Social Security numbers, and bank account numbers. They use this information to do things such as buy items, steal tax refunds, get credit cards, and open accounts, causing a large detriment to people's finances.

Ways that Hackers and Fraudsters Commit Identity Theft and Identity Fraud

Hackers and fraudsters perform identity theft and fraud in a variety of ways. Some of the most common ways they do this are sending spam emails, activating people's credit cards after they have discarded applications they received for "pre-approved" credit cards, and "shoulder surfing". Shoulder surfing involves watching someone as someone enters its personal information or gives it to someone over the phone.

Steps Individuals Can Take to Prevent Identity Theft and Identity Fraud

People can prevent identity theft and fraud in many ways. Before they do this, they must first determine if an act of identity theft or fraud has occurred. Here are a few ways that individuals can detect identity theft and fraud.

1. Check your bank account statement.

Review your monthly statements to see if there are suspicious charges and inconsistences. It is a good idea to see if your bank statements can be given to you through a mobile app or by mail.

2. Get and review your bills and credit reports.

Obtain your bills and credit reports to see if there is anything that should not be there, such as a changed address or a false subscription to an iPhone application. It is best to get them once every two weeks rather than once a month so that, when an act of identity theft or fraud has been executed, you can take care of it faster.

The second step when preventing identity theft and fraud is protecting personal information. Here are some tips that can help you improve your personal data protection.

1. Keep all financial records, Social Security and Medicare cards, and other documents with personal information in a secure place that is difficult for your loved ones and cybercriminals to find.

When protecting physical copies of documents, think of places that your children would not look for items, such as the attic or basement. The problem with placing important documents in rooms that families use is that these documents can be found more easily. Another helpful tip is placing important documents with personal data in a place in which you can lock them, such as a safe or a LockBox. It is essential that you do not give the passwords and passcodes to anyone and that you keep them in a place you can find them, such as the Notes app on your iPhone.

When dealing with digital copies of your personal information, you should store them on a flash drive. This way, nobody can know where you have stored them.

2. Create strong passwords when creating new accounts.

It is easy to create passwords with information, such as your name and birth year, because you can remember them better. But creating a password without this personal information can greatly decrease the chances of your personal data being stolen. Another tip is to create a password with a variety of characters, such as exclamation points and anestric, because it can be harder to figure out one's password when they contain a variety of characters.

3. Never respond to spam phone calls, emails, and text messages.

If you cannot recognize a phone number, do not answer the phone or a text message from that person. People too often send texts and emails with fraudulent links that generate viruses or software that steals other people's personal information. Therefore, it is of the utmost importance to only respond to individuals whose phone numbers and emails that you can recognize, such as those of your friends and coworkers.

4. Update your passwords every 60 to 90 days.

Creating new passwords every 60 to 90 days can decrease the chances of them getting stolen by hackers and fraudsters. Make sure that you create strong passwords with lowercase and uppercase letters and a variety of characters, such as exclamation points and parentheses. This way, it is harder for cybercriminals to figure them out and thus access your accounts.

3. Do not use public Wi-Fi.

Since individuals create public Wi-Fi networks to keep them open to the public, they often forget to protect and encrypt them. When you do not use public Wi-Fi networks, you reduce your chances of hackers and fraudsters receiving and using your personal information. Also, it is important to know that some people utilize emergency public Wi-Fi networks, such as Optimum Emergency Wi-Fi, for unethical, illegal purposes. So, it is best to avoid using such networks unless you unethical, illegal purposes. So, it is best to avoid using such networks unless you need to make an emergency phone call to someone.

1. Always ask questions before giving out your date of birth, address, and other personal information, especially your Social Security number.

Some organizations, such as your bank, will need your personal information to identify you, especially your Social Security number. But many other organizations may ask for it too, such as your medical provider. It is always smart to ask questions before freely giving out your personal data. Some examples are the following:

1. Why do you need it?

2. How will you protect this information?

3. Can you please use a different identifier?

Identity Theft Protection Services

There are a variety of identity theft protection services that organizations sell, such as banks and credit unions. Common examples include credit monitoring, identity monitoring, identity recovering services, and identity theft insurance. Here is a breakdown of each kind of service.

1. Credit monitoring services

Credit monitoring services scan activity that people see on their credit reports and may monitor activity at one, two, or three of America's largest credit bureaus: Equifax, Experian, and TransUnion. They are used to alert people during a wide range of situations, such as: when companies check someone's credit history, a new loan or credit card account shows up on credit reports, a creditor or debt collector tells someone that their payment is late, a record reveals that someone has filed for bankruptcy, a person files a lawsuit against someone, somebody's credit limit changes, or someone's personal data changes.

2. Identity monitoring services

Identity monitoring services are services companies offer that check databases that hold a variety of information about people to identity if they have new or inaccurate information about them. They are used to detect uses of people's personal data that often do not appear on their credit reports. Identity monitoring services will tell individuals when their personal information appears in a change of address request, court or arrest records, orders for services, applications for loans, requests to cash checks, and on social media and websites that identity thieves utilize to trade stolen personal information.

Even though many companies sell them, it is a great idea to ask your bank or credit union, credit card provider, employer's benefits program, or insurance company to see if they sell them. This way, you can benefit from additional security from organizations that work to help people.

How VeriAccount Protects Your Personal Information

In conclusion, knowing how to prevent identity theft and identity fraud is an essential part of protecting your personal information and improving your financial management. By identifying when someone has taken or used your personal information, taking measures protect your personal information, and using identity theft protection services, individuals can ensure that their data is not misused and that they are financially secure and trusted by their employers.

At VeriAccount, ensuring that your personal information is protected is paramount to us. We do not gather personal information about people unless they choose to give it to us or decide to use products or services that are available on our website. The thing that separates us is our ability to utilize personal information solely to operate our website, deliver services, and inform people of products that we offer. In this way, no third party can get access to your personal data. As a business, VeriAccount is completely committed to protecting your personal information. Therefore, what better way to offer your loved ones a more secure experience than to partner with us?

Fun Fact: Identity theft and identity fraud cases have nearly tripled over the last decade.