VeriAccount

FInance Magazine October 2025

Serving Your Needs with Resilient Financial Solutions, Every Day

Understanding Cybersecurity Threats: What You Need to Know to Protect Your Financial Information

page 6

Table of Contents

VeriAccount Quiz

How Well Can You Protect Your Financial Information?

1. Which of the following is the strongest password?
    a. password234
    b. Sally1988
    c. !vC8&X$3mN@z
    d. ilovepasta
2. When should you give out your Social Security number?
    a. Anytime you are asked for it
    b. Only when it's legally required or absolutely necessary
    c. When signing up for online shopping accounts
    d. Never under any circumstances
3. What does two-factor authentication do?
    a. It makes your password longer
    b. It backs up your data automatically
    c. It requires an additional step to verify your identity
    d. It encrypts your files
4. You get a call from someone claiming to be from your bank asking for your account number. What should you do?
    a. Give it to him to be helpful
    b. Hang up and call your bank using a verified number
    c. Ask for their badge number
    d. Tell them to call you back another time
5. Which of the following is a sign of a phishing email?
    a. A personalized greeting
    b. Grammatical errors and urgent requests
    c. A familiar company logo
    d. All of the above

6. You're on public Wi-Fi at a restaurant. What should you avoid doing?
    a. Logging into your bank account
    b. Watching YouTube videos
    c. Browsing the news
    d. Reading LinkedIn newsletters
7. You receive an email from your bank asking you to confirm your account details via a link. What should you do?
    a. Click the link and enter your details to stay compliant
    b. Ignore the email
    c. Forward the email to your friends to warn them
    d. Contact your bank using a known, official method
8. You get a text saying that there is suspicious activity on your bank account, asking you to call a number. What do you do?
    a. Call the number right away
    b. Check your bank account through the bank app or website
    c. Respond to the text to ask for more information
    d. Don't answer it

Quiz Answers

1. **C**
2. **B**
3. **C**
4. **B**
5. **B**
6. **A**
7. **D**
8. **B**

VeriAccount Service Spotlight

Need to Recover Hidden or Hard-to-Access Funds?
Save money and time with our Hidden Asset Retrieval Service!

Finding hidden or difficult-to-access funds during an unexpected event can be stressful and feel overwhelming. Our Hidden Access Retrieval Service is there to help you track all funds down so you can have the financial stability and closure you need.

What We Do:

- Locate hidden bank accounts
- Track down lost life insurance proceeds and pensions
- Uncover mislaid investments and escheated funds
- Employ advanced financial tracing techniques

At VeriAccount, we don't make you pay an upfront cost. Our fee is ⅓ of pocket savings or additional coverage found.

Take the first step toward financial clarity. Visit www.veriaccount.com/ to schedule a free consultation!

Get Started

VeriAccount Featured Article

Understanding Cybersecurity Threats: What You Need to Know to Protect Your Financial Information

In today's digital age, cybersecurity threats to people's financial information have become increasingly commonplace and more difficult to identify. From making unauthorized purchases upon stealing credit card information to logging into people's bank accounts to transfer money, cybercriminals will do anything to put others' financial data and cybersecurity at risk. At a time when people have easier access to individual financial information than ever before, it is paramount to know how to protect your financial information.

Types of Cybersecurity Threats

Cybercriminals utilize a variety of tactics to access and utilize people's financial data for their own benefit. It is important to know the difference between identity theft and identity fraud. Identity theft happens when someone accesses and steals someone's financial information on the internet, such as through a bank database, while identity fraud occurs when someone uses someone's financial information to do something, such as make an unauthorized purchase. Here are some of the most common cybersecurity threats that cybercriminals do in today's world.

1. Phishing

Phishing is perhaps the most common way cybercriminals steal and use people's financial information. It occurs when someone makes a phone call or writes an email, text message, or social media message or that seems like it is from a known organization, tells you there is a problem or that you need to do something, and asks you for your financial information. Phishers disguise themselves as employees at banks, credit card companies, government agencies, and sometimes online stores to tell individuals messages, such as "There's a problem with your account" and "You're due for a refund", and to ask them to do things, such as verify a transaction. These messages ask you for your financial data or have a link or attachment that asks you for it. Examples of financial data cybercriminals ask for include credit card numbers, bank account details, and login credentials.

2. Data Breaches

Another way cybercriminals access financial information is through hacking, which is the process in which someone gets unauthorized access to a computer, network, or digital system to steal, damage, or exploit data. Cybercriminals breach financial data by getting into financial and governmental databases and networks to retrieve, steal, and use people's financial information.

3. Direct Theft

Direct theft occurs when someone accesses someone's financial information, such as their credit or debt card information, and uses it to do something. Examples of direct theft include withdrawing money from bank accounts and making unauthorized purchases.

4. Identity Theft

Identity theft happens when people use others' financial information to do illegal acts that ruin their credit scores and damage their financial wellbeing. Cybercriminals commit acts of identity theft in many ways, including opening new credit cards, loans, and bank accounts in the victim's name.

5. Selling Financial Information

One of the most dangerous ways cybercriminals threaten individual financial security is by selling their financial information on underground marketplaces, such as full credit card details and account login information.

6. Tax and Insurance Fraud

Another dangerous way cybercriminals threaten the security of people's financial data is through getting and using people's tax and insurance information. For example, they may file a tax return or insurance claim after stealing someone's data.

Ways You Can Protect Your Financial Information

1. Use strong passwords for different websites and apps

It is important to create and utilize strong passwords for every financial website and digital app. If you use the same passwords, hackers and other cybercriminals can retrieve this information and use it unethically or illegally. Strong passwords have a combination of capital and lowercase letters, numbers, and characters, such as exclamation points.

2. Enable two-factor authentication on all financial accounts

Two-factor authentication is a process in which an organization sends you a code to your phone or email that you enter to access a website or app. We recommend enabling it on all sensitive accounts including bank accounts, PayPal, Venmo, and email accounts.

3. Don't click on links or attachments phishers provide or give them financial information

It is essential to not give phishers your financial data because they can steal it and use it to do things that damage your financial health, such as withdrawing a significant amount of money from one of your bank accounts.

4. Keep Your Devices and Software Updated

It is essential to update your phone, computer, browsers, and financial apps when necessary. Up-to-date devices and software can reduce the chances of cybercriminals stealing and using your financial data.

5. Do Not Use Public Wi-Fi to Make Financial Transactions
You should not utilize public Wi-Fi networks to bank because they can be easily hacked. If you are in an area that lacks private networks, be sure to use a VPN, or a virtual private network, to make a transaction. Using a VPN can greatly increase your cybersecurity when you are in places that only have public Wi-Fi.

Knowing how to protect your financial information from being accessed and utilized by cybercriminals is essential for achieving long-term financial stability. At VeriAccount, we know the importance of detecting and responding to cybersecurity threats. For information about how we can help you safeguard your financial data, contact us for a free consultation!