HOW TO PLAN FOR

HACKS & ATTACKS

techpocus.com©

Ultimate Plan Guide

Have you ever felt Vulnerable?

In 2022 Millions of people have already fell victim to Identity Theft

Every 3 Seconds

Someone's Identity has been compromised!

SIM CARD SWAPPING & PORT HIJACKING

E-MAIL HACK & FRAUD

IDENTITY THEFT

It is Overwhelming

To Resolve on your own

PC & IOS ATTACKS

MAIL & DOOR FRAUD

FINANCIAL THEFT

Types of Attacks & Fraud

SIM Card Swapping or Port Hijacking

This is when someone gains access to your phone using information found on the internet such as social media and other websites. Once the information is compiled, they will try to access your account information on those sites. Many times they contact the carrier of your service and pose as you trying to claim to have lost or the SIM Card has been stolen. The hacker then asks the representative to activate a new sim card they supposedly purchased which is their own SIM. The Customer Service Representative activates that SIM with your number attached. You now have lost control of your cell phone number. They then start hacking your two step authentications such as username and password resetting them on all of your accessible sites and apps. Now they can receive the authentication codes sent via SMS and change your passwords to all of your accounts. The key is to secure your account and app information. Our Full Guide goes deeper into this area of attack and fraud.

How to Protect yourself from SIM Port Hijacking or Swapping

One of the first ways to protect your phone from this type of attack is to create a new SIM Pin number at your Carrier Provider's website. Also change passwords accessing your account to a secure password. Ask your cell phone provider to add port validation - which ensures that if there is an attempt to change your personal information you will be contacted to verify all of the items requested for change on your account.

Reduce the amount of information about you on social media such as Facebook, Twitter, and Instagram. These are common sites for hackers to browse through and piece all that they need to know about you. Use Two Factor Authentication.

Use third party authentication apps such as Google Authenticator, Microsoft Authenticator, and **Authy** are good ones to use.

Each app will direct you how to setup authentication.

The difference between using an app to authenticate your information verses direct authentication from Facebook or other websites is that the app is a go between you and the site you are logging into.

A hacker cannot access your authentication codes from the third party authenticator app without your security pin from that authentication app. Also; it is one more layer of protection for you on your phone and personal computer.

Using Software such as **SecSign** will help with documents and security whether on your computer or smart phone.

Types of Attacks & Fraud

E-mail Fraud

Your e-mail address is listed on the internet through many sources. No matter how private you try to make it; it is very difficult to avoid spam and e-mail fraud. Here is how E-mail fraud works; You receive an e-mail from what looks like a major social media, entertainment, communications, bank, or an online payment website. You look at the content and almost click on the button that says Renew Subscription, Pay Bill, or Update Account Information.

These scammers know how to copy the correct language, logos, and copyright information that looks identical to your active account at the real institution or entity they are "representing."

Be fully aware and do not click on these links. If you think that your bill is past due, account needs to be updated, or there are other issues; always go to the website directly not through the e-mail notification.

Look for weird inconsistencies in the e-mail such as the greeting, wording, demands, and other things that do not add up to common sense evaluation.

More information can be found at this website link **Consumer Trade Commission**

Never click on anything that you think might be a scam. Use your gut feeling and know the difference.

How to Protect against E-mail Fraud

E-mail is one of the oldest digital communication tools since the internet was created.

Sending e-mails is so common that we forget about the security dilemma that exists due to all of the e-mail fraud. One of the greatest challenges any person faces is keeping your e-mail clear of spam, junk mail, and special offer e-mails. Once you sign up for e-mail updates and notifications from a website such as software, food, clothing, electronics, financial, and others, you will immediately be bombarded with offers and updates.

The challenge is to limit this requesting of information to a minimal in order to not allow your e-mail address to be sold or shared online.

Many websites share your information and are legally obligated with privacy acts in place to request your permission before they share to third party vendors. Some do not comply with this or are not honest with you.

There are fine print disclaimers with some that will hide in the paragraphs the authorization of your e-mail to be shared with third party for research and information. Little did you know that you would start receiving emails from companies you have never heard of. This is a challenge but one must be always vigilant to stop information from being shared. The next slide will explain measures that you can do in order to secure your e-mail more tightly and stop from being a security risk.

STEPS TO TAKE TO

SECURE YOUR E-MAIL

- **Stop signing up for subscriptions** unless you absolutely have to.
- **Unsubscribe from e-mails** that you do not wish to receive any longer. At the bottom of every e-mail is an unsubscribe link usually in blue. Click this and enter your e-mail that you wish to have removed from the website server.
- **Do not share your information** with third party popups and websites that claim they are linked to the primary site that you are entering your information
- **Do not click on any e-mail links** that you do not recognize. Do not open e-mails from sources that you do not recognize as well.
- **Do not click on e-mails that are "Look a like's"** such as an e-mail that has an invoice amount due with the logo of your cellular provider information. These e-mails are frauded with logos, color schemes, wording, and links that look very similar to the actual notification from your providing service. Verify online on the actual website for the service or provider before clicking on the e-mail.
- **Check e-mail addresses in the FROM area** of the e-mail tags. If there is any added name, address, or different description with the address that does not equate to the direct site for the provider; it is a scam and you will be hacked.

Types of Attacks & Fraud

Mail & Door Fraud

You receive a letter in the mail that looks professional and so you open the contents.
In the letter it is requesting you to take some sort of action. Whether it is to sell your property, sign up for a membership, call in for a chance to reserve your spot at an event, or other types.
You immediately feel empowered or lucky as you do not receive this kind of reward letter very often. It is 90% a scam.
Once you call, fill out the forms, mail back the information they are requesting, or even meet in person, you are risking your personal identity and information. They will use this against you and will have more personal information that will increase their ability to gain access to your financial institutions, create a new identity, and steal your most precious and valuable assets.
The bottom line; never trust mail that is sent unless you can verify the contents are true and real.
Door Fraud is very common and has been around for decades. People posing as your Utilities or Power company needing to perform a routine check. These two are most common. Your Local Power or Utilities company will never ask to enter your home. They have highly technical ways to read your meter which is always accessible outside your house.
Never let strangers enter your home no matter how nice they seem. Here are a list of common door fraud scammers.

Mail & Door Fraud Posers

Scammers pose as the following:

- Window Cleaners
- Utilities Worker
- Power Company Representative, Window & Door Replacement Sales Person
- Home Inspector
- Government Agent
- Book Label Sales Rep
- and more.

How to Protect against Door Fraud

What to say against pushy scam artists

What to say to Door to Door Scam Artists

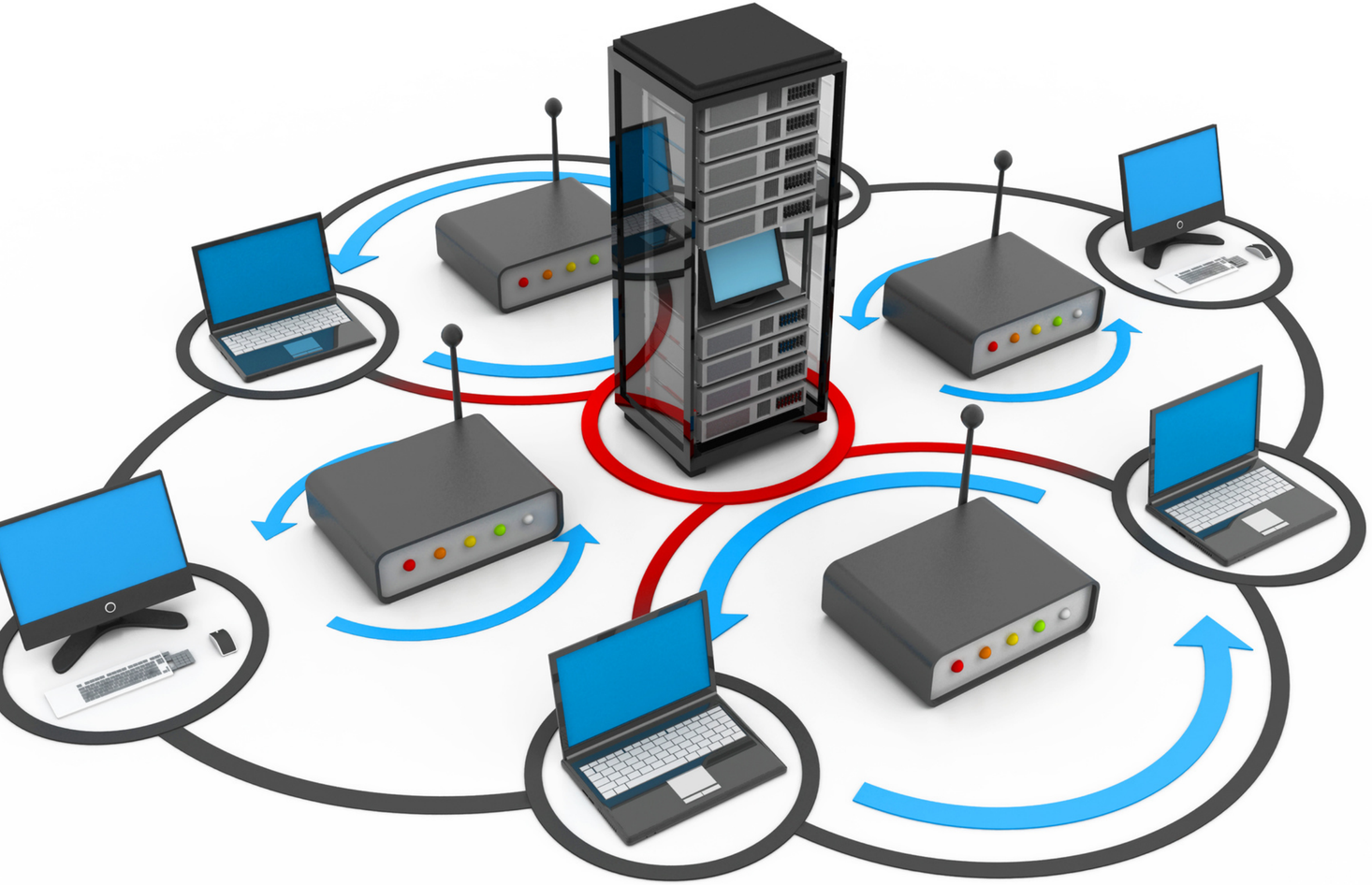
Many door to door sales people are genuine and are trying to make a living.
Unfortunately because of the stigma and bad experiences of this type of selling; it has put millions of people on edge to even answer the door.
Here is what to say if they do not go away a couple polite attempts.
TIP: Never crack door open to listen; always talk through a locked screen door. They will literally try to get a foot hold and come in. Some are this bold.

"I see that you are persistent; and I am running out of patience. Please leave now before I have none."
"I am not interested. Please leave my property before I contact the authorities."
"You are not authorized to come inside and I do not feel comfortable with you entering my home."
TIP: Scam artists will want to know when they can come back in case you change your mind; this is a ploy to come when you are not home. Especially if you forget you made the appointment. Never schedule any time unless you are willing to hire the company they represent. Also; Ask if you can contact their company and verify the person working for that company. Most cases they will leave.
You can install a security linked camera or doorbell through **Ring**, & **Simply Safe**. This enables you to see and talk to the person at your door with or without you being home or opening your door.

PC Security

Securing your PC from Attacks and Hackers

Networks



Networks can be tricky to setup and difficult to maintain. Whether you have one router and a few devices with a PC or several routers with multiple PC's and devices; your network is the stopping point for many security breaches.

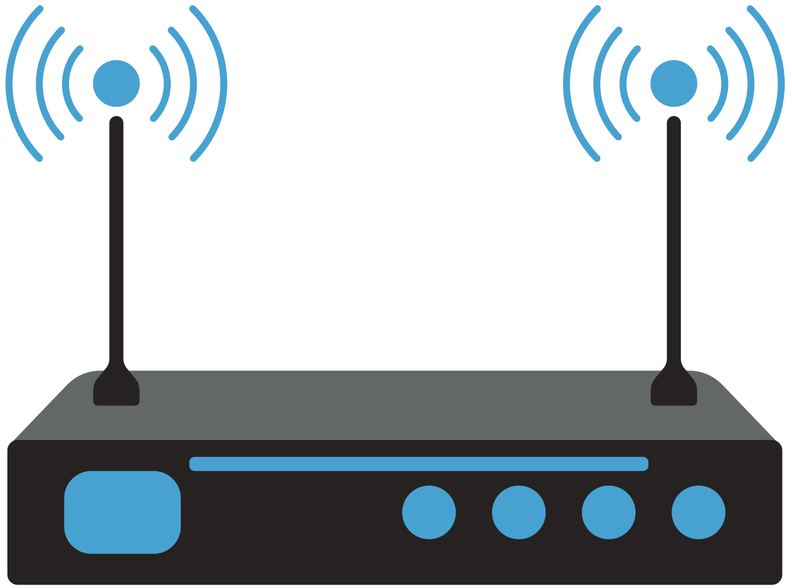
If you have a Server on the network; know that this is your most secured asset in the network itself.

Networking is a brilliant way for your home or office to communicate others.

Many companies have networks within the confines of their office buildings. This is called a intranet. All information shared and stored is within this network. There are not internet access points without permissions from the server in user accounts and privileges. **This ensures that viruses, hacks, corrupt files, and infiltration is kept to a very low risk factor.**

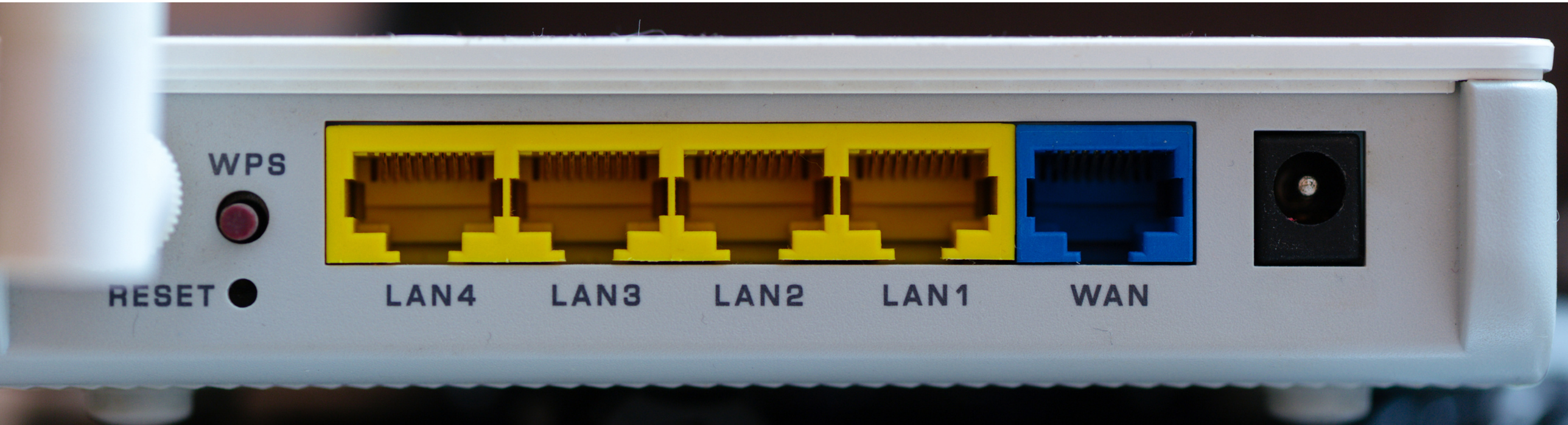
Common Home Network

Multiple Devices
Connected to One Router



Common Home Network Router

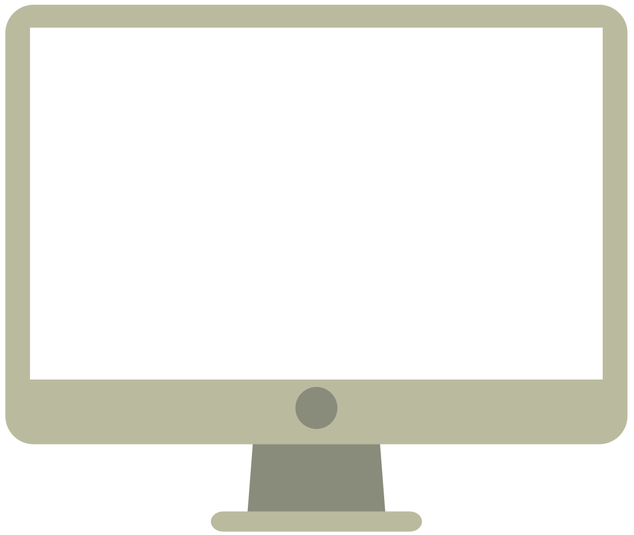
Routers are designed to be setup quickly and without error. The common mistake that many people make is that they do not reset the Admin Username and Password to their router. This is a given access point by any hacker who tries to connect to the router. In the instructions and setup of your router software; there is a link that you can click on to change the Admin Username, Password, Security Settings, Filters for Online Browsing Settings, and much more. We recommend that the permissions to this router are changed; username and password. This will help provide one extra layer of protection to your home network. Upgrading your router every couple years will help with security as well. **Always check for software updates** for your router. If you don't the hackers will be able to get past your encryption and security settings if not updated. Even if the only router you have is the Internet Provider's Router - Same steps apply.



Securing your PC on Networks

Your Router is built with Technology that keeps your network secure.

But what about your PC?



Your PC is the most valuable asset you have to access information at your fingertips. Yes your cell phone (Smart Phone) is a phenomenal small computer with powerful attributes; but there is nothing like seeing a larger screen view of what you are working on. With the capabilities of technology today your PC is faster, more efficient, and more reliable. The only hitch is that it cannot keep safe from dangerous incoming information on it's own.

Here are some crucial tips to help keep your PC Secure from Hacks and Attacks

Crucial Tips for Securing your PC

Keep PC Clean of Common Dead Files - Run Disk Clean Up often

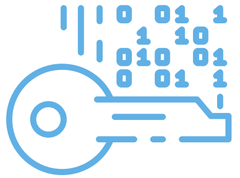
Install Antimalware / Antivirus Software - This will help protect from viruses, scans, & penetration attempts through your connectivity ports on your router to your pc. Set your antimalware / antivirus to scan automatically daily after booting or at night.

Do not always allow cookies - Cookies are a great way to have hundreds of websites track your location(s), habits of searches, and information you enter. They build a database of your likes and interests. This is click marketing and tracing.

Stay away from websites that are not encrypted - You will know because your browser security will most likely prevent you from accessing the website if the encryption is not high enough or certified for access through the browser. If you continue to the site; you are at your own risk and will be liable for damages from trojans, viruses, and hacks.

Backup your PC often - This is crucial because if your system crashes and you cannot access beyond the home screen; you will be forced to recover, restore, and or format

More Crucial Tips for Securing your PC



Encrypt Sensitive Documents - This step is very important especially if you have information that is highly sensitive and aligns with your identity information. Encrypting is simple; in document settings you can find how to encrypt this document or search online for ways to encrypt office type or other documents via Apple etc.

Do not install software from unknown Websites - Installation of quick fix software can be very risky. You have an issue with a hardware driver or need software to meet a requirement; so you search for free (software type name) it comes up with links many solutions. Problem is that the website names are obscure and you have never heard of any of them. Beware; many of these are full of popups, tracking ads, and trojan entry links that can penetrate your pc once clicked. Never download anything without researching and always verify. Go to a reputable software website not third party sites that list software trial versions etc. Go to trusted sites and read about the software before downloading. If it looks off; it probably is a scam.

More Crucial Tips for Securing your PC

Clear Search History - It is important to clear search history when exiting massive amounts of searching online. Your browser settings will have an option to clear site history or search history. This is another way to protect and secure your pc.

Never Join Un-Secure Networks - If you have a Windows PC (Surface type) or an Apple Laptop, or General Laptop that is mobile; you will have a temptation to join a WiFi network that is not secured or "free" to the public. Never do this. I mean never. Unless you have a security software or device that prevents infiltration you will be victim to a hack or attack. Many people prey on people's pc's or devices that are on free networks such as Hotels, Restaurants, Bistro's, and other public places.

On Exit; close out all browsers and programs - Many people do not close their browsers or programs online after a few hours or at all. This can lead to cyber attacks from websites that are vulnerable or being hacked. If your logged in and stay logged in for multiple periods of time; you are risking your information to being compromised.

Information

Greatest Downfall to Hacks & Attacks

Financial Information

Everyone has financial information that is stored on a Server for you to access your banking, investing, products, and services. The problem with information of this magnitude is that the responsibility is usually placed upon the bank, investment firms, stores, and service websites and entities that we use everyday. We do not always think that our information can and will be compromised. We put much trust in corporations and online entities to store our information especially our financial identity.

This includes:

Bank Accounts, ACH Numbers, Debit & Credit Card Numbers, Investment Account Connecting Numbers, Insurance Policies, and more.

Personal Information

Everyone has financial information that is stored on a Server for you to access your banking, investing, products, and services. The problem with information of this magnitude is that the responsibility is usually placed upon the bank, investment firms, stores, and service websites and entities that we use everyday. We do not always think that our information can and will be compromised. We put much trust in corporations and online entities to store our information especially our financial identity.

This includes:

Bank Accounts, ACH Numbers, Debit & Credit Card Numbers, Investment Account Connecting Numbers, Insurance Policies, and more.

How to Secure our Information

Create Strong Passwords

Your Passwords should consist of Letters, Numbers, and Symbols to allow a strong authentication for your accounts. Never use personal names, dates, or anything that can easily be found on social media for your passwords. Think abstract!

Keep Life Info Private

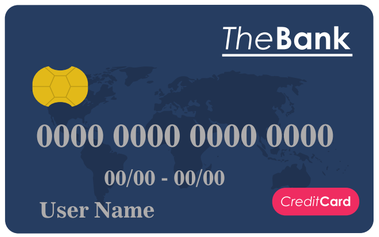
On Social Media it is easy to assume that everyone likes you and you are sharing your life with pets, places, past experiences, and likes. Unfortunately these are targeted by hackers for the sole purpose of building a file of information that will lead to cracking your identity. Be vague and don't disclose too much information. Keep it secure.

How to Secure our Information

Know the Risks of Apps

We are app driven and the fact that apps help us with our daily living makes it even harder not to use them. We are not suggesting that apps are bad or not secure. Be careful when using apps. Make sure your information is secured and set with authentication software from a third party such as Google Authenticator, Microsoft Authenticator, or Authy. These add another wall of protection when logging in and out of your apps.

Limit ACH Deposit Info



Using ACH Deposit or Withdrawal information is a risk. It is easier due to the variable of allowing funds to transfer (deposit & withdrawal) quickly without fees. Drawbacks are that unlike a Debit / Credit Card, if your Checking account is compromised; your ACH is now compromised and will have to be fully deleted from your bank account which upends your account. A new account must be created for security. This can be a significantly grueling process verses replacing your debit card.

Your End Goal

Knowledge is Power and **Action** is Key

Stay informed & follow the steps for a more secure life!

techpocus.com©