20 Tips for Securing Your Online Presence

Tip #1

Use Strong, Unique Passwords

Be sure to use passwords that are complex and unique for every account. Each one should contain a combination of letters, numbers and special symbols to ensure stronger security.

Tip #2

Enable Two-Factor Authentication (2FA)

To add an extra layer of security.Enable 2FA wherever it's possible. This ensures that you have an extra layer of protection against unauthorized access. It will be sent as a code to your phone or email.

Tip #3

Keep Software Updated

Be sure to update your software regularly. This includes your operating systems, apps, browsers, and additional software you may be using. If necessary, enable automatic updates.

Tip #4

Be Wary of Public Wi-Fi

When using public Wi-Fi networks, please be sure to avoid accessing sensitive information. If you must, please use a VPN to encrypt your connection.

Tip #5

Use a VPN

Virtual Private Network.Or VPN will encrypt your Internet connection to ensure that your data is private and secure. This can be useful when you're connected to a public network.

Tip #6

Monitor Your Accounts

Be sure to review your accounts on a regular basis for any unauthorized transactions or changes.Particularly your financial and online accounts that you use regularly. If you notice any suspicious activity, please report it immediately.

Tip #7

Watch Out for Phishing Scams

Be cautious of any emails, messages or calls that are unsolicited. Especially when they're specifically asking for any sensitive information. You should verify the sender's authenticity.Before you hand over any data.

Tip #8

Be Careful with Your Personal Information

You want to limit the amount of personal information that you share online. Be sure to adjust and review any privacy settings on platforms that you use, including social media.

Tip #9

Back Up Your Data Regularly

Backing up your data on a regular basis to an external hard drive or cloud storage will help protect you against data loss even if you fall victim to a cyber attack. This way you can be able to retrieve the data and easily restore it to a new system.

Tip #10

Educate Yourself on Scams

Be sure to keep yourself in the loop about common online scams. These include, but are not limited to, phishing, social engineering, and malware. Awareness can help you avoid becoming another victim.

Tip #11

Use Encrypted Messaging Apps

For private conversations you want to use messaging apps that feature end to end encryption.

Tip #12

Check for HTTPS

When visiting a website.Check for HTTPS.In the address bar. The S indicates that the connection will be secure.

Tip #13

Secure Smart Devices Accordingly

Use any smart devices. It is important to utilize strong passwords and also regular software updates. Shut off any features that you may not be using to minimize any risks.

Tip #14

Use Secure Browsers

A browser That focuses on security and privacy Work as one of your best tools.Especially when it has features like ad blockers and private browsing.

Tip #15

Limit App Permissions

Be sure to review the app permissions and also restrict any unnecessary access to your data.This also includes permissions to reveal your location, microphone, and contact information.

Tip #16

Be Careful with Downloads

Sure to download software and apps from trusted sources. Do not download any email attachments from senders that are unknown to you.

Tip #17

Create Guest Networks

If you have smart Devices Or guess who want to use your Wi-Fi, Be sure to create a separate guest network. This will ensure that your primary network will be even more secure.

Tip #18

Log Out of Accounts

Always log out of any accounts that you use after you're done with them. This is especially if you are using a public or shared computer.

Tip #19

Review Your Security Settings

Regularly check and adjust the security settings on each of the devices that you use. Do the same to your accounts so they are set up for maximum protection.

Tip #20

Educate Others

One of the best ways to stop cyber attacks is to make other people aware. Be sure to inform your family, friends and employees, assuming you own a business, to help them secure their online presence as well.The more people apply to these practices, the better.