



CYBER SECURITY TIPS

INDIVIDUAL EDITION

Matt Meline, CFP®

Founder and CEO

Registered Representative of Sanctuary Securities Inc. and Investment Advisor Representative of Sanctuary Advisors, LLC. Securities offered through Sanctuary Securities, Inc., Member FINRA, SIPC. "Advisory services offered through Sanctuary Advisors, LLC, an SEC Registered Investment Advisor." PrairieFire Wealth Planning is a DBA of Sanctuary Securities, Inc. and Sanctuary Advisors, LLC.

PRAIRIE FIRE

W E A L T H P L A N N I N G

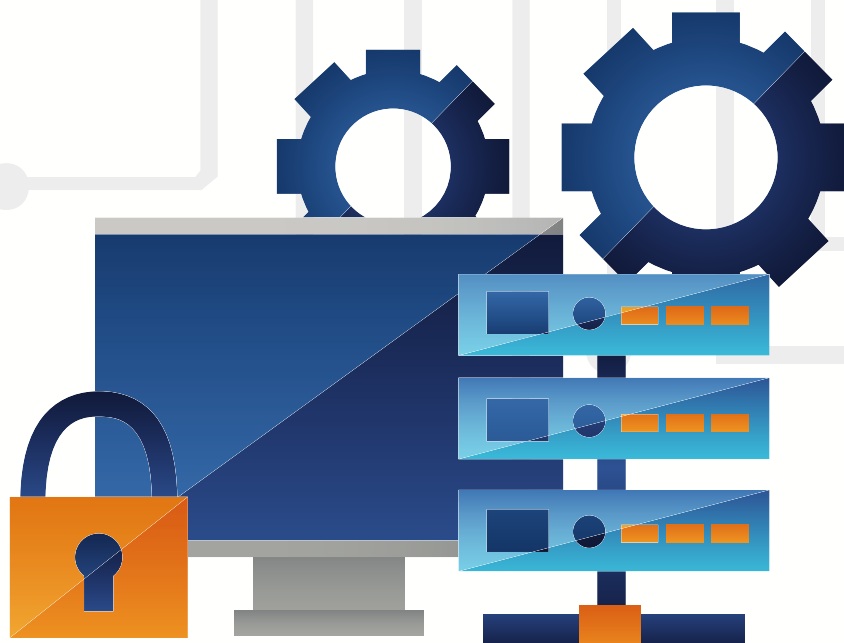
INTRODUCTION

The mid 20th century was disrupted by the Information Age. In this current age, your data is the most valuable resource. Modern wars are fought in cyber space – not with guns.

Information technology impacts our lives daily. By the end of the 1980's, cellphones became one of the most widespread technologies. These tiny but powerful computers hold information that is collected through search engines (Google), social media (Facebook), ecommerce websites (Amazon) and much more.

These large companies store your information on servers and fight off hackers trying to steal it. According to AT&T Cybersecurity, Microsoft CEO, Satya Nadella, recently revealed in a statement that the tech behemoth “will invest more than \$1 billion each year in cybersecurity for the foreseeable future”.

If you own a computer, your data is at risk of being stolen by hackers. Large corporations have the money to invest in advanced security measures, but what can individuals and small businesses do? This manual has 10 protocols that you can follow to protect your private data.



PRAIRIE FIRE

W E A L T H P L A N N I N G



1

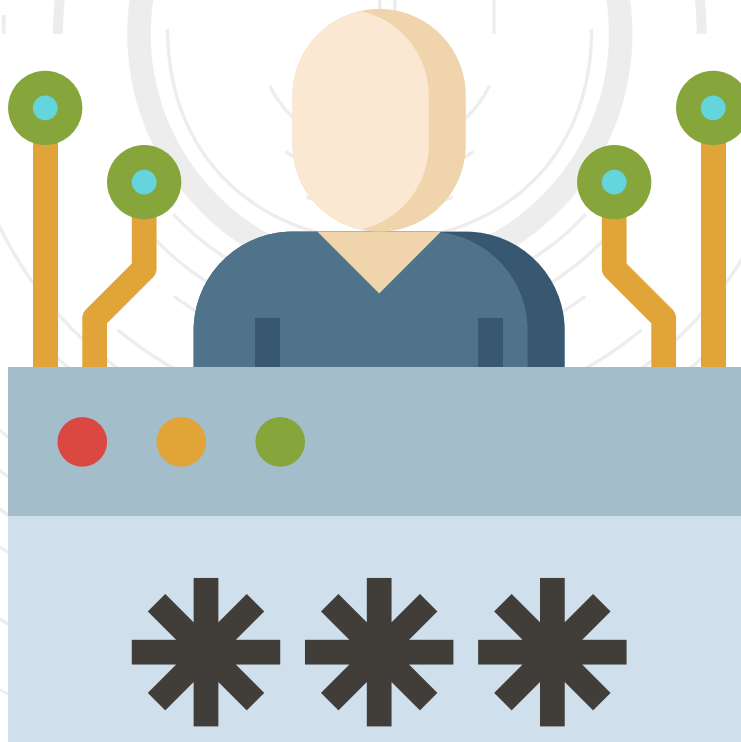
UPDATE YOUR COMPUTER

No matter what kind of computer you're using, make sure you update its software. You can do this manually or turn on automatic updates. Just navigate to the settings on your device and look for software updates. You should do this for both your cell phone and desktop computers.

2

USE STRONG PASSWORDS

One of the worst things you can do is use the same password for all of your accounts. Choose one that has a mix of letters, numbers, and symbols and change it regularly. You can use a free password manager like LastPass. It will automatically generate passwords for you and save them securely in one central place.



PRAIRIE FIRE

W E A L T H + P L A N N I N G



3

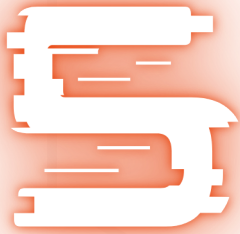
INSTALL AN ANTIVIRUS

Your computer's native software may have some security in place, but installing antivirus software will add an extra layer of security. There are many antivirus software programs like Microsoft Defender and Kaspersky Security Cloud that you can download for free. This software will watch out for harmful websites or internet scams.

4

RECOGNIZE SAFE URL'S

When you go to a website, make sure it has an HTTPS tag in the name at the top of your screen. This is usually more secure than an HTTP tag, especially if you're entering payment information. A safe website will also display a green padlock icon to the left of the website's URL. You can click on it to verify its security details.



DON'T TRUST POP UPS

Similarly, never download or install something you didn't go looking for. If a website tells you Flash is out of date, Chrome needs to be updated, or a plugin needs to be added, pump your brakes. This is a common trick to get you to install something for an attacker. If you think the pop-up might be legitimate, you still don't want to click on it.



INTERNET OF THINGS

Internet of Things devices are popping up everywhere. The more devices you add to your home, the greater the risk as they are often unsecured and run vulnerable software that provide hackers a direct pathway into your internal network.

PRAIRIE FIRE

W E A L T H P L A N N I N G



7

MONITOR YOUR BANK ACCOUNTS FREQUENTLY

Review your statements, credit reports, and other critical data on a regular basis and report any suspicious activity.

8

SOCIAL SECURITY

When you're shopping online and about to check out, make sure the required information is reasonable and necessary. No online store will need your Social Security number to make a sale. Your social security card and information should be memorized and locked away in a safe.

9

AVOID 401K SCAMS

Make sure you are on your own private WiFi when doing online banking of any kind. You should also set up two step authentication for your 401k accounts. This means there are two walls of security that only you can bypass with certain passwords or keys.

10

SAFE SOCIAL MEDIA

Be careful of what information you share publicly on social media. Even if you delete a post, it stays on the servers and might have been seen/saved by someone else. Only interact with people you know and keep your account private.



Matt Meline, CFP®

Founder and CEO

matt@pfwplanning.com

515-334-4055

www.pfwplanning.com



Registered Representative of Sanctuary Securities Inc. and Investment Advisor Representative of Sanctuary Advisors, LLC. Securities offered through Sanctuary Securities, Inc., Member FINRA, SIPC. "Advisory services offered through Sanctuary Advisors, LLC, an SEC Registered Investment Advisor."

PrairieFire Wealth Planning is a DBA of Sanctuary Securities, Inc. and Sanctuary Advisors, LLC.