ARE YOU READY

to reduce your chances of becoming the next Cybercrime victim without purchasing additional products/services or having an advanced degree in computers?

CYBERSECURE MINDSET

I'm

SCOTT AUGENBAUM

Retired FBI Supervisory Special Agent, Author, Keynote Speaker, and Cybercrime Prevention Trainer. I spent most of my 30-year career handling Cybercrime investigations. In January 2019 I released my book "The Secret to Cybersecurity, A Simple Plan to Protect Your Family and Business from Cybercriminals". It gave me an opportunity to share my thoughts about Cybercrime prevention with the world and also led to accomplish a major personal goal. I was interviewed on popular News broadcasting programs and even shared my message on the Dr. Phil Talk Show to his multi-million viewers.

During my tenure with the FBI, I interviewed well over a thousand Cybercrime victims and discovered commonalities which I call the “The Four Truths About Cybersecurity”

TRUTH ONE

**Not a single victim ever expects to be a victim.
Every victim is caught off guard.**

TRUTH TWO

**Once the Cybercriminals steal your money or
data it was almost impossible to retrieve.**

TRUTH THREE

**Since most of the Cybercriminals are located outside the
United States, the chances of law enforcement bringing them to
justice is harder than getting your money or data back.**

TRUTH FOUR

**Most of the Cybercrime incidents could have been prevented
if the victims were armed with a couple of key pieces of information.**

CYBERCRIME

Modern Day Security Crisis

Unfortunately, the Cybercrime problem continues to get worse and wreak havoc on government agencies, large enterprises, small businesses, non-profits and even families. No one is immune from becoming a victim of Cybercriminals, from the elderly to children. As the annual global cost of Cybercrime keeps increasing, the amount of money being spent to mitigate the threat increases at almost the same rate.

What does it really mean when we keep spending time, resources, and money to fix a problem but the problem keeps getting worse? It means we are not doing things correctly. Some might call it Einstein's New Theory of Insanity.

You might say I am oversimplifying the problem. But I respectfully ask, if a majority of the Cybercrime incidents dealt with could have been prevented, then why are we not focusing on these issues?

CYBERSECURE

Mindset Framework

During my decades with the FBI, I researched and analyzed the root causes of cybercrime victimization. Through this work, I created the Cybersecure Mindset Framework, which, if followed, will help you reduce your chances of becoming the next cybercrime victim without purchasing additional products and/or services or needing to have a technical background.

If you focus on the following steps and understand the strategies behind them, then your money and data will be safer – and you will proactively help prevent Cybercriminals from destroying your life.

1. Understanding the Scope of the Cybercrime Problem.

The Cybercrime problem continues to grow and we keep spending more money on products and/or services hoping they will keep us safe. Spending money on products and/or services is important. However, it is not enough. Nothing beats embracing the Cybersecure Mindset

2. Understanding the Four Truths of Cybersecurity.

If I learned anything about Cybersecurity from my decades with the FBI, I can assure you that the chances of law enforcement 'saving the day' is practically zero. That does not mean you should give up hope as a majority of Cybercrime could have been prevented if the victims were armed with a couple of key pieces of information and a few simple controls.

3. Phishing, text messages and telephone calls are the weapons of choice for Cybercrime Criminal.

For the past twenty years, Cybercriminals have been using social engineering techniques to trick end users to turn over their account credentials and install malware. This resulted in money and data being stolen and used by others. When you get an email, text message or telephone call from someone you know and trust, that message likely passes through your spam filter and email protection. Nevertheless, you need to think twice.... if not more.... before you click and act. Your first line of defense is becoming your own human firewall.

4. The Dark web and Password Reuse are a Cybercriminals best friend & lead to a majority of Cybercrime victimizations.

The Dark web is a real place where literally billions of usernames and passwords are bought and sold by Cybercriminals. These passwords were obtained through major data breaches. The Cybercriminals count on the fact that 66% of the population uses the same username and passwords on multiple sites. I bet that YOU use the same password for important sites?

5. Identifying your mission critical accounts.

Imagine a CyberCriminal who finds one of your passwords on the Dark web and, from knowing that one password, is able log into your financial, work or cloud accounts. That happens every day to millions of people and the results are always good for the CyberCriminal and bad for the victims. Do you know which accounts you need to protect? Now is the time to identify those important accounts.

6. Creating and remembering strong passwords.

Now that your mission critical accounts have been identified, you need to make sure you have a strong robust DISTINCT password for each one. A good password should be twelve characters (of course, fifteen is much better). I use special symbols, numbers upper- and lower-case letters and no dictionary words. Consider using passphrases to remember your complex passwords.

7. Making Two Factor Authentication (2FA) your best friend.

Even with a strong robust password for all your mission critical accounts, Cybercriminals still can get access to your password. That's why two-factor authentication (2FA) was created. Think of it as a second lock/dead bolt on your front door. The password is the first key for entry but you need the special six-digit code (that you obtain from an authenticator app or directly from the website host via text message) to gain complete access. This is such an important control that everyone needs to install right away wherever it is available!

8. Understanding and preventing the Business Email Compromise.

Even if you embrace all the above strategies, you must remember that your family, friends, co-worker, and vendors will most likely be subject to an account takeover. When this happens, you will get an email from them. The business email compromise is one such scam that takes advantage of unsecured emails. This is one of the greatest financial frauds today and it tricks end users to either send money or sensitive information to Cybercriminals as the victim believes the email comes from a trusted source.

9. Ransomware: Be prepared or get destroyed.

What would happen if you found out a Cybercriminal locked up all your important files and you couldn't get them back unless you paid a ransom? And then, to make matters worse, you discover that you don't have a workable backup. Can your day get any worse? Yes, it can as now you found out the Cybercriminals also stole all your data. This is not a new issue and unless you are properly prepared in advance, the outcome will not be good.

10. Keeping Your Family Safe.

Every moment of the day the Cybercriminals are targeting our family members with fraudulent activities. Today our children and elderly parents spend a majority of their time online and the Cybercriminals know it. We need to be aware of the different scams targeting our family.

Take this information and apply it to your life and make sure you share these simple steps with your family, friends, and co-workers as it can reduce a majority of Cybercrime incidents.

The above-mentioned information gives you awareness. To help you with readiness and practice, I've developed the Cybersecure Mindset Academy. It's a collection of ease-to-use resources and secure knowledge-sharing communities that bring together Cybersecurity professionals and people just like you.

ARE YOU READY

to reduce your chances of becoming the next Cybercrime victim without purchasing additional products/services or having an advanced degree in computers?

For more information contact : scottaugenbaum@cybersecuremindset.com