BSSi2

Innovations

Review Twice, Implement Once. Doing IT Right the First Time.

THIS IS A TEST

You are a participant in a race. You overtake the second person, what position are you in?

Answer : if you answered that you are first, then you are absolutely wrong! If you overtake the second person and you take his place, you are in second place!

Try to do better next time.

Now answer the second question, very tricky arithmetic! Note: this must be done in your head only. Do not use paper and pencil or a calculator. Try it.

Take 1000 and add 40 to it. Now add another 1000. Now add 30. Add another 1000. Now add 20 .. now add another 1000. Now add 10.. what is the total?

The correct answer: Did you get 5,000? The correct answer is actually 4,100...

If you don't believe it, check it with a calculator!

Don't take a job in accounting.

Keep Your Business Protected By Becoming Aware Of The Most Common Types Of Cyber-Attacks

The rate of cyber-attacks has significantly increased over the past few years. Businesses of all sizes are at risk of becoming victims of them, which is why it's crucial that every business owner and leader is aware of the most common cyberthreats impacting the business world today. Being aware of common cyberthreats and developing plans to prevent them is the best way to protect your business, customers and employees from cybercriminals.

These criminals' tactics will improve as technology continues advancing, but cyber security defenses will as well. Knowing exactly what you're up against with cyber-attacks and creating the proper safeguards will protect your business. If you're new to the idea of cyber security or need an update on the common threats that could impact your business, we've got you covered. Below, you will find the most common types of cyber-attacks out there and how to protect your business from them.

Malware

Malware has been around since the dawn of the Internet and has remained a consistent problem. It is any intrusive software developed to steal data and damage or destroy computers and computer systems. Malware is an extensive type of cyber-attack, and many subcategories belong to it, including viruses, spyware, adware and Trojan viruses. One type of malware that has lately been used more frequently is ransomware. Ransomware threatens to publish sensitive information or blocks access to necessary data unless a sum of money is paid to the cybercriminal who developed it.

Unfortunately, malware can be detrimental to nearly every operation of your business, so you should do two essential things to prevent it from affecting your company. First, you should install the latest anti-malware programs. If you hire a services provider, they will take care of this for you. If not, you'll need to find anti-malware that works best for your system. You should also train your team about these risks and ensure they are aware not to click on any suspicious links, websites or files that could be dangerous.

Continue on the next page...

Continued from previous page...

Phishing
Have you ever received an e-mail asking for sensitive information that looked official, but something just wasn't quite right? Chances are it was probably a phishing scam. Phishing occurs when cybercriminals send official-looking messages to individuals, posing as another organization, in an attempt to receive personal information. Falling for a phishing scam can quickly result in you becoming a victim of identity fraud. The results can be substantially worse if a business falls for the scam.

So, how do you best prepare for and protect your team against phishing scams? Utilize employee cyber security trainings so they can spot the warning signs. The actual e-mail will usually line up differently from whom the cybercriminal is trying to represent. Also, most organizations will not request private information over e-mail. Common sense will prevail over phishing scams.

Distributed Denial Of Service
DDoS attacks can bring your business to a standstill. These attacks occur when malicious parties overload servers with user traffic, causing them to lag or shut down since they are unable to handle incoming requests. If your business falls victim to this kind of attack, your employees might not be able to access key functions required to do their jobs, and customers may not be able to use your website or purchase items from you.

DDoS attacks are very difficult to thwart, and a determined cybercriminal can lock up your websites and networks for days on end. You'll have to identify malicious traffic and prevent access before it can cause damage. Hiring an MSP is your best bet to prevent DDoS attacks. If a DDoS attack is successful, you'll probably have to take your servers offline to fix the issue.

Password Attacks
If a cybercriminal gets your password or another employee's password, this is the easiest way for them to access your valuable information. They may attempt to guess the passwords themselves or use a phishing scam to gain access. It is vital that you enable multifactor authentication for your employees and require complex passwords so you can defend your company against password attacks.

Now that you know the most common forms of cyber-attacks currently happening, you can take the necessary precautions to protect your business, employees and customers.

"Being aware of common cyberthreats and developing plans to prevent them is the best way to protect your business, customers and employees from cybercriminals."

On the Lighter Side

How Distractions Steal Your Money and Peace of Mind by Bill Ulivieri

In the audiobook '*Stolen Focus; Why You Can't Pay Attention ---and How to Think Deeply Again*", by Johann Hari, the author takes a deep dive into our culture and why we cannot focus for any length of time on tasks or topics.

As a race our mental focus has been in decline for centuries, but has accelerated exponentially in the past 15 years since the rise of social media and the smartphone.

It's a *perfect storm* for the collapse of intelligence and deep thinking. Hari blames social media because it trains our mind to skim and skip the information we consume on smartphones. We no longer read hardcover books and let information quietly steep in our mind.

Push notifications inject dopamine in our veins as instant gratification alerts force us to be always online.

Like a magician performing slight of hand tricks, the media is an expert in distracting our focus. We focus on what they want us to focus on and therefore nudge our decisions and beliefs.

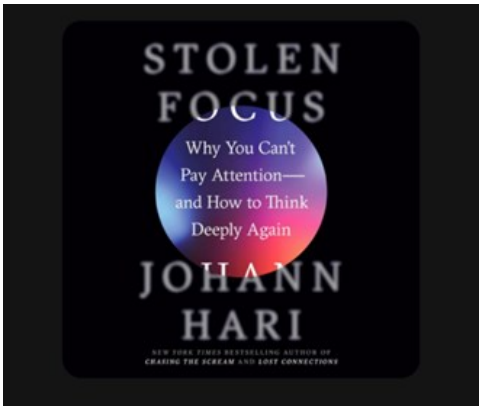
The science of persuasive decision making is studied in universities around the globe and the core results are monetized by social media companies. This isn't a conspiracy theory. Just watch the documentary "The Social Dilemma" on Netflix.

I'll rate *Stolen Focus* a "10" on a scale of 1 to 10, 10 being the best. How does this relate to our retirement accounts?

From my perspective the market "skips and skims" from one crisis to another causing ***fear***.

Fear of loss makes us sell at market bottoms; while FOMO; **Fear** of Missing Out compels us to overpay at the top.

I'm no longer perplexed to why the market has become more irrational in its behavior. Hari's book explains something I knew but struggle to describe.



This phenomenon sheds light on the 2018 stock market despair, 2019 hopeful optimism, the 2020 pandemic depression, the unbelievable 2021 peak expansion in prices and the 2022 Technology / bond market collapse.

Since 1980 I have never seen such extremes. What's in store for 2023? More of the same I'm afraid to say. Only 43 days in and it's Chinese spy balloons, recession fears, tech layoff's, nuclear missiles, prohibition on gas stoves, the skyrocketing price of eggs, unexpected deaths, the US military blowing up pipelines.

They're stealing our retirement funds and peace of mind by stealing our focus.

I do not submit.

This is the hamster wheel we're on. Hari's book says scientific studies prove our attention span is pulled in any direction social media want it to. We're described as "easily manipulated chunks of meat".

We must not submit. We must be relentless in our discernment of external noise and distraction. We must reclaim the desire to spotlight our focus one task or topic instead of believing we can successfully multi-task. We must read books.

Bill Ulivieri, AIFA(r) is owner and managing director of Cenacle Capital Management, LLC, a state registered investment advisor, using low cost Exchange Traded Funds. His role as CEO of Mining Rig Solutions, LLC has placed him at the forefront of disruptive technology by providing informative presentations on Bitcoin, Blockchain and Distributed Ledger Technology to C-Suite executives. He can be reached 847-686-4800 https://cenaclecapital.com/

March 2023

35 Aztec Court
South Barrington, IL 60010
(312) 752-4679
www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

Shiny New Gadget of the Month

Valve's Steam Deck

Nintendo, Microsoft and Sony are some of the most prominent players in the video game console industry, but there's another name making headlines in these console wars: Valve's Steam Deck. In fact, this is the perfect gaming system for anyone who is looking for a powerful and portable console.

The handheld system is capable of playing the most advanced AAA games available and comes in three different storage sizes. If you've used Steam in the past on your PC, you'll immediately gain access to your library of games and will be able to purchase any other games from Steam directly on the device. Check out the Steam Deck if you're in the market for an affordable, powerful and portable gaming PC.

Stay up-to-date with the latest Cybersecurity News!

Follow our Chief Security Fanatic, Nick Espinosa, on social media for cybersecurity videos and articles:

F www.facebook.com/NickAEsp

twitter.com/NickAEsp

I www.linkedin.com/in/nickespinosa/

Follow BSSi2 at:

F www.facebook.com/bssi2

twitter.com/BSSi2llc