



Technology Update

The SaviorLabs technology publication for power users.

Welcome!

by Paul Parisi

Welcome to **Episode Two** of the infamous **SaviorLabs Technology Update Newsletter**. This month, we delve into how hackers work, what ChatGPT is and why it's going to change the world, our book of the month: *Never Split the Difference: Negotiating As If Your Life Depended On It*, recent important happenings with Comcast email and Apple updates, some humor, and so much more!

As always, **please keep us up to date with what you'd like to see covered next.**

Be sure to scan the QR code at the end of this issue (pg. 6) - scanning the QR code will bring you to an online index of all the references used in this issue. Also, please visit our website to keep in touch!

Enjoy!

Humor

Following the theme of keeping it dynamic and interesting, this issue features some of SaviorLabs' founder and president Paul Parisi's favorite jokes.

A message from Paul: "Considering all that is happening in the world, we hope that we're able to make you laugh with some light humor! Here are some truly terrible dad jokes harvested from the internet over many years.

We hope you enjoy the issue!"

Without further ado...

- Why are elevator jokes so good? *They work on so many levels.*
- Why did the guy get fired from his job at the orange juice factory? *He couldn't concentrate.*
- What do you call an alligator in a vest? *An investigator.*
- What do you call a fake noodle? *An impasta.*
- Why does a chicken coop have two doors? *Because if it had four doors, it would be a chicken sedan.*

- Why don't cannibals eat clowns? *They taste funny.*
- What did the left eye say to the right eye? *Between you and me, something smells.*
- Why can't you hear a pterodactyl go to the bathroom? *Because the "P" is silent.*
- What do you call a group of rabbits walking backwards? *A receding hare-line.*
- Where did the general put his armies? *In his sleeveies.*
- What did the father buffalo say to the boy buffalo when he went to school? *"Bison."*
- Where are the spiciest peppers commemorated? *The hall-of-peño.*
- What do you call a can opener that doesn't work? *A can't opener.*

Attention – Xfinity Users!

Recently, an undisclosed number of Comcast email accounts were hacked. **If you have a Comcast email address, we strongly recommend that you reset your password as soon as possible. This attack is a prime example of why it's a great idea to regularly change your password!** Good password security is one of the most important and effective ways to circumvent a cyberattack. **Please make sure that your password is secure by updating it regularly, never including personal information, and using the tips mentioned later in this issue!**

If you are subscribed to <https://horizon.saviorlabs.com>, you know about this breach already. For more important updates like this, **I encourage you to subscribe as soon as possible.** Just fill out the **"Subscribe Now"** form on the front page of our website.

Did you know?

Every continent except for Antarctica has at least one McDonald's...

McCrazy, right?



How Hackers Work: The Single Biggest Threat

by Paul Parisi

The single biggest asset to your business is **you and your people**. However, the single biggest threat to your business is **also you and your people**.

Let me explain. Hacking into a computer or system can be very difficult and it takes a lot of time and effort to crack a password. For example, I have been working on cracking the password to a friend's PDF file for weeks. I checked over 14 million passwords in less than 12 hours and nothing worked. The issue with his password was that he made it complicated- so complicated that he forgot it. Because his password is so complex, it will take either me being smarter or more patient in order to crack it. **Brute force password hacking**, as it is called, is not easy and may prove unfruitful. **So why are we all worried about getting hacked?** Remember what I said was the biggest threat to your business? **Your people.** Why? Because sometimes people do things without thinking it through, especially when it comes to the internet. So, **the easiest way to get the information needed to access a system is to simply ask for it! The majority of breaches occur because someone gives away information to someone they shouldn't have.**

Questions like: *"Where did you grow up? What high school did you go to? What is your favorite animal?"* may all seem benign. But what if I were to write these answers down and associate them with you? You may think that no one is going to target you. **Wouldn't cybercriminals want to go after bigger fish?** Hackers don't care who you are. They have built complex systems to harvest all the information they can about you and then use that to get your login and password. (Just so you know, there are large profes-

sional office buildings staffed with some of the best and brightest, working daily on how to gather all this information about you. **They even use Google to do the work for them.**) Now you're probably saying: *"That's ridiculous. It can't really be that easy to get hacked. I'm careful!"*

Let me ask you a question. Have you ever seen a quiz on Facebook and taken it? Have you ever been asked what your favorite color says about you, so you enter it into a website, and it tells you that you are gentle, smart, and decisive? You get the point. There it is. **It just happened!** Now someone knows your favorite color. This happens all the time, and **each little piece of personal information is tied to you on the internet forever.** Not only simple things like your favorite color, but also where you grew up, your favorite sports team, and so on; even things you are interested in can be used against you. (That gets us into advertising. See last month's issue of our Newsletter for more on that). Now you may ask: *"What can a hacker even do with my favorite color?"*

Many websites require you to answer confidential questions to recover your password. They might ask you what the name of your first pet is or even your favorite color. You then enter one of the above, and you can reset your password. **A hacker can do the same thing**, and since they know your favorite color because you took that quiz, they can now login as you. Hackers use bots to do it automatically. Once they get in, reset your password, and login as you, **they can do whatever they want. Anything you keep on your computer or other devices is fair game!**

Another tactic is to send you a link to a website with a phishing email. (We covered the definition of phishing in last month's newsletter. In short, **phishing is fishing for information.**) For example, you receive an email from a seemingly legitimate email address saying that you have an abnormal charge on your credit card. In the email is a link to your bank of choice, so you click on the link and log in to the fraudulent site with your real information. **Now the phishing scammers have your banking details.** If, for some reason, you forgot your password, you may have tried to enter a few different options. **Now the scammers have several of your current passwords.**

There are two takeaways from that:

1. **Phishing is sneaky and often undetectable unless you learn to expect it and look out for it.** (See last month's issue.)
2. **Never use the same password for more than one site.** If you use one password for everything and a cybercriminal gets it, **they can hack everything.**

Now you're left with one question: "How do I prevent that from happening?"

The Solution

Although you might think a custom, personal password might be hard to crack, as stated above, that's not the case. Instead, a randomly generated password that looks more akin to a keyboard smash than anything comprehensible might be the solution.

Then you might ask: "How do I create a password that's truly hard to crack?"

Tip 1. Use a password generator.

Here is an example of one of the passwords created using a password generator: **6u\$D\$3nQU6udB#o5^gawATY%**

It is *24 characters long* and includes *numbers (0-9), uppercase letters (A-Z), lowercase letters (a-z) and assorted special characters (!@#\$%^&*)*.

Tip 2. If not using a password generator, use a combination of numbers, characters, and upper and lower case letters that adds up to at least 12 characters. (We recommend 24 characters, but 12 is the minimum.)

Here are two examples of passwords using that combination made up on the spot:

12 characters (*the minimum*):

&78k*Lb45\$SsW

24 characters (*our recommendation*):

98KJL\$F34Re@!112ghLKJ^5

Now that you have your passwords set, you might ask: "How will I possibly be able to keep track of them all?"

Well, that requires us to spend some time talking about **password managers**.

Tune into next month's issue to find out more about that.

What Is ChatGPT?

by Paul Parisi

If you haven't heard of ChatGPT, *you will. ChatGPT is going to change the world.* No, this is not an overstatement. It is an incredible, innovative new way to interface with a computer **that has most of the information indexed from the internet.** The "Chat" part is simply that! Having a chat (via typed text) with the computer. Imagine you're curious about how to optimize your gas mileage, so you ask:

What is the best way to get better gas mileage?

Here is the answer from ChatGPT:

Improving your gas mileage can be beneficial for both your wallet and the environment. Here are some tips that can help you get better gas mileage:

- 1. Maintain Your Vehicle: Regular maintenance of your car can help improve gas mileage...*
- 2. Drive More Efficiently: Driving more efficiently can also help improve your gas mileage. Avoid aggressive driving, excessive idling, and speeding...*
- 3. Reduce Weight: The more weight your car carries, the more fuel it consumes...*
- 4. Plan Your Trips: Combine multiple errands into one trip to reduce the number of times you have to start and stop the engine.*
- 5. Use the Right Fuel: Using the right fuel for your car can also improve gas mileage...*

By following these tips, you can increase your gas mileage and save money on fuel costs.

This fundamentally changes the nature of the quick internet search. We no longer have to carefully sort through page after page of what a search engine is returning. **ChatGPT does that for you.** Only time will tell if that analysis is correct: whether biased, unbiased, true, or false. But it will do so in plain English.

To better explain what ChatGPT even is, GPT is an acronym for **Generative Pre-trained Transformer**. In more detail:

Question:

Describe GPT.

Answer from ChatGPT:

GPT (Generative Pre-trained Transformer) is a type of large language model developed by OpenAI, which uses deep learning techniques to understand and generate natural language. The model is pre-trained on a massive amount of text data, such as books, articles, and web pages, which enables it to learn the patterns and structure of human language.

GPT uses a Transformer architecture, which is a neural network that can process sequences of data, such as words in a sentence, in parallel. This allows GPT to generate human-like text by predicting the most likely words to follow a given sequence of words.

The model has been trained on a diverse range of text data, which allows it to generate text on a wide

variety of topics and in different styles. This makes GPT a versatile tool for tasks such as language translation, question-answering, and text completion. GPT-3, the latest version of the model, has 175 billion parameters, making it the largest language model to date.

So how do we use all this information?

We ask a question, and, depending on how we ask the question, we will get a corresponding answer. This is fun in theory, but in practice, it's a bit more nuanced. Here is an example of another interaction with ChatGPT:

Question:

Write a brief interesting article introducing the new newsletter from SaviorLabs called Technology Update and how it can help medium-sized business owners better manage their IT systems and security and leverage technology to make business more efficient.

Answer from ChatGPT:

SaviorLabs, a leading provider of technology services for businesses, has recently launched a new newsletter called Technology Update. The newsletter is specifically tailored to help medium-sized businesses owners better manage their IT systems and security, and leverage technology to make their operations more efficient.

As businesses continue to face new challenges, technology has become more critical than ever. But keeping up with the latest developments in technology and ensuring that your IT systems and security are up to par can be a daunting task for many medium-sized businesses. The SaviorLabs Technology Update newsletter aims to solve this problem by providing businesses with timely and relevant information on the latest technology and security trends.

The newsletter covers a wide range of topics related to IT systems and security, including network infrastructure, cloud computing, data backup, and disaster recovery. It also provides practical advice and guidance ... through real-world case studies and expert advice.

...The newsletter is a valuable resource for any business owner looking to streamline their operations and stay competitive in today's fast-paced business environment.

It's obvious ChatGPT has some incredible value to offer today, and the sky is the limit for the future.

However, I stumbled upon a confession ChatGPT made. "As an AI language mod-

el, my training only goes up until September 2021, so I cannot provide the most current updates." That is a long time ago, especially in Internet time. I'm sure the data will be updated and incorporated more quickly.

Until then, **happy chatting!**

Featured Book of the Month

by Paul Parisi

One my favorite business books is *Never Split the Difference: Negotiating As If Your Life Depended On It*, written by former FBI hostage negotiator, Chris Voss. **This book is a secret weapon to understand and work better with people.** He provides practical advice for negotiating effectively in a wide range of situations, including business, politics, and personal relationships. *Everything is a negotiation, even getting up in the morning.*



Voss argues that the key to successful negotiation is to adopt a collaborative mindset and focus on the needs and interests of the other party. He also stresses the importance of effective communication and active listening, and provides techniques for defusing conflict and building trust.

Overall, the book is designed to help readers become more **skilled, confident negotiators**, whether they are trying to secure a higher salary, resolve a dispute, or simply get what they want in their daily lives.

I cannot recommend this book more highly. Get it in paper or audio format today and read it. You won't regret it! We've included a link to Amazon to make it easier- *it's just that good!*

<https://a.co/d/1hOPjGi>

**We Keep Your
Computers Working
Your Network
SECURE**

Trust and Technology

by Paul Parisi

In this month's issue, I wanted to talk about the idea of "zero-trust".

I work with lots of users and their networks, and one thing I often notice is they assume that their network is secure. In reality, **often their network is not secure**, and is, in fact, a lot more likely to be a conduit to pain, suffering, and **exploit**. Think about it. The mysterious network I'm referencing is the place where all the computers are connected and able to communicate freely with each other. Normally this wouldn't be a concern, but **what happens if someone connects to your network that is a bad actor and deliberately wants to exploit your systems? These bad actors would then have the ability to probe and test your entire network and all its devices.**

This is one of the main reasons why we have to make sure each and every one of your computers is fully protected. Recently, there was a vulnerability discovered in Windows that allows an attacker easy access to a computer by using a flaw in the Remote Desktop Protocol (RDP). **Many computers have RDP enabled, so having RDP enabled and not having your computer fully patched presents an extremely easy target.**

Now, I know what you are thinking. "We don't allow outsiders access to our network." That is a good policy to have. However, **what happens when a computer, even one of your managed computers, gets compromised?** Let's imagine that one of your employees takes a laptop out of the office and into the world. **If it gets compromised and then that computer reconnects to your network, bingo! That compromised machine is used as an access point to attack all the computers on your network.** On many occasions I have talked with business owners about things like this and they say, "No one would want to target little old me..." But if you look at what I have written up until this point, I didn't mention any targeting! These attacks are completely automated. When a crack in your security is found, **the breach is transmitted back to a command-and-control infrastructure, and then they task your computers to do their bidding.**

So, **how do we fix all of this?** First and foremost, **we should never trust any network**, hence "zero trust networks." We need to assume that every network we connect to could be death and the destroyer of worlds. **We recommend a multilayer approach to security**, which I will discuss in detail over the coming issues. **Two critical components to help**

prevent compromise of computers while "in the wild" is to always make sure that the computer is fully updated and to always use a VPN when connecting via a public network.

Hopefully this has been helpful and has gotten you thinking. **Don't let the things you know you should be doing something about languish too long. It's your responsibility to make sure your systems work for your company.** And, a reminder, **please forward your technology questions along and we will get them addressed!**

Apple Security Updates Needed NOW!

by Paul Parisi

If you have an iPhone 8 or newer running iOS or iPadOS 16, **be advised that there are new, important updates crucial to the security of your devices! So important that you should stop what you are doing and install the update now.**

There is a huge security flaw, and it's a great example of why we should keep all of our operating system and application software up to date. Any app on your Apple device can run and execute any code it wants to with the highest privileges.

This specific exploit allows hackers to gain full control over an iPhone or iPad.

Naturally, we expect that our devices are always secure, but software bugs can fall through the cracks. **When a bug is discovered by someone**, in this case Xinru Chi of Pangu Lab and Ned Williamson of Google Project Zero, **a race starts between the release of the exploit, hackers' attempts to leverage the bug, and the company (Apple, in this case) to fix the bug.**

In order to prevent you and your Apple technology from being exploited, be sure to update your devices as soon as possible!

See Apple's iOS 16.3.1 security page for more details and a link to the technical articles about these exploits.

For a good overview, read Apple iOS 16.3.1 Release: Should You Upgrade? (forbes.com)

Contact Us

SaviorLabs, 978-561-6025

info@saviorlabs.com

https://saviorlabs.com

READ THIS NOW

In This Issue

- Welcome 1
- Humor 1
- Attention — Xfinity Users! 1
- How Hackers Work: The Single Biggest Threat 2
- What Is ChatGPT? 3
- Featured Book of the Month 4
- Trust and Technology 5
- Apple Security Updates Needed NOW! 5

SaviorLabs LLC
273 Middleton Road
Boxford, MA 01921

Place
Stamp
Here

To:

“O Lord, what a variety of things you have made! In wisdom you have made them all. The earth is full of your creatures.”

—Psalm 104:24

**SCAN
ME**

