SaviorLabs™
Managing Technology to Propel Your Growth

Episode #1 - $47
info@saviorlabs.com
978-561-6025

Technology Update

The SaviorLabs technology publication for power users.

Welcome!

by Paul Parisi

With everything being so online focused, we thought it would be a good idea to have something people could hold in their hands. **We decided to send out a monthly printed newsletter that gives good insight into today's technology so you can most effectively use it to your advantage.** Of course, there will also be some fun articles and facts along the way to keep you interested.

Most of all, we want to know what you would be interested in reading about. **Let us know what areas you'd like covered, so we can keep you in the IT loop.**

You will also see a QR code at the end of this issue (pg. 6) - scanning this QR code will bring you to an online index of all the references used in this issue. That way you can easily share them and do more research yourself (if you're interested).

Humor

This month, we decided to feature some jokes from comedian Steven Wright. Not many people realize that he was born in Cambridge and grew up in Burlington, Massachusetts. Here are 25 of his jokes that are our favorites. (For more info on Steven Wright, visit: http://www.steven-wright.com.)

1. I'd kill for a Nobel Peace Prize.
2. Borrow money from pessimists -- they don't expect it back.
3. 82.7% of all statistics are made up on the spot.
4. A clear conscience is usually the sign of a bad memory.
5. All those who believe in psycho kinesis, raise my hand.
6. The early bird may get the worm, but the second mouse gets the cheese.
7. I almost had a psychic girlfriend, ... But she left me before we met.
8. OK, so what's the speed of dark?
9. How do you tell when you're out of invisible ink?
10. If everything seems to be going well, you have obviously overlooked something.
11. Depression is merely anger without enthusiasm.
12. When everything is coming your way, you're in the wrong lane.
13. Ambition is a poor excuse for not having enough sense to be lazy.
14. Hard work pays off in the future; laziness pays off now.
15. I intend to live forever... so far, so good.
16. If Barbie is so popular, why do you have to buy her friends?
17. What happens if you get scared half to death twice?
18. My mechanic told me, "I couldn't repair your brakes, so I made your horn louder."
19. A conclusion is the place where you got tired of thinking.
20. The hardness of the butter is proportional to the softness of the bread.
21. To steal ideas from one person is plagiarism; to steal from many is research.
22. The problem with the gene pool is that there is no lifeguard.
23. The sooner you fall behind, the more time you'll have to catch up.
24. Everyone has a photographic memory; some just don't have film.
25. If at first you don't succeed, skydiving is not for you.

Did you know?

Dogs, on average, sleep for 16 hours a day... *how do I apply for that job?*

Facial Recognition **Gone Bad**?

From the American Bar Association and Ars Technica

The following is excerpted from an article in the ABA Journal from December 21, 2022, and it is **very** hard to believe.

A mom took her daughter to Radio City Music Hall to see a show, and Facial Detection Technology matched her face to a law firm that previously sued the hall. ***Let's break it down.***

First, they had to have the technology up-and-running to photograph every face. This means even minors. (It would be interesting to read the terms of the ticket to see what limits there are.) Second, they had the capability to match it to a pre-existing facial database. And third, they had to have (at the very least) the personal information of where each person worked and possibly much more. Here is some of the article. All emphasis has been added.

From the ABA article

> **A New Jersey mom taking her daughter to see a show** featuring the Rockettes as part of a Girl Scouts field trip **was recently ousted from the Radio City Music Hall because facial recognition technology identified her as a lawyer at a law firm that sued a related venue.**
>
> **"They knew my name before I told them. They knew the firm I was associated with before I told them. And they told me I was not allowed to be there,"** Conlon told NBC New York.
>
> Conlon waited outside, while her daughter saw the show.
>
> **…**
>
> Madison Square Garden Entertainment sent this statement to NBC New York: "MSG instituted a straightforward policy that precluded attorneys pursuing active litigation against the company from attending events at our venues until that litigation has been resolved."
>
> **…**
>
> Sam Davis, a partner at Davis Saperstein, told NBC New York that **the ban "is absolutely absurd,"** and **the use of facial recognition technology to implement it is "frightening."**
>
> **…**

Now back to our regularly scheduled program…

There is more wrangling going on between lawyers, judges, plaintiffs, and defendants, but the real issues are the "pay no attention to the man behind the curtain" sort of things. As I outlined in the opening paragraph of this story, the hall had to correlate a lot of data to get the fact that this mom works where she works. This is not just concerning and invasive, but downright scary. Given that the hall has done this, let alone their posturing in court, I want to pose a question: **How do we control facial recognition technology, and what is crossing the line from safety protocol into invading privacy?** But not to worry, *I'm sure this doesn't happen anywhere else…*

Be sure to scan the QR code at the end of this issue (pg. 6) for the complete article.

Notes From the Field

As you might imagine, we come across quite a few technology horror stories as we are ever vigilant in trying to protect our clients' digital assets. This month's story comes from a friend on the west coast. All emphasis has been added.

> "I just got a call from an architect, who has always said that they were too small to need IT services with only eight employees. **He just lost $61K and $170K to fraudulent wire transfers after his email was hacked a week ago.** His incoming cell calls and text messages are being redirected. His online data seems to be 'gone.'
>
> He doesn't know if they have cyber insurance, does not have an attorney, and does not know what else might be affected. **But he does know they do not need IT because they are too small to need IT support."**

This situation could have been easily prevented, but hey, small businesses don't *really* need IT support… *right?*

Computer Security Checklist

Keeping systems and data safe from cybercrime is essential for your company's future – *an estimated 60% of businesses that experience a cyberattack go out of business within a year.* This computer security checklist helps ensure that you're doing all the right things to keep cybercriminals out of your business.

- □ Make sure everyone is using a strong, unique password for every account
- □ Use multifactor authentication to protect credentials
- □ Follow safe email-handling practices
- □ Review compliance to ensure industry standards are met
- □ Eliminate unsafe password storage (in documents, on paper, etc.)
- □ Patch and update all software regularly
- □ Conduct regular security awareness training
- □ Set up alerts for compromised credentials on the dark web
- □ Create an incident response plan for security mistakes
- □ Learn more about cyberattacks like ransomware

Are you sure you're using the right security solutions to protect your business from cyberattacks?

Paul's Old PCs

by Paul Parisi

I thought it might be interesting to give you a view into some of the computers I have owned in past decades. This month's issue features:

The Timex Sinclair ZX-81

- Year: *1982*
- RAM: *1KB*
- Cost: *$99.00*
- Display: *TV*

A little over 40 years ago, I was given my very first computer. It was a Timex Sinclair ZX-81. My father bought it at a local Fay's Drug Store in Batavia, NY, for $99 in 1982 (about $300 in today's dollars). I'm sure that my mother thought he was crazy. I, on the other hand, thought it was so cool. While it did have a keyboard, it didn't have a display; it connected to the TV. It had a hard to use, flat, membrane keyboard and the computer weighed just 12 oz. It produced a black-on-white video character-based video, with no real graphics. The display screen was 32 characters across by 24 lines. 22 lines displayed the output of the program and the last two were the "input area", where users entered programs or responded to a program.

It had a whopping 1KB of memory. Today's smartphones have over 6 million times that amount of RAM. Its Z801 8-bit microprocessor ran at 3.5 MHz. Today's computers run at one billion times that speed, at 3.5 GHz. In 40 years, RAM has multiplied a million times and CPU speed has gone up a billion times. Needless to say, *we've come a long way since 1982.*

This Month's Question

Does Your Organization Perform Security Awareness Training?

Information security professionals know how to recognize most attempts to circumvent the controls an organization maintains, but this knowledge requires a significant amount of training. **Most employees simply don't have the time to learn everything that an information security professional knows.**

The goal of security awareness and training is to provide your employees with enough information to make informed decisions on which emails to interact with, which phone calls to engage with, and how to spot attempts to defraud them and their organization.

Ransomware often succeeds because cybercriminals trick employees into downloading and opening software through corrupted links on websites, or links/attachments in emails. Employees mistake these links/attachments as having legitimate business purposes, and cybercriminals prey on the employees' desire to do their job well, as well as their ignorance of how common this tactic is.

Effective security awareness and training can help an employee recognize when a cybercriminal is attempting to trick them so that they don't open that attachment or click on that link.

Some training approaches use simulations to teach, which imitate real attacks, but are really sponsored by the organization. This method can be quite effective, but when done poorly, it can erode trust between a business and its employees without teaching anything. One solution is to reward employees for making correct decisions rather than penalize them for making mistakes. Tabletop exercises are also important to help plan for situations that may occur and to educate executives and corporate boards on what an attack and response looks like.

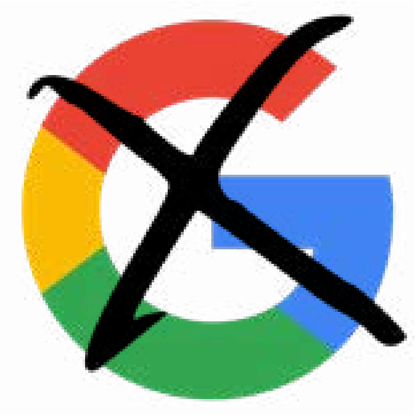
To sum up, **security awareness and training is a vital component in your business' safety and wellbeing, and *not properly equipping your employees to safeguard against cybercriminals' tactics is just as bad as leaving your front door unlocked.***

Is Google Evil?

by Paul Parisi

As for me, I say **YES.** ***I strongly recommend that you no longer use any Google software on any of your devices and that it be proactively uninstalled.*** The entire infrastructure of Google is designed to gather as much information as it can about you. Why, you ask? So that Google can sell advertising. That's how they make their money **– it's all about monetizing you.** All Google products are used to get more details about who you are and what you are interested in. They gather this information and match you to ads that have been effective on people like you. They then sell those ads to companies that want your attention and money. For example, they could buy access to people who have blonde hair, make $80,000 a year, and have a fish tank. This is just one example of what we know is being done with our data. Who knows what else they're doing. In the past, we read books like George Orwell's '1984' and tales about the future. I never imagined that we as a society would let that happen. We did and we do, knowingly or not. Using Chrome gives away far too much information to Google. **EVERYTHING you do in Chrome is tracked and sold to advertisers.**

Further, because Google website tracking is built into just about every website in the world, **Google knows what sites you visit and when you visit them.** (There are ways around this.)



How do we fix this? It's not easy. First, your data is already out there. Second, it's hard to put a genie back in a bottle. The EU's GDPR (https://gdpr.eu/what-is-gdpr/) legislation has provisions that allows users to request removal of all their data from a site, and most importantly, remove it from anyone they may have shared it with.

How do we go forward? I have removed every piece of Google software from my life. I use Microsoft Edge (Chromium) which is built on the Chromium engine (the open-source basis of Google Chrome) and gives all the benefits of Google Chrome with none of the downsides. Thankfully, Microsoft Edge doesn't have the same level of tracking as Google Chrome. But (there is always a but), Edge needs to have its settings tweaked to protect you best. However, one great bonus is that Edge has great integration with Microsoft Office.

Contact us and let us know how we can help!

SaviorLabs' Vision & Mission

Our Vision

A world in which technology helps people experience the pleasure of effectively and efficiently pursuing their purpose.

Our Mission

Helping organizations leverage technology to mature and strategize for the future.

New SaviorLabs Website

We recently launched a new website and would love to have you take a minute to look at it. We would love your feedback and any ideas on how we can improve it. ***Let us know!***

Definition of the Month

Fishing **fish·ing** (NOUN)

The activity of catching fish, either for food or as a sport.

"This lake is well-known for its excellent fishing."

Phishing **phish·ing** (NOUN)

The activity of someone posing as a legitimate institution using email, telephone, or text message to lure individuals into providing sensitive data such as Personally Identifiable Information (PII), banking and credit card details, and passwords, and then using that to access important accounts.

"This email is likely a phishing scam."

SaviorLabs: Member of FBI InfraGard!

As part of SaviorLabs' professional relationships, we have been a member of the FBI InfraGard team for some time.

InfraGard membership is designed for individuals involved with the 16 U.S. critical infrastructure sectors, which include members of local, state, and federal law enforcement, government agencies, academia, and nonprofit organizations. Given that security requires a cross-functional approach, members also represent all disciplines that have a nexus to security, such as finance, legal, human resources, and more.

All members are vetted by the FBI prior to being accepted, creating a level of trust that is unmatched by any other partnership in the country. **SaviorLabs is a member of the local Boston InfraGard chapter and is affiliated with the Boston FBI Field Office.**

As part of our membership, **we have access to InfraGard's secure web portal** which features a comprehensive suite of threat intelligence information and daily news feeds from the FBI, DHS and other federal, state, and local law enforcement agencies. **Through this, we receive time-sensitive, infrastructure-related security information from government sources such as the FBI and DHS.**

We use this relationship and the information they provide to help protect our clients just like you!

> "Forget the former things; do not dwell on the past. See, I am doing a new thing! Now it springs up; do you not perceive it? I am making a way in the wilderness and streams in the wasteland. Isaiah 43:18-19

You Can Get Hacked Through Wi-Fi?

Connecting your devices to Wi-Fi networks opens a host of potential cybersecurity issues. While this is a risk on any insecure Wi-Fi network, some locations have more vulnerabilities than others.

Hackers leverage poor cyber hygiene and insecure Wi-Fi to exploit vulnerabilities in your computer.

These vulnerabilities could allow an attacker to access credentials for Microsoft Office 365, G Suite, Dropbox, and other cloud apps, or to deliver malware to the device and the cloud. The attacks could potentially give adversaries access to an entire organization, leading to disruption and financial losses.

When you are at a Starbucks, a local restaurant, or anywhere that has Wi-Fi, your computer becomes the front line you need to defend. **If your computer has a weakness, that weakness can and will be exploited.** However, you can take precautionary steps to ensure that your devices and data stay safe while on other networks. Some say that using a VPN can help, but it only solves part of the problem; it keeps your network data private. However, your computer is still connected to the network, and this allows attackers to talk directly to your computer and take advantage of cracks in your security. A crack can be as simple as a program that has not been updated, or an operating system patch that is missing.

The big takeaways are that hackers can use poor cyber hygiene and Wi-Fi to exploit vulnerabilities, compromise your computers, and access your data.

Let us help you protect your company.

We Keep Your
Computers Working
Your Network
SECURE

Contact Us

SaviorLabs, 978-561-6025
info@saviorlabs.com
https://saviorlabs.com

READ THIS NOW

In This Issue

SCAN
ME

SaviorLabs LLC
273 Middleton Road
Boxford, MA 01921

Place
Stamp
Here

To: