SaviorLabs
Managing Technology to Propel Your Growth

Episode #3 - $17
info@saviorlabs.com
978-561-6025

Technology Update

The SaviorLabs technology publication for power users.

Welcome!

by Paul Parisi

You're reading Episode 3 of the SaviorLabs Technology Update Newsletter! In this issue, we cover topics anywhere from whether blue light glasses are just a placebo, to an incredibly insightful book on the way we think, to the what and why of password managers, to a deep dive into what ***"the cloud"*** really is. ***Oh, and some goofy jokes too.***

Please be sure to scan the QR code at the end of the issue (pg. 6) in order to visit the online index of all the references used. **As always, please contact us with any topics you'd like covered, and visit our website to learn more about our mission in depth.** *Thank you for reading, and we hope you enjoy Episode 3!*

Humor

As per usual, we like to start off each episode of our "Technology Update" newsletter with lighthearted jokes to keep things fresh and interesting. In this issue, we decided to change course from our usual brand of jokes, and ***feature technology and IT centric humor instead.***

Without further ado, ***we hope you enjoy the issue!***

- Where's the best place to hide a body? *Page two of Google Search.*
- A password looks at itself in the mirror: "Don't listen to Google. *You are a strong, confident password.*"
- I can't see an end. I have no control and I don't think there's an escape. I don't even have a home anymore. *I think it's time for a new keyboard.*
- How many programmers does it take to change a lightbulb? *None, because it's a hardware problem.*
- We'll we'll we'll... *If it isn't autocorrect.*
- Person 1: "Do you know how to use Outlook?"
- Person 2: "As a matter of fact, *I Excel at it."*
- Person 1: "Was that a Microsoft Office pun?"
- Person 2: *"Word."*
- Question: "What is the biggest lie in the entire universe?"
- Answer: "*I have read and agree to the Terms & Conditions."*
- Did you hear about the monkeys who shared an Amazon account? *They were Prime mates*
- Have you heard of that new band, "1023 Megabytes"? They're pretty good, *but they haven't gotten a gig just yet.*
- I just got fired from my job at the keyboard factory. *They told me I wasn't putting in enough shifts.*
- I was showing my kids an old rotary phone when my nine-year-old asked, "How did you text on it?" My fifteen-year-old roared with laughter, until a thought occurred to her: "*Wait, where did you store your contacts?"*
- I've given up social media for the New Year and am trying to make friends outside Facebook while applying the same principles. Every day, I walk down the street and tell passersby what I've eaten, how I feel, what I did the night before, and what I will do tomorrow. Then I give them pictures of my family, my dog, and me gardening. I also listen to their conversations and tell them I love them. *And it works. I already have three people following me- two police officers and a psychiatrist*.

And finally, a few hilarious words of wisdom: *"Whoever said that the definition of insanity is doing the same thing over and over again and expecting different results,* ***has obviously never had to reboot a computer."***

Did you know?

White-faced capuchin monkeys greet each other by sticking their fingers up each others' noses. Proving wrong the old adage that you can pick your friends and you can pick your nose, but ***you can't pick your friend's nose.***

Do Blue Light Glasses Work?

by James Meher

Burning, itchy, watery, or dry eyes are common side effects if you spend vast amounts of time looking at a screen. Better categorized as ***DES, Digital Eye Strain has become increasingly prominent in our digital age.*** With Americans consuming screens for an average of 7 hours a day, **the problem of DES requires a solution.**

Invented back in the 1960's, **blue light glasses were designed with a special coating on the lens to reflect blue light rays, keeping your eyes safe from any strain.** The product didn't become vastly popular until the early 2000's with the adoption of computers, not only in more businesses, but also in homes. With the increase in usage came the uptick in DES. **Blue light glasses were then marketed to be the saving grace for anyone needing to use computers for long periods of time.**

The explosion in sales and instant adoption of this product was perceived as a cure. However, the drop in DES symptoms for blue light glasses users didn't happen. **Official studies into blue light glasses' effectiveness have now been conducted, leading to the conclusion that they are yet another in a long line of placebo remedies.**

So, while wearing blue light glasses won't hurt you, *they certainly won't help with any DES symptoms.*

Instead, ***you should consider using a technique referred to as the 20-20-20 rule.*** This refers to *20 minutes of screen time*, then *staring for 20 seconds at an object 20 or so feet from where you are, allowing your eyes to refocus and prevent straining.*

What's A Password Manager?

by Paul Parisi

A password manager is a software application that securely stores and manages all of your passwords for online accounts. **Instead of trying to remember each password or using the same password for multiple accounts** (which is a security risk, *see last month's newsletter*), ***a password manager generates and saves unique, strong passwords for each account.*** Your password manager is accessed by a master password that only you know. For example, my master password might look something like this:

`XHDk39WJg$Yg!wQ$h@8w7$4%`

Yes, I know it's hideous and incomprehensible, but *you don't want a password that's easy to guess.* This password is 24 characters, includes upper and lowercase letters, numbers, and several different special characters. *(12 characters is our recommended minimum.)*

Here are some examples of how long it would take to manually crack a password. (*This assumes an attacker can make 1 billion attempts per second,* and most attacks will get the password halfway through (on average), *so cut those times in half.*)

8 characters would take **63 days** for *letters a-z, all lowercase.*

10 characters would take **44 years** for *letters a-z, all lowercase.*

8 characters would take **2.17 years** for *letters a-z (uppercase and lowercase), numerals, and special characters.*

If, like me, you use *24 characters* with *letters a-z (uppercase and lowercase) and numerals and special characters,* it would take ***3.51 x 10^27 years*** **(3,510,000,000,000,000,000,000,000 years,** *which is three quintillion, five hundred and ten quadrillion years).*

This is one of the main reasons why it is easier for a hacker to trick someone into giving away their password rather than trying to hack it themselves.

Once they get the password, they can try that same password on multiple logins. Protecting your passwords is one of the best ways you can protect what they allow access to. *(See our previous article on password security.)*

When you need to log in to an account, the password manager fills in the correct login information automatically. Some password managers also offer additional features such as password strength analysis and alerts for compromised passwords. ***Overall, a password manager can help you create and manage strong and unique passwords, improve online security, and save time.***

You might be asking: *"How do I remember such a complicated master password?"* **It's actually pretty simple. Firstly, create a file on your computer with an innocuous name.** For example: **measurements.txt**, something that would not catch someone's eye. **Then store your master password in the new file, for example:**

`XHDk39WJg$Yg!wQ$h@8w7$4%Beep`

The secret trick is to add/remove a word *(or something else like a number, special character, etc.)* **to/from the end of the password that you've just stored.** **(***Using the example, you would simply have to remember to remove the word Beep when using the password.)*

I would recommend using something less obvious, maybe something like: `xtk*`. **This is how you hide in plain sight.** (Alternatively, you could take a few characters away from the original password, *but you would have to remember what you removed when using it*.)

However, it's important to remember that naïve use of your password manager can be just as bad or risky as not having one at all. *Here are some examples of common mistakes:*

1. Weak Master Password – If you use a weak or easily guessable master password to protect your password manager, then all of your other passwords could be at risk. Hackers can use various techniques to crack weak passwords, and **once they have your master password, they can potentially access all of your other passwords.** *(We covered how to fix this earlier, and in last month's issue.)*

2. Breach of Password Manager – If the password manager company experiences a security breach or hack, then all of the passwords stored in the password manager could be compromised. Even if the passwords are encrypted, if the encryption key is stolen, *then the passwords could be decrypted and used by hackers.* *A real example of this happening is with LastPass, so I highly recommend you stop using LastPass as soon as possible.*

3. Single Point of Failure – A password manager is a single point of failure for all of your passwords. If the password manager fails or malfunctions, then you could potentially lose access to all your passwords at once. ***This is exactly what backups are for.*** *I recommend saving/exporting all of your passwords to a thumb drive you keep at home. (I put my password backups on a VeraCrypt volume.)*

4. Dependency on Technology – If you rely solely on a password manager to manage your passwords, then you may not be able to remember any of your passwords if you do not have access to the password manager. This could become a problem if you are traveling, have lost your device, or if the password manager is down. **One solution to this is to store an encrypted export of the passwords in a secure location like the cloud.** *(We'll be covering what the cloud really is in a future article.)*

In summary: ***use a strong and unique master password, choose a reputable password manager with good security practices, and regularly update your passwords.*** Again, *I recommend keeping a backup of your passwords in a secure location in case you lose access to your password manager, or your password manager is breached for whatever reason.*

Password managers aren't just for individuals, *they work in business environments as well.* There are additional advantages when your staff uses a corporate password manager.

1. Centralized Management – A company-wide password manager can allow for centralized management of user accounts and passwords, making it easier to monitor and control access to sensitive information. ***You can also keep track of who has accessed each password.*** *For example, if "Barney" has just left the company, you can get a report of all the passwords that he had access to and then change just those.*

2. Security – Using a company-wide password manager can improve overall security by allowing for the use of strong, unique passwords across all systems and applications. ***This can help reduce the risk of data breaches and cyber-attacks.***

3. Time Saving – Using a password manager can save time and increase productivity by eliminating the need for employees to remember multiple passwords and constantly reset them. *Additionally,* ***you can share passwords without sending them via email or other means,*** *which also helps avoid security risk.*

4. Compliance – A company-wide password manager can help ensure compliance with security and regulatory requirements, by enforcing password complexity and regular password changes

While using a password manager can boost efficiency and help make your devices more secure, *it's also important to exercise extra caution when it comes to password security.*

Please be sure to read our previous article on password security, and if you have any further questions or concerns on this subject, ***we would be happy to talk with you.***

Are You Afraid of the Cloud?

by Paul Parisi

Depending on who you ask, you get different answers to what "the cloud" is exactly. **That is because the cloud is many things, and, depending how you use it or who supplies your "cloud," you could do well or do very badly.** *But what exactly is "the cloud"?* ***The cloud is basically all the servers and systems we used to have in a closet or server room, all kept somewhere in a giant computer farm/warehouse and managed by someone else. You never have to replace your server hardware again.*** *Many people worry about the security of the cloud; that once they put something in "the cloud," anyone can easily get it.* That is theoretically true, sort of, but should be discussed a bit more.

First, using your own computers and file servers *(i.e., computers physically located at your business and accessible to employees over a network)* implies that they are more secure than the cloud. **This is usually not the case.** As a professional IT consultant, I must tell you that many IT people may not really know what they are doing when it comes to security. They say they do, but don't let them fool you. **Most of the breaches that happen are because a person made a mistake and did not do basic things like update a system/application or even close a door. *So, if you are certain that your systems are as secure as they need to be, then you are safe. But I would go as far as saying that 90% of most IT systems are not secure.***

This is where the cloud comes in. For example, Microsoft has designed Office 365, which runs in the cloud, to be secure. *In fact, it has been intentionally set up to not be accessible to their administrators.* They have built big server farms, and, when you subscribe, your company gets a "tenant" on one of their server clusters. *(A tenant is difficult to briefly define, but is essentially a representation of your organization, or a partition of Microsoft's system.)* **These servers are designed to run and be fault-tolerant using shared storage that is distributed across Microsoft data centers. *Backups are happening all the time in the background.* Policies are in place to keep deleted items and only purge them after a certain amount of time has passed. If a user deletes a big folder or malware** starts accessing lots of files, you get an alert so you can stop it and roll back.

So, what is to prevent a Microsoft engineer from simply logging in as you, you might ask. **Well, they can't! *It's not designed that way, so much so that, when you call Microsoft technical support, a Microsoft engineer can only view your screen and tell you how to fix it.* You have to do the work, so they never have access to your data or your tenant.**

But what about in the data center? **If you are really paranoid here, what is stopping a rogue engineer from *going to your tenant's server, removing a hard disk, taking it home, connecting it to their computer and reading your data?***

Well, first, the data on the disk is encrypted with Bitlocker encryption, so the game is pretty much over at this point. But let's say they can get past Bitlocker. They open the disk and they see your files, *right?* **Wrong! *In Office 365, files are stored as "shards," much like shards of glass. And the Office 365 tenant system is the only thing that knows how to put the shards back together in the right order to reconstruct your files***. (Continued on pg. 5)

("Are You Afraid of the Cloud?"- Continued from pg. 4)

But it goes further! **Each shard is encrypted with a private key specific to that file and that shard.** ***The "Rosetta stone" for how to put these back together is stored in your tenant and each file and each version of a file has a different Rosetta stone and different key.*** *(This is starting to get a bit complicated!)*

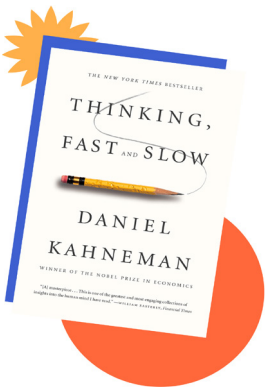
(Please scan the QR code to read the rest of the article.)

Featured Book of the Month

by Paul Parisi

This month, I wanted to delve into *Thinking, Fast and Slow*, a bestselling book written by psychologist and Nobel laureate, Daniel Kahneman. **It's an incredibly thoughtful and insightful book that explores why we think the way we think, and more importantly, the mysterious dichotomy of human cognition.** Although admittedly a bit of a dense read, I find it well worth the time of anyone interested in how and why the human mind gets from point A to point B.

It has many gems of wisdom throughout and breaks down the differences of thinking in a helpful way. There are two main ways of thinking: ***"System 1"***, which is fast, instinctive and emotional (*fast*); and ***"System 2"***, which is slower, more deliberative, and more logical (*slow*).



"System 1" is the automatic part of the brain, which is responisble for quick reactions. It operates automaticaly and instinctively with little to no conscious effort. *"System 2"*, on the flip side, *is the slow, analytical part of the brain, which is responsible for complex problem-solving, logic, and critical thinking*. It uses both conscious effort and mental energy.

Kahneman argues that people often rely too much on "System 1", which leads to to cognitive biases, errors in judgment, and poor decision-making. ***However, these biases can be overcome by learning to recognize when "System 1" is in control and making a conscious effort to engage "System 2" instead.***

The book is divided into five parts:

Two Systems: *An introduction to the dual-process theory and the differences between "System 1" and "System 2" thinking.*

Heuristics and Biases: *An exploration of cognitive biases and shortcuts that arise from over-reliance on "System 1" thinking, such as anchoring, availability, and representativeness heuristics.*

Overconfidence: *A discussion of how overconfidence can lead to poor decision-making and the planning fallacy, which causes people to underestimate the time and resources needed for a task.*

Choices: *An examination of decision-making, including prospect theory (an alternative to classical utility theory), loss aversion, and the endowment effect.*

Two Selves: *An exploration of the experiencing self and the remembering self, which highlights the discrepancies between how people experience events and how they remember them.*

This book was both insightful, and genuinely helpful in learning to recognize what triggered my *Systems 1 and 2*. *I find that Kahneman offered both excellent advice, and comprehensive understanding of the human psyche.* *I highly recommend you pick up a copy for yourself!* We've linked a copy below to make it easier. *You should take a look.*

https://a.co/d/bOTSkev

> "For my thoughts are not your thoughts, neither are my ways, declares the Lord. For as the heavens are higher than the earth, so are my ways higher than your ways and my thoughts than your thoughts."
>
> – Isaiah 55:8-9

Contact Us

SaviorLabs, 978-561-6025

info@saviorlabs.com

https://saviorlabs.com

READ THIS NOW

In This Issue

We Keep Your Computers Working
Your Network SECURE

SCAN ME

SaviorLabs LLC
273 Middleton Road
Boxford, MA 01921

Place Stamp Here

To: