SaviorLabs
Managing Technology to Propel Your Growth

Episode #5 - $17.50
info@saviorlabs.com
978-561-6025

Technology Update

The SaviorLabs technology publication for power users.

Welcome!

by Paul Parisi

Welcome to Episode 5 of the SaviorLabs Technology Update Newsletter! Thank you to everyone who have given us such great feedback. Over the coming issues, we will be addressing all of the topics you have brought up. ***Keep the suggestions coming, and let us know what you think!***

As always - ***thanks for reading, and we hope you enjoy this issue!***

Humor

As per usual, we're starting this month's issue off with some ridiculously funny jokes. However, this month, we decided to go with some slightly longer ones. But don't let that deter you- ***we promise you won't be bored!***

1. Sherlock Holmes and Dr. Watson were going camping. They pitched their tent under the stars and went to sleep. Some time in the middle of the night, Holmes woke Watson up and said, "Watson, look up at the sky, and tell me what you see."

Watson replied, "I see millions and millions of stars."

Holmes asked, "And what do you deduce from that?"

Watson replied, "Well, if there are millions of stars, and if even a few of those have planets, it's quite likely there are some planets like Earth out there. And if there are a few planets like Earth out there, there might also be life."

Holmes said, ***"Watson, you idiot, it means that somebody stole our tent."***

2. A cruise ship passes by a remote island, and all the passengers see a bearded man running around and waving his arms wildly.

"Captain," one passenger asks, "who is that man over there?"

"I have no idea," the captain says, ***"but he goes nuts every year when we pass him."***

3. "If there are any idiots in the room, will they please stand up?" said the sarcastic teacher.

After a long silence, one freshman rose to his feet.

"Now then mister, why do you consider yourself an idiot?" inquired the teacher with a sneer.

"Well, actually I don't," said the student, ***"but I hate to see you standing up there all by yourself."***

4. A fellow was walking along a country road when he came upon a farmer working in his field. The man called out to the farmer, "how long will it take me to get to the next town?"

The farmer didn't answer. The guy waited a bit and then started walking again. After the man had gone about a hundred yards, the farmer yelled out, "about 20 minutes!"

"Thank you. But why didn't you tell me that when I asked you?"

"Didn't know how fast you could walk".

5. A tough old cowboy from Texas counseled his granddaughter that if she wanted to live a long life, the secret was to sprinkle a pinch of gun powder on her oatmeal every morning.

The granddaughter did this religiously until the age of 103, when she died.

She left behind 14 children, 30 grandchildren, 45 great-grandchildren, 25 great-great-grandchildren, ***and a 40-foot hole where the crematorium used to be.***

And one last shorter one, because we just couldn't help ourselves:

6. Two men walk into a bar. One says, "I'll have some H2O."

The other says, "I'll have some H2O, too."

The second man died.

Did you know?

Giraffes hum to each other at night to make sure their herd stays together. ***How sweet!*** Although, when I try to do the same, ***I get a pillow thrown at my head.***

Did You Know These Objects Can Steal Your Identity?

You wouldn't think a child's toy could lead to a breach of your personal data. But this happens all the time.

What about your trash can sitting outside? You wouldn't normally think of it as a treasure trove for an identity thief, *would you?*

Surprisingly, many inconspicuous everyday objects can actually lead to identity theft.

Old Smart Phones

A cybercriminal could easily strike data theft gold by finding your old smartphone. **Make sure that you properly clean any old phones by erasing all your data before disposing of them.**

Wireless Printers

Protect your wireless printers by ensuring you keep their firmware updated. You should also keep it turned off whenever you aren't using it.

USB Sticks

You should never plug a USB device of unknown origin into your computer. This is an old trick in the hacker's book. **They can plant malware on these sticks and then leave them around as bait for an unsuspecting user.**

Old Hard Drives

When you are disposing of an old computer or old removable drive, make sure it's wiped clean first. Simply deleting your files isn't enough.

It's best to get help from an IT professional to properly erase your computer drive. This will make it safe for disposal, donation, or reuse.

Trash Can

Identity theft criminals aren't only online. They can also be trolling the neighborhood on trash day. **Be careful what you throw out in your trash.**

Children's IoT Devices

You should be wary of any new internet-connected kids' devices you bring into your home. **Install all firmware updates and do your homework first.**

ATMs

Bad actors can plant hidden devices on ATMs or card readers to steal your card information during transactions. This tactic is called skimming. **Try using cardless ATM transactions, and make sure to double check your bank statements frequently for any suspicious activity.**

Keeping all these things in mind*, make sure to do your research, use extra caution, and stay safe!*

Why Every Company Is a Technology Company

Whether you sell shoes or run an accounting firm, *you need some type of technology to operate.*

Today's companies aren't just in the business of selling their own goods and services anymore.

Here are 8 reasons why you should start prioritizing your company's technology.

1. Your technology is a critical part of your business.

2. Your customers expect/deserve an excellent digital experience.

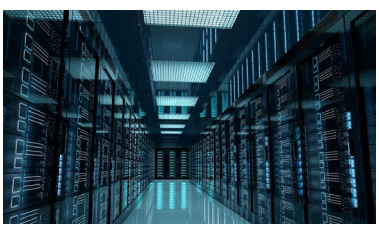
3. Your employees need devices in order to drive their productivity.

4. Companies rely on AI & automation to stay competitive.

5. Information is being generated at a rapid pace. Technology helps keep you ahead of the game.

6. Technology expertise is needed as your vendors/suppliers leave legacy systems behind.

7. Company growth is tied to tech innovation and needs cutting-edge tools to propel your business forward.



What Is App Fatigue & Why Is It a Security Issue?

The number of apps and web tools that employees use on a regular basis continues to increase. *Most departments have about 40-60 different digital tools that they use.* **71% of employees feel they use so many apps that it makes work more complex.**

Many of the apps that we use every day have various alerts. We get a "ping" when someone mentions our name on a Teams channel. We get a notification popup that an update is available. We get an alert of errors or security issues.

This can end up being distracting, overwhelming, and exhausting.

App fatigue is a very real thing and it's becoming a cybersecurity problem. *The more people get overwhelmed by notifications, the more likely they are to ignore them.*

Just think about the various digital alerts that you get. They come in:

- *Software apps on your computer*
- *Web-based SaaS tools*
- *Websites where you've allowed alerts*
- *Mobile apps and tools*
- *Email banners*
- *Text messages*
- *Team communication tools*

Some employees are getting the same notification on two different devices. *This just adds to the problem.*

Besides just alert bombardment, every time the boss introduces a new app, *that means a new password.* **This leads to many issues that impact productivity and cybersecurity.**

Employees are already juggling about (an estimated) 191 passwords.

They use at least 154 of them sometime during the month. *That means that this overwhelming number becomes even more so with each new application installation.*

How Does App Fatigue Put Companies at Risk?

Employees Begin Ignoring Updates

When digital alerts interrupt your work, you can feel like you're always behind.

This leads to ignoring small tasks seen as not time-sensitive. Simple tasks like clicking to install an app update get put on the shelf for later.

When employees are overwhelmed with too many app alerts, they tend to ignore them.

When updates come up, they may quickly click them away. *They feel they can't spare the time right now and aren't sure how long it will take.*

However, ignoring app updates on a device is dangerous.

Many of those updates include important security patches for found vulnerabilities.

When they're not installed, the device and its network are at a higher risk. *It becomes easier to suffer a successful cyberattack.*

Employees Reuse Passwords (That Are Often Weak)

Another security casualty of app fatigue is password security.

The more SaaS accounts someone must create, the more likely they are to reuse passwords. **It's estimated that passwords are typically reused 64% of the time.**

Credential breach is a key driver of cloud data breaches. *Hackers can easily crack weak passwords.* ***The same password used several times leaves many accounts at risk.*** (See our previous newsletters for more on password security.)

Employees May Turn Off Alerts

Some alerts are okay to turn off. For example, *do you really need to know every time someone responds to a group thread?*

However, turning off important security alerts is not good. It could mean the difference between a security breach and a close call.

There comes a breaking point when one more push notification can push someone over the edge.

So What's the Answer to App Fatigue?

It's not realistic to just go backward in time before all these apps were around.

Most of your applications and tools are in use for a reason, *so simply getting rid of them all is not the solution.*

(Continued on pg. 4)

Insider Threats Are Getting More Dangerous! Here's How to Stop Them

One of the most difficult types of attacks to detect are those performed by insiders.

An *"insider"* would be anyone that has legitimate access to your company network and data via a login or authorized connection.

Because insiders have authorized system access, they can bypass certain security defenses, including those designed to keep intruders out.

Since a logged-in user isn't seen as an intruder, those security protections aren't triggered.

A recent report by Ponemon Institute found that over the last two years:

• *Insider attacks have increased by 44%*

• *The average cost of addressing insider threats has risen by 34%*

4 Types of Insider Threats

1. **A malicious/disgruntled employee**
2. **A careless/negligent employee**
3. **A third party with access to your systems**
4. **A hacker that compromises a password**

Ways to Mitigate Insider Threats

Thorough Background Checks

When hiring new employees make sure you do a thorough background check.

Malicious insiders will typically have red flags in their work history.

You want to do the same with any vendors or contractors that will have access to your systems.

Endpoint Device Solutions

Mobile devices now make up about 60% of the endpoints in a company. But many businesses aren't using a solution to manage device access to resources.

Put an endpoint management solution in place to monitor device access. *You can also use this to safelist devices and block unauthorized devices by default.*

Multi-factor Authentication & Password Security

One of the best ways to fight credential theft is through multifactor authentication.

Hackers have a hard time getting past the 2nd factor.

They rarely have access to a person's mobile device or FIDO (Fast IDentity Online) security key.

Employee Data Security Training

Training can help you mitigate the risk of a breach through carelessness.

Train employees on proper data handling and security policies governing sensitive information.

Network Monitoring

Use AI-enabled threat monitoring.

This allows you to detect strange behaviors as soon as they happen.

For example, *someone downloading a large number of files, or someone logging in from outside the country.*

("What Is App Fatigue"- Continued from pg. 3)

But you can put a strategy in place that puts people in charge of their tech, *and not the other way around*.

Here are some ways how:

1. **Streamline your business applications.**
2. **Have your IT team properly set up notifications.**
3. **Automate application updates.**
4. **Open a two-way communication system about alerts.**

We Love Referrals!

Please don't hesitate to mention us to your fellow business owners!

When your friends end up becoming a client, **we'll give you a $200 Amazon Gift card.**

If you end up referring us, *just let us know and we'll take care of the rest!*

You Should Think About Switching to Virtual Meetings In Microsoft Teams

In today's fast-paced world, the need for efficient and effective communication has never been more critical.

With the rise of remote work and the increasing reliance on technology, virtual appointments have become an essential tool for businesses and organizations worldwide.

Microsoft Teams,* a powerful collaboration platform, *has emerged as a game-changer in this arena, offering seamless virtual appointments that redefine the way we connect, collaborate, and communicate.

The Rise of Virtual Appointments

The global pandemic has accelerated the adoption of remote work, *with businesses and organizations scrambling to find ways to maintain productivity and communication while keeping their employees safe.*

Virtual appointments have become the go-to solution, **allowing teams to connect and collaborate without the need for physical presence.**

Microsoft Teams, a platform designed to facilitate teamwork and communication, *has risen to the challenge, offering a comprehensive suite of tools that make virtual appointments a breeze.*

From video conferencing to file sharing, *Microsoft Teams has everything you need to conduct successful virtual appointments, all in one place.*

> "The Rock, his work is perfect, for all his ways are justice. A God of faithfulness and without iniquity, just and upright is he."
>
> —Deuteronomy 32:4

The Benefits of Virtual Appointments in Microsoft Teams

1. Enhanced Collaboration

Microsoft Teams allows users to collaborate in real-time, making it easier than ever to work together on projects, share ideas, and make decisions.

With features like screen sharing, whiteboarding, and file sharing, **virtual appointments in Microsoft Teams enable teams to work together seamlessly, no matter where they are located.**

2. Increased Flexibility

Virtual appointments in Microsoft Teams offer unparalleled flexibility, allowing team members to join meetings from any device, anywhere. **This means that employees can participate in important discussions and decision-making processes even if they're on the go or working from home.**

3. Cost Savings

By eliminating the need for physical meeting spaces and reducing travel expenses, virtual appointments in Microsoft Teams can result in significant cost savings for businesses and organizations.

Additionally, the platform's robust features and integrations eliminate the need for multiple software subscriptions. (Our personal favorite bonus.)

4. Improved Communication

Microsoft Teams' virtual appointments facilitate clear and effective communication, thanks to high-quality video and audio capabilities. The platform also offers features like live captions and translations, **ensuring that language barriers and accessibility issues are no longer a hindrance to effective communication.**

5. Enhanced Security

Microsoft Teams is built on the secure and reliable Microsoft 365 platform, ensuring that your virtual appointments are protected by enterprise-grade security measures. **This means that you can conduct your meetings with confidence, knowing that your data and conversations are safe.**

Microsoft Teams is an all-around incredible tool! We at SaviorLabs use Microsoft Teams, have implemented it in many of our clients' businesses, and *we highly recommend it to you.* **Contact us if you're interested in learning more.**

Contact Us

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

READ THIS

In This Issue

SCAN ME

SaviorLabs LLC
273 Middleton Road
Boxford, MA 01921

Place Stamp Here

To:

We Keep Your Computers Working Your Network SECURE