SaviorLabs
Managing Technology to Propel Your Growth

Episode #4 - $17.50
info@saviorlabs.com
978-561-6025

Technology Update

The SaviorLabs technology publication for power users.

Welcome!

by Paul Parisi

You're reading Episode 4 of the SaviorLabs Technology Update Newsletter! There is a rumor going around the office that we may have been nominated for a Pulitzer prize- ***we'll keep you updated.***

In this issue, we have an introduction to the concept of risk as well as some other interesting topics to change everything you have ever thought you knew about anything. ***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 us.

Thank you for reading, and we hope you enjoy Episode 4!

Quotes

We are switching things up a bit this month from ***"Humor"*** to ***"Quotes"***. Here are some of our favourite quotes about computer technology:

- "The computer was born to solve problems that did not exist before." - *Bill Gates*
- "The best way to predict the future is to invent it." - *Alan Kay*
- "Computers are useless. They can only give you answers." - *Pablo Picasso*
- "The computer is a bicycle for the mind." - *Steve Jobs*
- "The digital revolution is far more significant than the invention of writing or even of printing." - *Douglas Engelbart*
- "Technology is just a tool. In terms of getting the kids working together and motivating them, the teacher is the most important." - *Bill Gates*
- "I think it's fair to say that personal computers have become the most empowering tool we've ever created. They're tools of communication, they're tools of creativity, and they can be shaped by their user." - *Bill Gates*
- "The human spirit must prevail over technology." - *Albert Einstein*
- "The great myth of our times is that technology is communication." - *Libby Larsen*
- "The Internet is becoming the town square for the global village of tomorrow." - *Bill Gates*

Humor

And, because we couldn't help ourselves:

A priest, a doctor, and an IT person were waiting one morning for a particularly slow group of golfers. The engineer fumed, "What's with those guys? We must have been waiting for fifteen minutes!" The doctor chimed in, "I don't know, but I've never seen such inept golf!"

The priest said, "Here comes the greens keeper. Let's have a word with him." He said, "Hello George, what's wrong with that group ahead of us? They're rather slow, aren't they?"

The greens keeper replied, "Oh, yes. That's a group of blind firemen. They lost their sight saving our clubhouse from a fire last year, so we always let them play for free anytime."

The group fell silent for a moment. The priest said, "That's so sad. I think I will say a special prayer for them tonight." The doctor said, "Good idea. I'm going to contact my ophthalmologist colleague and see if there's anything he can do for them." The IT person said, "Why can't they play at night?"

And one more:

There are 10 types of people in the world... those who understand binary, and those that don't!

Did you know?

Despite being commonly known as cute and fluffy, some wild and domesticated rabbits have been observed engaging in cannibalistic eating habits. I guess you could say that when they get hangry, ***it gets a little... hairy.***

Managing Risk Isn't Just A Job – It's YOUR Job.

by Paul Parisi

If you run a business, you have one major thing to think about – *your business!* That's it. *What exactly is "your business"? It's the machine you run to make money. That's it.* **It is your responsibility to make sure that the machine runs as efficiently as possible.** The minute you take your eye off that ball is the moment you move from a business to a hobby.

One of the most important things in business comes down to managing risk. *Some very important questions to ask yourself are what would happen if:*

- *You can't find new customers.*
- *You can't get your customer what they want or what they need when they need it.*
- *You don't have employees that actually want to work.*
- *There is no power at your office.*

As a technology company, people often ask us what we do. The short answer is: **we manage technology risk for our clients.** Some of our clients have very little risk, some have more. You need to have a technology provider that "gets this one thing". You can have all the shiny new toys, *but if your roof leaks, those toys just don't matter.*

Let's use a couple of analogies:

- You own a home with air conditioning. If your air conditioner stops working during summer, you'll be warmer than is comfortable until you fix it. *Low risk.*
- You own a home with heat and live in a cold climate. If your heating system breaks in the dead of winter, *that's a much bigger risk. How will you stay warm?*

Everyone has risks and manages those risks every day. **Your business has risks, and you manage them every day.** *I will bet you manage the risks that squeak the loudest:* the roof is leaking; you can't find employees; you have employees - but they don't come to work; your costs are going up; the coffee machine isn't working; your client data isn't protected; etc.

Only you can determine the level of risk you are taking and, once a risk has been identified, what you may want/need to do about it.

We recommend that each and every business do regular risk audits. These audits need to happen in several areas:

1. **Business –** What do you actually do to make money? Is this on the mark or off the mark?
2. **Employees –** Do you have the right people in the right seats?
3. **Resources –** Do you have the right resources for solving the right problems?

How do we manage these risks? Remember, none of these risks may apply to you, but more than likely, some of them do.

1. **Insurance –** Does your insurance protect what it should be protecting, ie. do you have the right coverages? *Insurance is all about managing the risks you don't want to manage.*
2. **Legal –** Are your agreements up to date? Are you covering yourself with the right contract language? *Legal is all about protecting you from known risks.*
3. **Financial –** Are you actually making what you think you are making? Do you have any leakage? *Financial is making sure that the risks you are taking create a net positive.*
4. **Technology –** Does technology keep my stuff safe and my staff more effective? Does it not leave me open to needing everything else on this list? *Technology is making sure what happens in your company stays in your company.*

These are some important things to think about carefully.

Over the next few episodes, we will begin to dig more into business risks and how to get a handle on them and *manage them in the future.*

8 Ways to Secure Your Wireless Printer

Many people worry about someone hacking their computer. *But they're not really thinking about their wireless printer getting breached.* It's a tool that most individuals use sporadically. For example, when you want to print out tax forms or mailing labels. *Who would expect their printer to get hacked?*

Printers tend to be out of sight, out of mind. *That is until you need to print something and run out of ink.* **Well, they're not out of the mind of hackers. In fact, unsecured printers are a classic way for criminals to gain access to a home network.**

Here are 8 ways to prevent that from happening:

1. **Change the default login credentials.**
2. **Keep your printer firmware updated.**
3. **Use a network firewall.**
4. **Put your printer on a guest network.**
5. **Disable any unused ports/services.**
6. **Unplug it when it's not in use.**

7. **Teach your family cybersecurity best practices.**
8. **Don't use Wi-Fi, use a cable.**

Is It Time to Ditch Passwords for More Secure Passkeys?

I know we have covered passwords quite a bit lately but there are some recents changes afoot. **Passwords are the most used method of authentication, but they are also one of the weakest.** *Passwords are often easy to guess or steal.* Also, many people use the same password across several accounts. *This makes them vulnerable to cyber-attacks.* (We've discussed the cons of this in previous newsletters.)

The sheer volume of passwords that people need to remember is large. ***This leads to habits that make it easier for criminals to breach passwords.*** *Such as creating weak passwords and storing passwords in a non-secure way.*

61% of all data breaches involve stolen or hacked login credentials.

In recent years a better solution has emerged – ***passkeys.*** Passkeys are more secure than passwords. They also provide a more convenient way of logging into your accounts.

Passkeys work by generating a unique code for each login attempt. This code is then validated by the server. This code is created using a combination of information about the user and the device they are using to log in.

You can think of passkeys as a digital credential. A passkey allows someone to authenticate in a web service or a cloud-based account. *There is no need to enter a username and password.*

This authentication technology leverages Web Authentication (WebAuthn).

This is a core component of FIDO2, an authentication protocol. *Instead of using a unique password, it uses public-key cryptography for user verification.*

The user's device stores the authentication key. This can be a computer, mobile device, or security key device. *It is then used by sites that have passkeys enabled to log the user in.*

Advantages of Using Passkeys Instead of Passwords

More Secure

One advantage of passkeys is that they are more secure than passwords. Passkeys are more difficult to hack. This is true especially if the key generates from a combination of biometric and device data.

Biometric data can include things like facial recognition or fingerprint scans. Device information can include things like the device's MAC address or location.

This makes it much harder for hackers to gain access to your accounts.

More Convenient

Another advantage of passkeys over passwords is that they are more convenient. **With password authentication, users often must remember many complex passwords.** This can be difficult and time-consuming.

Forgetting passwords is common and doing a reset can slow an employee down. Each time a person has to reset their password, it takes an average of three minutes and 46 seconds.

Passkeys erase this problem by providing a single code. You can use that same code across all your accounts. *This makes it much easier to log in to your accounts.*

It also reduces the likelihood of forgetting or misplacing your password.

Phishing-Resistant

Credential phishing scams are prevalent. Scammers send emails that tell a user something is wrong with their account.

They click on a link that takes them to a disguised login page created to steal their username and password.

When a user is authenticating with a passkey instead, this won't work on them. *Even if a hacker had a user's password, it wouldn't matter. They would need the device passkey authentication to breach the account.*

To sum up, there are many benefits to using passkeys rather than passwords.

However, if you insist on continuing to use a password, **make sure to take a look at our previous newsletters that discuss password security and best practices when using a password.** *Better to use a less efficient precaution than no precaution at all!*

How To Create Insightful Dashboards in Microsoft Power BI

Data visualization is a powerful tool for communicating complex data.

But it is not enough to simply create a graph or chart and call it a day. To truly make use of information, it is important to create insightful reports.

Creating holistic and insightful reports requires the use of several data points. **One tool that enables this is Microsoft Power BI.**

What Is Microsoft Power BI?

Microsoft Power BI is a business intelligence tool. It allows you to connect many data sources to one dashboard. *Using Power BI, you can easily model and visualize data holistically.*

Tips for Designing Great Data Visualization Reports

Consider Your Audience

You should design reporting dashboards with the end user in mind. CEOs and CFOs are interested in different aspects of the business, so make the information interesting to them.

- *What is it that this audience wants to see?*
- *Are they looking for bottom-line sales numbers?*
- *Or do they want to cover insights that can help target productivity gaps?*

Don't Overcomplicate Things

Many times, less is more. *If you find that your dashboard looks crowded, you may be adding too many reports.*

The more you add, the more difficult it is to read the takeaways from the data.

Try Out Different Chart Types

Experiment with presenting your data in different ways.

Flip between bar, pie, and other types of charts to find the one that tells the story the best.

Just don't go overboard. Keep it simple but interesting.

(Continued on pg. 5)

What is Your Company's Attitude Toward Technology?

Place an "X" of where you are today.

Place a "Y" where you would like to be.

(Power BI - Continued from pg. 4)

Get to Know Power Query

Power Query is a data preparation engine.

Take time to learn how to leverage this tool for help with:

- *Connecting a wide range of data sources to the dashboard*
- *Previewing data queries*
- *Building intuitive queries over many data sources*
- *Defining data size, variety, and velocity*

Build Maps with Hints to Bing

Bing and Power BI integrate, allowing you to leverage default map coordinates. Use best practices to utilize the mapping power of Bing to improve your geo-coding.

Tell People What They Are Looking At

A typical comment heard often when presenting executives with a new report is, *"What am I looking at?"* **Tell your audience what the data means by using features like tooltips and text boxes to add context.**

Use Emphasis Tricks

People usually read left to right and from top to bottom. So put your most important chart at the top, left corner. *Follow with the next most important reports.*

Contact Us

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

"Where there is no guidance, a people falls, but in an abundance of counselors there is safety."

- Proverbs 11:14

6 Immediate Steps You Should Take When Your Netflix Account Is Hacked

Netflix is one of the most popular streaming services. It has become an essential part of many people's daily entertainment routines. *Unfortunately, like any online service, Netflix accounts can be vulnerable to hacking.*

Hackers take advantage of "phishing overload." **Once they breach your account, they're usually quiet for a bit, hoping you'll mistake the Netflix suspicious login warning for a fake.**

Here are some things to do right away if you fear your account is hacked:

1. **Go to the Netflix site & try to log in.**
2. **If you can log in, change your password immediately.**
3. **If you can log in, remove any strange payment methods**
4. **Contact Netflix support and let them know that you think you've been compromised. (Don't skip this step!)**
5. **Watch your bank statements.**
6. **Change the password for other accounts that used the same one as your Netflix account.**

We Love Referrals!

The greatest gift anyone can give us is a referral. **When your friends end up becoming a client, *we'll gift you a $200 Amazon Gift card.*** Let us know and we will take it from there.

NOW HEAR THIS

In This Issue

SCAN ME

SaviorLabs LLC
273 Middleton Road
Boxford, MA 01921

Place Stamp Here

To: