SaviorLabs™
Managing Technology to Propel Your Growth

Episode #6 - $17.50
info@saviorlabs.com
978-561-6025

Technology Update

The SaviorLabs technology publication for power users.

Welcome!

by Paul Parisi

You may have noticed that there's something special about this month's issue- *it's issue number six,* **which means the SaviorLabs Technology Update Newsletter has officially been running for six months!** *I wanted to start off Episode 6 by saying a big thank you to everyone who reads our newsletter each month,* and please keep sending in your feedback and requests for future article topics. ***We greatly appreciate your support!***

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

Humor

As you already know, we like to start off each newsletter with some humor to lighten the mood. In this month's issue, *we decided to feature a handful of our favorite jokes from Reader's Digest.*

Now, **get to reading!**

- What breed of dog can jump higher than buildings?

  —Any dog, *because buildings can't jump.*

- I got my daughter a fridge for her birthday.

  —*I can't wait to see her face light up when she opens it.*

- I poured root beer in a square glass.

  —*Now I just have beer.*

- The numbers 19 and 20 got into a fight.

  —*21.*

- Why can't male ants sink?

  —Because they're *buoy-ant.*

- Want to hear a construction joke?

  —Oh never mind, *I'm still working on that one.*

- I tried to sue the airport for misplacing my luggage.

  —*I lost my case.*

- Where do you find a cow with no legs?

  —*Right where you left it.*

- What type of sandals do frogs wear?

  —*Open-toad.*

- What do you call a boomerang that doesn't come back?

  —*A stick.*

- Did you hear about the kidnapping at school?

  —It's okay. *He woke up.*

- What do you call a bear with no teeth?

  —*A gummy bear.*

- I told my wife she was drawing her eyebrows too high.

  —*She looked at me surprised.*

- Why don't pirates take a shower before they walk the plank?

  —*They just wash up on shore.*

- Moo.

  —Knock knock.
  —Who's there?
  —*Time-traveling cow.*

- I tried to organize a hide-and-seek tournament, but it was a complete failure.

  —*Good players are hard to find.*

- What happens when you rearrange the letters of MAILMEN?

  —*They get really upset.*

And one last longer joke because we couldn't help ourselves:

Phoning a patient, the doctor says, "I have some bad news and some worse news. The bad news is that you have only 24 hours left to live."

"That is bad news," the patient replies. "What's the worse news?"

The doctor answers, ***"I've been trying to reach you since yesterday."***

Did you know?

There's only one letter of the alphabet that doesn't appear in any of the names of the US states: ***the letter Q. How quizzical...***

Align Your Team to Company Targets with Microsoft Viva Goals

You often hear the words **“digital transformation”** and **“collaboration.”** *But what do they actually mean? And what do they mean for the day-to-day of running your business?*

Collaboration can’t happen without shared goals. *When departments are siloed and unconnected, priorities can conflict.* ***People are doing their best but may not be moving in the same direction.***

Digital transformation is simply the use of technology to better reach business goals. *This encompasses moving from analog ways of doing things and transitioning to tools that are more automated and connected.*

Microsoft has been at the forefront of digital transformation and collaboration and its Viva platform drives an improved employee and business-wide experience.

It does this by use of AI, automation, cloud connectivity, and many more helpful tools.

What is Viva Goals?

Viva Goals is one of the newest Viva applications from Microsoft.

It connects teams so they’re moving toward a shared set of goals. *Employees are able to better align with each other, whether someone works in the accounting department or customer support.*

Business leaders can look at Viva Goals as a way to solidify company objectives. ***They can then tie these objectives to meaningful targets for each department.***

For example, say you have a corporate target to provide exceptional customer support. *This goal by itself is generic.* ***It doesn’t connect to what teams need to do to make it happen.***

In Viva Goals, that target can have directives for various teams.

For example: **customer support aims to reduce ticket resolution time by 8 hours. *This brings goals to a meaningful level and allows organizations to track progress.***

Here are the key value-adds of using Viva Goals:

Aligns Your Team to the Same Goals

Viva Goals puts company goals and targets in a tangible form. ***There is a definition of success for teams and individuals, and work outcomes are directly connected to company-wide objectives.***

Maintains Focus on Goals

Viva connects to other M365 apps, making it easier to gather data insights. ***These insights help leaders more easily see goal progress.***

It also helps employees to more easily stay focused on goals. **This is because goals connect to their daily work targets.**

Rather than being something they hear at a company event, *goals get infused into the workflow.*

Integration with Teams & M365

The integration with Teams keeps goals front and center.

Employees get recognized for meeting targets and helping the company achieve its goals. **This keeps everyone engaged and moving together.**

In summary, *Microsoft Viva Goals can help greatly in keeping everyone motivated, aligned with company goals, and on the right track in order to meet and exceed expectations.*

We Love Referrals!

We would love nothing more than for you to refer us to your fellow business owners!

If you do end up referring us, and your friend becomes a client, **we’ll give you a $200 Amazon gift card as a thank you.**

If you do refer us, *be sure to reach out and let us know so we can take care of the rest!*

Here's Why Small Businesses Are Attacked by Hackers 3x More Than Larger Ones

Have you ever felt more secure from cyberattacks simply because you have a smaller business? *Maybe you thought that you couldn't possibly have anything that a hacker could want; after all, how could they know about your small business?*

Well, a new report out by cybersecurity firm Barracuda Networks debunks this myth. *Their report analyzed millions of emails across thousands of organizations.* ***It found that small companies have a lot to worry about when it comes to their IT security.***

In fact, *Barracuda Networks found that employees at small companies saw an alarming 350% more social engineering attacks than those at larger ones.* *It defines a small company as one with less than 100 employees.* ***This puts small businesses at a much higher risk of falling victim to a cyberattack.***

Why Are Smaller Companies Targeted More?

There are many reasons why hackers see small businesses as low-hanging fruit, *and why they are so quickly becoming the targets of hackers out to score an easy cash-out.*

Here are just a few:

Small Companies Tend to Spend Less on Cybersecurity

When you're running a small business, it's often a juggling act of where to prioritize your cash. *You may know cybersecurity is important, but it may not be at the top of your list.* So, at the end of the month when cash runs out, it's moved to next month's to-do list of expenditures.

Small business leaders often don't spend as much as they should on their IT security. *They may buy an antivirus program and think that's enough to cover them.* **But with the expansion of technology to the cloud, that's just one small layer**. ***In reality, you need several more components for adequate security.***

Hackers know all this and see small businesses as an easier target. *They can do much less work to get a payout than they would trying to hack into an enterprise corporation.*

Every Business Has "Hack Worthy" Resources

Every business, even a 1-person shop, has data that's worth scoring for a hacker. *Credit card numbers, SSNs, tax ID numbers, and email addresses are all valuable*. **Cybercriminals can sell all of these on the Dark Web.** From there, other criminals use them for identity theft.

Here are some of the data that hackers will go after:

- ***Customer records***
- ***Employee records***
- ***Bank account information***
- ***Emails and passwords***
- ***Payment card details***

Small Businesses Can Provide Entry Into Larger Ones

If a hacker can breach the network of a small business, they can often make a larger score.

Many smaller companies provide services to larger companies including digital marketing, website management, accounting, and more.

Vendors are often digitally connected to their client's systems.

This type of relationship can enable a multi-company breach. While hackers don't need that connection to hack you, ***it*** *is a nice bonus*.

Small Business Owners Are Often Unprepared for Ransomware

Ransomware has been one of the fastest growing cyberattacks of the last decade.

So far in 2022, over 71% of surveyed organizations experienced ransomware attacks.

The percentage of victims that pay the ransom to attackers has also been increasing. ***Now, an average of 63% of companies pay the attacker money in hopes of getting a key to decrypt the ransomware.***

In summary, *never assume your small business is safe just because it's small.* ***It's better to invest in the protection you might not need than regret not taking care of the safety of your assets.***

Contact SaviorLabs for this very protection.

Learn How to Fight Business Email Compromise

A significant cyber threat facing businesses today is Business Email Compromise (BEC). *BEC attacks jumped 81% in 2022, and as many as 98% of employees fail to report the threat.*

What is Business Email Compromise (BEC)?

BEC is a type of scam in which criminals use email fraud to target victims. These victims include both businesses and individuals. *They especially target those who perform wire transfer payments.*

BEC attacks are usually well-crafted, sophisticated, and very difficult to identify. The attacker first researches the target organization and its employees online. They gain knowledge about the company's operations, suppliers, customers, and business partners.

The scammer will often pretend to be a high-level executive or business partner. Scammers send emails to employees, customers, or vendors. These emails request them to make payments or transfer funds in some form.

The email will often contain a sense of urgency, compelling the recipient to act quickly. The attacker may also use social engineering tactics, *such as posing as a trusted contact or creating a fake website that mimics the company's site.* **These tactics make the email seem more legitimate.**

According to the FBI, BEC scams cost businesses about $2.4 billion in 2021.

These scams can not only cause severe financial damage to businesses and individuals, but can also harm their reputations.

How to Fight Business Email Compromise

BEC scams can be challenging to prevent. ***But there are measures businesses and individuals can take to cut the risk of falling victim to them.***

Here are just a few:

- **Educate employees**
- **Enable email authentication**
- **Deploy payment verification processes**
- **Check financial transactions**
- **Establish a response plan**
- **Use anti-phishing software**

The big takeaway is to always make sure to use cautious, analytical eyes when reading your email.

6 Steps to Effective Vulnerability Management for Your Technology

Technology vulnerabilities are an unfortunate side effect of innovation.

Often times when software companies push new updates, *there are weaknesses in the code they haven't taken the time to catch.* ***Hackers love to exploit these.***

Software makers then try to address the vulnerabilities with something called a security patch, which is more or less a quick fix. *Then the cycle continues with each new software or hardware update.*

An alarming 61% of security vulnerabilities in corporate networks are over 5 years old.

Here are 6 steps to effectively manage your technology's vulnerabilities yourself:

Step 1: Identify your assets

Step 2: Perform a vulnerability assessment

Step 3: Prioritize vulnerabilities by threat level

Step 4: Remediate vulnerabilities

Step 5: Document activities

Step 6: Schedule your next vulnerability assessment scan

We Keep Your
Computers Working
Your Network
SECURE

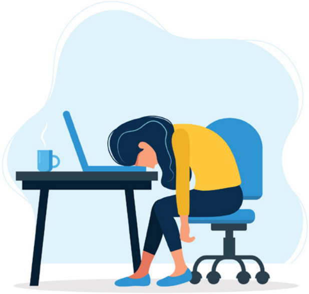
5 Mistakes Companies Make in the Digital Workplace

The pandemic has been a reality that companies around the world have shared. *It required major changes in how they operate.* **No longer did the status quo of having everyone work in the office make sense for everyone.** ***Many organizations had to quickly evolve to working through remote means.***

Overcoming the challenges and reaping the benefits of moving to the digital workplace takes time and effort. **It also often takes the help of a trained IT professional, so you can avoid costly mistakes.**

Here are the top five mistakes companies make when working in the digital workplace:

1. **Poor cloud file organization**
2. **Leaving remote workers out of the conversation**
3. **Not addressing unauthorized cloud app use**
4. **Not realizing remote doesn't always mean from home**
5. **Using communication tools that frustrate everyone**



What Is Push-Bombing & How Can You Prevent It?

Cloud account takeover has become a major problem for organizations.

Between 2019 and 2021, account takeover (ATO) rose by 307%.

Many organizations use multi-factor authentication (MFA) as a way to stop fraudulent sign-ins.

But its effectiveness has spurred workarounds by hackers. ***One of these is push-bombing.***

How Does Push-Bombing Work?

When a user enables MFA on an account, they typically receive a code or authorization prompt of some type.

When the user enters their login credentials, *the system then sends an authorization request to the user to complete their login.*

> "For the Lord God is a sun and shield; the Lord bestows favor and honor. No good thing does he withold from those who walk uprightly." — Psalm 84:11

With push-bombing, hackers start with the user's credentials and take advantage of that push notification process.

They attempt to log in many times. **This sends the legitimate user several push notifications, one after the other.**

When someone is bombarded with these, it can be easy to mistakenly click to approve access.

Push-bombing is a form of social engineering attack designed to:

- ***Confuse the user***
- ***Wear the user down***
- ***Trick the user into approving the MFA request to give the hacker access***

Ways to Combat Push-Bombing at Your Organization

- **Educate employees**
- **Reduce business app "sprawl"**
- **Adopt phishing-resistant MFA solutions**
- **Enforce strong password policies**
- **Put in place an advanced identity management solution**

Additionally, businesses can use identity management solutions to install contextual login policies.

Contact Us

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

SaviorLabs LLC
273 Middleton Road
Boxford, MA 01921

Place
Stamp
Here

To:

In This Issue

SCAN ME

READ THIS NOW