TECHSAGE
Monthly Newsletter

Tech News
YOU CAN USE

Tips & Awesome Info for Technology
www.techsagesolutions.com

Your monthly newsletter provided by John Hill, President and CEO of TechSage Solutions

Inside This March Issue

5 Signs You're About To Get Hacked — And What You Can Do To Prevent It

Hackers love to go after small businesses. There are many businesses to choose from, and many don't invest in good IT security. Plus, many business owners and their employees have bad cyber security habits. They do things that increase their risk of a malware attack or a cyber-attack. Here are five bad habits that can lead to a hack and what you can do to reduce your risk.

1. Giving out your e-mail Just about every website wants your e-mail address. If you share it with a vendor or e-commerce site, it's usually not a big deal (though it varies by site – some are more than happy to sell your e-mail to advertisers). The point is that when you share your e-mail, you have no idea where it will end up – including in the hands of hackers and scammers. The more often you share your e-mail, the more you're at risk and liable to start getting suspicious e-mails in your inbox.

If you don't recognize the sender, then don't click it. Even if you do recognize the sender but aren't expecting anything from them and do click it, then DO NOT click links or attachments. There's always a chance it's malware. If you still aren't sure, confirm with the sender over the phone or in person before clicking anything.

2. Not deleting cookies Cookies are digital trackers. They are used to save website settings and to track your behavior. For example, if you click a product, cookies are logged in your browser and shared with ad networks.

Continued on pg.2

Continued from pg.1

This allows for targeted advertising. There's no good way to tell who is tracking online. But you can use more secure web browsers, like Firefox and Safari. These browsers make it easy to control who is tracking you.

In Firefox, for example, click the three lines in the upper right corner, go into the Options menu and set your Privacy & Security preferences. Plus, every web browser has the option to delete cookies – which you should do constantly. In Chrome, simply click History, then choose "Clear Browsing Data." Done. You can also use ad-blocking extensions, like uBlock Origin, for a safe web-browsing experience.

3. Not checking for HTTPS Most of us know HTTP – Hypertext Transfer Protocol. It's a part of every web address. However, most websites now use HTTPS, with the S meaning "secure." Most browsers now automatically open HTTPS websites, giving you a more secure connection, but not all sites use it.

If you visit an unsecured HTTP website, any data you share with that site, including date of birth or financial information, is not secure. You don't know if your private data will end up in the hands of a third party, whether that be an advertiser (most common) or a hacker. Always look in the address bar of every site you visit. Look for the padlock icon. If the padlock is closed or green, you're secure. If it's open or red, you're not secure. You should immediately leave any website that isn't secure.

> **"Good IT security can be the best investment you can make for the future of your business."**

4. Saving passwords in your web browser Browsers can save passwords at the click of a button. Makes things easy, right? Unfortunately, this method of saving passwords is not the most secure. If a hacker gets your saved passwords, they have everything they could ever want. Most web browsers require a password or PIN to see saved passwords, but a skilled hacker can force their way past this if given the chance.

Protect yourself with a dedicated password manager! These apps keep passwords in one place and come with serious security. Password managers can also suggest new passwords when it's time to update old passwords (and they remind you to change your passwords!). LastPass, 1Password and Keeper Security Password Manager are good options. Find one that suits your needs and the needs of your business.

5. You believe it will never happen to you This is the worst mentality to have when it comes to cyber security. It means you aren't prepared for what can happen. Business owners who think hackers won't target them are MORE likely to get hit with a data breach or malware attack. If they think they are in the clear, they are less likely to invest in good security and education for their employees.

The best thing you can do is accept that you are at risk. All small businesses are at risk. But you can lower your risk by investing in good network security, backing up all your data to a secure cloud network, using strong passwords, educating your team about cyberthreats and working with a dedicated IT company. Good IT security can be the best investment you make for the future of your business.

Free Cyber Security Assessment Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security assessment to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To get started and claim your free assessment now, go to:

www.techsagesolutions.com/cyber-security-assessment/ or Call 210-582-5814

Password Report Card

Most people are failing miserably when it comes to password length and complexity. The most common passwords (cleartext, alphanumeric) are all brute forcible in a matter of seconds. This is if they have not already been exposed (unencrypted) in a previous data breach.

So how does your password stand up when it comes to crack-ability?

Check your passwords against this grade sheet, to see whether you would "pass" or "fail" the test.

All numbers or lowercase characters
(8 or fewer characters)

- Example: "123456"/ "soccer"
- Brute-forcible in the blink of an eye. Most people know not to do this. If you are still doing this, just stop it already!

F

Combination of numbers and lowercase characters
(8 or fewer characters)

- Example: "ncc1701"/ "michael1"
- Slightly better, but still super easy to guess or crack!

F

Combination of numbers, upper and lowercase characters
(8 or fewer characters)

- Example: "Drag0n!"/ "Cowboys#1"
- Where most people are at these days. Dictionary attacks will break both in a matter of minutes.
- Other considerations:
  - Often harder for an individual to remember.
  - When it comes time to change, most will just iterate; i.e., "Cowboys#1" becomes "Cowboys#2"

D

Long password phrases

- Example: "correcthorsebatterystaple"
- Better than those above. Easier to remember and the length of the password makes it harder to crack.

B-

Long password phrases with a "stop" character, symbol or number

- Example: "webutterthebre%adwithbutter"
- About the best you can do (other than increasing length).

B

Password Managers

- Randomly generated long passwords take the most exploitable element (the human element) out of password creation.

A+

TechSage Solutions

SHINY NEW GADGET OF THE MONTH

ThePhotoStick Mobile

Never worry about running out of memory on your smartphone again! It happens to all of us – you're trying to take a picture or record a video and you get a message saying your phone's storage is full. You don't want to buy another new smartphone, so what can you do besides delete old photos?

This is where ThePhotoStick Mobile comes in. It's a memory stick compatible with most Android and iPhone devices and will boost your phone's memory without your having to buy a new phone. ThePhotoStick Mobile is an insurance policy against lost photos and videos.

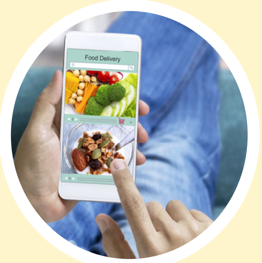
ThePhotoStick Mobile gives you more control. While most smartphones work without a hitch for years, you never know if something might happen or if you'll run out of memory. ThePhotoStick Mobile plugs into your device and allows you to copy photos over. You can keep them on ThePhotoStick or transfer them to another device. Learn more at GetPhotoStickMobile.io!

3 Top Smartphone Security Best Practices

Security for your smartphone is just as important as IT security for your business. It starts with best practices to keep cybercriminals from stealing your data. Here are three ways to keep your smartphone more secure.

Monitor app permissions. Many apps ask for permission to access your camera, calendar or contacts. For some apps, you can say yes – if it makes sense and you trust the app. For everything else, say no. Newer phones make it easy to configure permissions.

Keep your phone and apps updated. Make sure your apps and your phone's operating system are constantly updated to receive the latest security patches. The best way to do this is to set everything to automatically update.



Download from trusted sources. Only download apps from Google Play and Apple's App Store. Look up the app developer and read reviews and descriptions to make sure the app you're downloading is legitimate.

Who Is Responsible For Your Corporate Culture?

"Corporate culture" is the fundamental character or spirit of an organization that influences the loyalty and general behavior of its employees. When you learn how to combine the right corporate culture with the right core values, your organization will thrive regardless of the challenges it faces.

One problem I see in most companies today is they create a mission statement only because it's fashionable to do so … but they stop there. Some may even go so far as to create a list of core values to help guide their leadership and employees … but they fail to follow them. I see lots of mission, vision and value statements on corporate websites, but the majority of employees in any company cannot recite any of them.

Several months ago, one of my clients wanted me to work with their senior management team to identify ways they could create better employee engagement. An anonymous survey was conducted, and it turned up some alarming comments. Over 50% of their employees stated that the company:

- Isn't results-oriented
- Doesn't celebrate accomplishments
- Doesn't have training for growth
- Doesn't allow them to generate ideas
- Isn't empowering them
- Has leaders who play favorites
- Has leaders whose actions do not match their words
- Doesn't involve them in the decisions that affect their jobs
- Doesn't keep them informed about changes or important issues

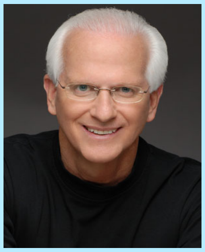
This company has five excellent "Guiding Principles" (core values) that address all these issues, but they weren't being followed. What most companies don't understand is that their "corporate culture" is in the hands of local middle management. In other words, your corporate culture is your LOCAL BOSS. They are responsible for making sure your guiding principles, core values, and mission and vision statements are being followed.

Last week I did a program for Herr Foods. Herr Foods understands the importance of living their core values. They have been in business for over 70 years and have over 1,500 employees. Their formula for success is based on the acronym L.O.V.E., which stands for:

L - Live
O - Our
V - Values
E - Every day

A recent Gallup poll found that only 34% of workers are committed to their company and are enthusiastic about their work. That means 66% are NOT engaged; they are just going through the motions, collecting a paycheck. As you look to the future, recognize that the principles that are instrumental to your success must be communicated throughout your organization on a constant basis. They should not only be part of your new employee training; they should also be part of every meeting, deeply rooted into every decision you make.

When your corporate culture is right, employees working for you no longer have jobs; in their minds, THEY HAVE CAREERS.



Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys *and* 52 Essential Habits For Success, *he's shared the podium with esteemed figures from across the country, including former President George H.W. Bush, former Secretary of State Colin Powell, Anthony Robbins, Tom Peters and Steven Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.*

Don’t Make This Critical Mistake In Your Business

Upward of 41% of companies don’t train their HR staff on data security. This is from a recent survey from GetApp. On top of this, 55% of HR staff don’t see internal data security as an issue.

HR departments often handle sensitive data and should take IT security very seriously. If a hacker were to get ahold of employee data, it could be potentially devastating to affected employees and to the company as a whole – and it could set up the company for a major lawsuit on the part of the employees.

The liability by itself isn’t worth it and neither is taking on the risk by not investing in data security. Data protection needs to be in place – along with employee training. Everyone, including HR, should be on the same page, and every company should adopt strong data security and policy to go along with it. *Small Business Trends, Nov. 30, 2019*

Follow This One Rule When Sending E-mails

We all use e-mail, and we all spend too much time reading and responding to these messages (one estimate cited by Inc. suggests the average office worker spends 2 1/2 hours per day reading and responding to e-mails).

Wasn’t e-mail supposed to save time? It can if you follow one important rule. It’s all about streamlining your process. That rule? The CC rule.

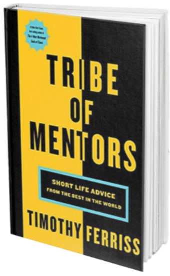
It works like this: If you expect a reply from a recipient, you put their name in the “to” field. If you want to add more people to read your message but don’t need a reply from them, put them in the “CC” field.

However, for the rule to work, everyone in the e-mail has to know how it works. If the e-mail is addressed “to” you, respond. If not and you’re just CC’d, do not respond. *Simple. Inc., Dec. 10, 2019*

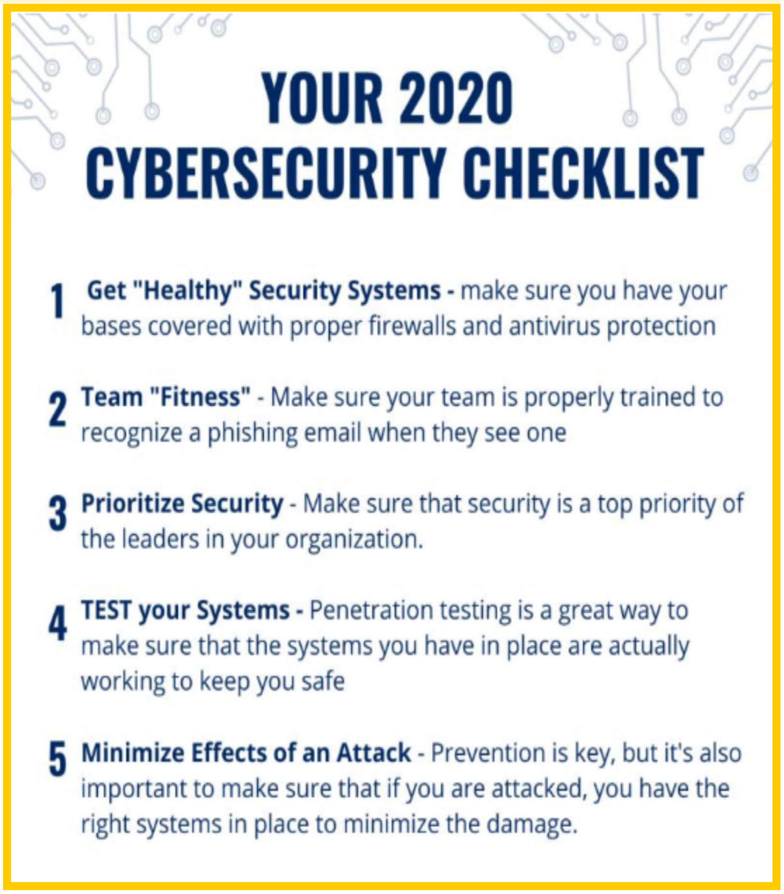
Tribe Of Mentors: Short Life Advice From The Best In The World

By Timothy Ferriss

Timothy Ferriss is renowned for *The 4-Hour Workweek*. It’s been a go-to book for countless entrepreneurs for over the past decade. Ferriss’s *Tribe Of Mentors: Short Life Advice From The Best In The World*, however, takes things in a new direction. Ferriss is looking for answers to questions like, “What’s next?”



He finds the answers by assembling a “tribe of mentors” – in this case, over 100 celebrities, athletes, founders and other entrepreneurs who found major success. He brings together their wisdom in life and business and shares it with readers. At the same time, the book highlights the importance of surrounding yourself with people you can lean on when you have questions about life or business – or when you need help to figure out “what’s next?



YOUR 2020 CYBERSECURITY CHECKLIST

1 **Get "Healthy" Security Systems -** make sure you have your bases covered with proper firewalls and antivirus protection

2 **Team "Fitness"** - Make sure your team is properly trained to recognize a phishing email when they see one

3 **Prioritize Security** - Make sure that security is a top priority of the leaders in your organization.

4 **TEST your Systems -** Penetration testing is a great way to make sure that the systems you have in place are actually working to keep you safe

5 **Minimize Effects of an Attack** - Prevention is key, but it's also important to make sure that if you are attacked, you have the right systems in place to minimize the damage.