TECHSAGE
Monthly Newsletter

Tips & Awesome Info for Technology
www.techsagesolutions.com

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

Inside This April Issue

Your #1 Threat Of Being Hacked Is INSIDE Your Own Organization

Small businesses are the biggest targets of hackers and cybercriminals. They are targeted because they are less likely to have strong – or any – security in place. But in so many cases, hackers don't need to use malicious code or cracking skills to get what they want. Instead, they rely on your biggest vulnerability: your own employees.

The #1 threat to any business's IT security is its employees. It all stems from a lack of training. Employees don't know how to spot threats, or they don't know not to click unverified links in their e-mails. Most of the time, these actions are simple mistakes – but mistakes aren't excuses and can result in MAJOR costs to your business.

Here are three things you can do to turn your employees from your biggest IT threat to your biggest IT asset:

Establish Regular Cyber Security Training.

First and foremost, get *everyone* in your business trained up on IT security. Wesley Simpson, the chief operating officer of $(ISC)^2$, an international cyber security certification group, suggests thinking about IT education as "people patching." Just as you continually update and patch your software and security, ongoing education serves to update, or patch, your employees. He says, "If you don't get your people patched continually, you're always going to have vulnerabilities."

Continued on pg.2

Continued from pg.1

But don't put the training solely on your shoulders. Work closely with a company that specializes in IT security. Doing it yourself can be stressful and time-consuming. An experienced IT firm is going to come in with all the education and resources you need to successfully train everyone in your organization on cyberthreats targeting your business today.

Keep Cyber Security Top Of Mind.

While you may have training or educational sessions once a quarter or biannually (regular sessions are recommended), you still need to keep IT security in the minds of your employees on a weekly basis. During weekly meetings, for example, talk about a cyber security topic. Or, if you share news or links with your employees in a weekly, company-wide e-mail, for example, include a cyber security story or tips article. It's all about utilizing systems you already have in place to keep your team informed and this important topic at the forefront.

Emphasize Safe Internet Usage Habits.

This should supplement regular training. Employees should always know the best practices when it comes to using the Internet, e-mail or anything else that brings them in contact with the World Wide Web. Part of it involves keeping the lines of communication open. If an employee sees something out of the ordinary come into their inbox, encourage them to bring it to the team's attention – whether they're telling their direct supervisor, manager or you. The easier the communication between everyone on your team, the easier it is to identify and stop attacks.

The goal is to eliminate guesswork. If an employee isn't sure about an e-mail, they should be trained to ask questions and verify. On top of that, you should have a policy in place that prevents employees from installing unverified software, which includes apps and app extensions (such as browser extensions), without permission. And one more thing – stress safe Internet usage habits not just in the workplace but at home as well. This is especially critical if your employees are bringing in their own devices. If that's the case, you should absolutely have a "bring your own device" (BYOD) security policy in place. It's just another wall between your business and potential threats.

How do you get all this started? Good question! It all starts with reaching out. If you're ready to lock down your business and you're serious about educating your employees and turning them into your best defense, we can help. The best IT security you've ever had is one phone call away.

> **"The #1 threat to any business's IT security is its employees."**

How Teams Can Stay Connected & Productive When Working Remotely

Whether you've worked on a team with members across different geographic locations, or if you have full remote employees on you team already, we have ways to work within the confines of temporary team member isolation. This free report will give you some tips and suggestions for how your company can stay productive and communicate during your time working from home.

To get started and claim your FREE Report now, go to:

www.techsagesolutions.com/files/2020/04/Covid-19-Stay-Connected-and-Productive-When-Working-Remotely.pdf

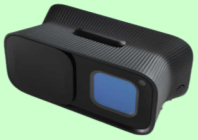
SHINY NEW GADGET OF THE MONTH

NexOptic DoubleTake Binoculars

Binocular technology has remained the same for a long time – and for good reason! It works well. But now, one company has decided to bring binocular optics into the 21st century and give it a technological makeover.

NexOptic's DoubleTake blends binoculars with common smartphone technology. With 10x digital zoom and a wide field lens, DoubleTake delivers outstanding 4K video and high-resolution photos. Plus, it's packed with a powerful imaging processor to ensure your videos and photos look fantastic every time, and its compact size makes it ideal for travel.

DoubleTake's battery provides three hours of continuous use, meaning it will last most people several days or more before the next charge. Images are saved to an onboard memory card and can be sent over WiFi to your phone or other device for easy sharing or personal use. Learn more at **NexOptic.com/doubletake.**



Are Browser Extensions Safe?

Browser extensions let us customize our Internet experience. You can find extensions to help with productivity or block ads. But how do you know if an extension is safe or not? Thankfully, there are red flags you can look for. Here are two common examples.

Permission Pop-Ups
After downloading a new extension, you may see a pop-up asking to "access your browsing activity" or something similar. While most extensions don't have malicious intent (they aren't going to sell your data), others might. If you aren't comfortable with this, you can deny permission or uninstall the extension.

An Extension's Legitimacy
There are a lot of copycats out there – scummy developers use icons or names similar to popular extensions and hope people download them by mistake. Read all the details on the extension download page and verify that the developer (or "offered by") name is correct.

Anticipating Customer Needs

What is the best way to create a loyal customer base and, therefore, a more profitable business?

Anticipate Customer Needs.

Anticipating needs is the best way to let your customers know that their success is your priority. When you deliver something customers need without asking, you create a sense of ease and let them know you have their best interests in mind – a proverbial "I have your back."

The most effective way to anticipate the needs of your customers is to know them well. How else will you know what their expectations are? You have to create a relationship with them to identify what their demands are and fulfill them before they even know what they wanted. So, how do we go about this? Here are just a few examples.

Establish A Relationship.

In most of my books, I have a call to action. I ask readers to e-mail me to make their commitment to improving their businesses. Developing this dialogue with readers is an act of accountability on both of our parts. Moreover, it is a big leap of faith for some, and I am honored they trust me. They tell me why they are committed, and I let them know I am here and interested in helping them succeed. My hope is that they feel less alone in their struggles as business owners and more motivated to make the necessary changes they need for a successful business.

Exceed Expectations.

The responses from readers when they receive e-mails or videos from me has been overwhelmingly positive. It seems that most assume their e-mails will go into a black hole, never to be answered. Not only do I answer, but I also include a ton of resources that basically equal free coaching. There is an FAQ, links to my *Entrepreneurship Elevated* podcast, links to find a Profit First Professional and become a Profit First Professional, links to Clockwork resources, links to Pumpkin Plan resources … You get my drift. And while it could be interpreted as marketing, anyone who knows me knows I am out to empower others and help their businesses become more profitable. I often get e-mails from readers who are pleasantly surprised – they are getting answers to questions before they even knew they had them. See? Anticipating needs!

Ask For Feedback.

I often request reviews of my books. Is this because I want to hear how great they are? No. I ask for reviews because I want that honest feedback. How the heck else will I know what to write next? How will I know what problems need solving and what business solutions entrepreneurs are seeking if I don't ask? Getting reviews enables me to focus on these key areas where business owners are trying to improve.

MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford – a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group. He is also a former small-business columnist for The Wall Street Journal; *MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book* The Toilet Paper Entrepreneur. *His newest book,* The Pumpkin Plan, *has already been called "the next E-Myth!" For more information, visit MikeMichalowicz.com.*

Cybercriminals Are Counting On You Letting Your Guard Down During This Global Pandemic- Here's How To Stop Them

The world is slowing down during this COVID-19 pandemic. Wall Street is being hit hard. People are no longer going out. We're told to quarantine or self-isolate and not engage in groups.

You can bet there's one group that's not slowing down at all. In fact, they're probably working overtime while the rest of us have our lives turned upside down. Cybercriminals and hackers know there's no better time to strike than during a global crisis. While you are distracted and spending your time trying to make sense of this new normal, they are finding new ways into your IT network so they can steal data and passwords, compromise your clients' private information and even demand large ransoms.

Cybercrime is already on the rise and is expected to cause $6 TRILLION in damages by 2021! But, if history repeats itself, hackers will be out in full force throughout this coronavirus scare. We fully expect in the upcoming weeks that headlines will change from stories about COVID-19 to accounts of a frenzy of cyber-attacks on corporations and small businesses.

Here are solutions you can implement now to help protect your business data, money and productivity:

1. Be more suspicious of incoming e-mails.
Because people are scared and confused right now, it's the perfect time for hackers to send e-mails with dangerous malware and viruses. At this moment, your in-box is probably filled with "COVID-19" subject lines and coronavirus-focused e-mails. Always carefully inspect the e-mail and make sure you know the sender. There's a cdc-gov e-mail address out there now that's not legitimate and is spamming in-boxes across the country.

Avoid clicking links in the e-mail unless it's clear where they go. And you should never download an attachment unless you know who sent it and what it is. Communicate these safeguards to everyone on your team, especially if they are working from home.

2. Ensure your work-from-home computers are secure.
Another reason we expect a rise in cyber-attacks during this pandemic is the dramatic increase in employees working from home. Far too many employers won't think about security as their team starts working at the kitchen table. That's a dangerous precedent.

First, make sure your employees are not using their home computers or devices when working. Second, ensure your work-at-home computers have a firewall that's turned on. Finally, your network and data are not truly secure unless your employees utilize a VPN (virtual private network). If you need help in arranging your new work-from-home environment, we would be happy to get your entire team set up.

3. Improve your password strategy.
During crises like the one we are all facing right now, your passwords could mean the difference between spending your time relearning how to grow your business and trying to recoup finances and private data that's been hacked. Make a point now to reevaluate your passwords and direct your team to create stronger passwords.

Also, while it's so convenient to save your passwords in your web browser, it also lessens your security. Because web browsers simply require their own password or PIN to access

saved passwords, a skilled hacker can bypass this hurdle. Once they access your saved passwords, they can steal as much as they want – credit card information, customers' private data and more!

Instead, you should consider a password manager to keep all of your passwords in one place. These password managers feature robust security. A few options are (MyGlue, LastPass)

You, your team and your family have enough to concern yourselves with in regards to staying healthy, living a more isolated lifestyle and keeping your business strong. There's no need to invite in more problems by letting your computer and network security slide during these times.