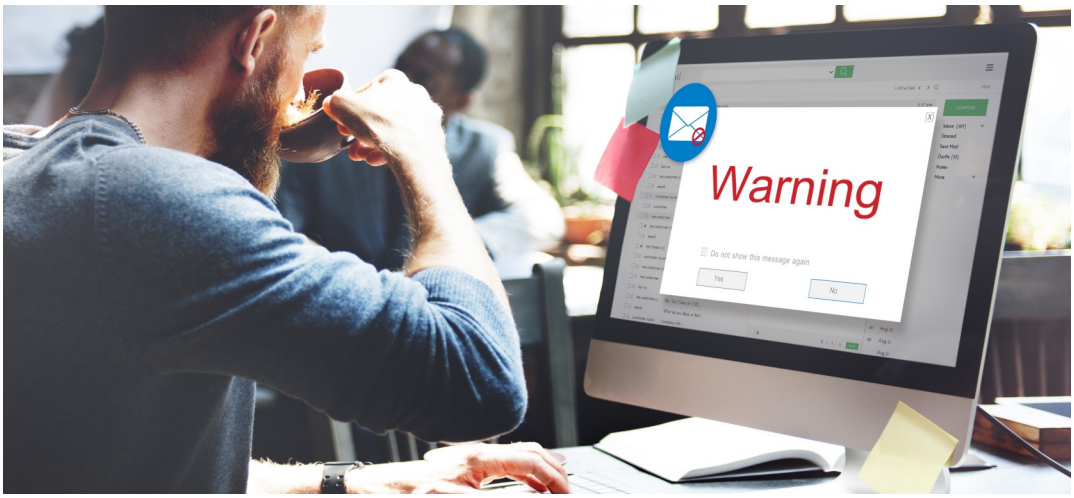
March 2021

CSU Connection



Employees Are Letting Hackers Into Your Network ...
What You Can Do To Stop It

Cyberthreats are everywhere these days. Hackers, scammers and cybercriminals are working overtime to break into your network – and the network of just about every business out there. They have a huge arsenal of tools at their disposal, from automated bots to malicious advertising networks, to make it possible.

But there is one "tool" that *you* may be putting directly into their hands: your employees. Specifically, **your employees' lack of IT security training**.

While most of us expect hackers to attack from the outside using malware or brute-force attacks (hacking, in a more traditional sense), the truth is that most hackers love it when they can get others to do their work for them.

In other words, if they can fool your employees into clicking on a link in an e-mail or downloading unapproved software onto a company device, all the hackers have to do is sit back while your employees wreak havoc. The worst part is that your employees may not even realize that their actions are compromising your network. And that's a problem.

Even if you have other forms of network security in place – malware protection, firewalls, secure cloud backup, etc. – it won't be enough if your employees lack good IT security training. In fact, a lack of training is the single biggest threat to your network!

It's time to do something about it. Comprehensive network security training accomplishes several things, including:

1. Identifying Phishing E-Mails Phishing e-mails are constantly evolving. It used to be that the average phishing e-mail included a message littered with bad grammar and misspelled words. Plus, it was generally from someone you'd never heard of.

These days, phishing e-mails are a lot more clever. Hackers can spoof legitimate e-mail addresses and websites and make

Continued on pg.2

Quote of the Day:

"THE BEST WAY TO GET STARTED IS TO QUIT TALKING AND BEGIN DOING."

– WALT DISNEY

Our Mission

is to deliver outstanding IT support to your business in order to improve uptime, productivity, and profitability.
You take care of running your business. We'll take care of your technology.

This monthly publication provided courtesy of Michelle Sherman, President of Computer Services Unlimited

Continued from pg.1

their e-mails look like they're coming from a sender you actually know. They can disguise these e-mails as messages from your bank or other employees within your business.

You can still identify these fake e-mails by paying attention to little details that give them away, such as inconsistencies in URLs in the body of the e-mail. Inconsistencies can include odd strings of numbers in the web address or links to YourBank.**net** instead of YourBank.**com**. Good training can help your employees recognize these types of red flags.

2. Avoiding Malware Or Ransomware Attacks One reason why malware attacks work is because an employee clicks a link or downloads a program they shouldn't. They might think they're about to download a useful new program to their company computer, but the reality is very different.

Malware comes from many different sources. It can come from phishing e-mails, but it also comes from malicious ads on the Internet or by connecting an infected device to your network. For example, an employee might be using their USB thumb drive from home to transfer files (don't let this happen!), and that thumb drive happens to be carrying a virus. The next thing you know, it's on your network and spreading.

This is why endpoint protection across the board is so important. Every device on your network should be firewalled and have updated malware and ransomware protection in place.

> **"Every device on your network should be firewalled and have updated malware and ransomware protection in place."**

If you have remote employees, they should only use verified and protected devices to connect to your network. (They should also be using a VPN, or virtual private network, for even more security.) But more importantly, your employees should be trained on this security. They should understand why it's in place and why they should only connect to your network using secured devices.

3. Updating Poor Or Outdated Passwords If you want to make a hacker's job easier than ever, all you have to do is never change your password. Or use a weak password, like "QWERTY" or "PASSWORD." Even in enterprise, people still use bad passwords that never get changed. Don't let this be you!

A good IT security training program stresses the importance of updating passwords regularly. Even better, it shows employees the best practices in updating the passwords and in choosing secure passwords that will offer an extra layer of protection between your business and the outside world.

If you or your employees haven't updated their passwords recently, a good rule of thumb is to consider all current passwords compromised. When hackers attack your network, two of the big things they look for are usernames and passwords. It doesn't matter what they're for – hackers just want this information. Why? Because most people do not change their passwords regularly, and because many people are in the habit of reusing passwords for multiple applications, hackers will try to use these passwords in other places, including bank accounts.

Don't let your employees become your biggest liability. These are just a few examples of how comprehensive IT and network security training can give your employees the knowledge and resources they need to help protect themselves and your business. **Just remember, you do not have to do this by yourself! Call CSU to get enrolled in Cyber Security Training.**

Shiny New Gadget Of The Month: FitTrack: Sticker—The Smallest Finder By Tile

First, there was the Tile – a small, square device used to find just about anything. You attach Tile to the thing you don't want to lose (keys, for example) and you pair Tile with the Tile app. Easy!

Now, Tile has introduced Sticker, their "smallest finder." It's a mini-version of their popular fob, and it can be stuck to just about anything, from TV remotes and portable electronics to tools, bikes, you name it – anything you don't want to go missing.

Plus, not only does Sticker stick to anything, but it also has a three-year battery life, so as they say, "you can set it and forget it." Once it's paired with the smartphone app, it's super-easy to track. And if you lose a "Stickered" device, Sticker emits a loud ring to help you locate your misplaced item, at a range of about 150 feet. Learn more about Sticker at:

TheTileApp.com/en-us/store/tiles/sticker.

Going Strong Or Burning Out?

"Burnout is what happens when you try to avoid being human for too long."
–Michael Gungor

What Is Burnout?

Burnout is a syndrome conceptualized as resulting from chronic workplace stress that has not been successfully managed. It is characterized by:

- Feelings of energy depletion or exhaustion
- Increased mental distance from one's job or feelings of negativism or cynicism related to one's job
- Reduced professional efficacy

This is considered in occupational context and should not be applied to experiences in other areas of life.

Ask yourself, how many times have you felt burnout in your career? Those who are highly engaged in their work are more likely to have burnout, not necessarily people who just "clock in and clock out." Just because someone is productive does not mean they aren't at risk.

Why do we keep putting ourselves in stressful situations? Stress can be an addiction.

- People want to make sure they are good enough and want to feel valuable.
- It can give you the sense of feeling significant and important.
- There's a sense of guilt and fear of not doing enough.

As long as stress is satisfying those needs, you will not get rid of that behavior. Start flipping how you are satisfying your needs in order to get rid of that behavior.

Burnout Signals – Emotions And Feelings

If you are feeling like this every day, you may be burnt out:

- Physical and emotional exhaustion
- Lack of energy
- Feeling sad or hopeless
- Lack of joy from things that used to bring you joy at work
- Diminished connection with colleagues
- Feeling like you are not contributing anything to your job

What Is The Cause?

- Heavy workloads
- Job insecurity
- Frustrating work routines (too many meetings, far too little time for creative work)
- Crunch on downtime that is necessary for restoration

Burnout = High Resources + High Demands

High Resources:

- Supervisor support
- Rewards and recognition
- Self-efficacy and work

Low Demands:

- Low workload
- Low cumbersome bureaucracy
- Low to moderate demands on concentration and attention

What's Needed?

- Employee support/high resources
- Acknowledgment/feel good about work
- Opportunities for recovery from stress
- Mental and emotional well-being

Reevaluate

- Zero-base meeting calendar
- Team up the A-players
- Culture around "precious time" and wellness

Mark Comiso has over 25 years of experience in founding, building and scaling numerous companies. He's been with start-ups and publicly traded companies, including digital marketing agencies, SaaS companies and much more. He's renowned for helping other entrepreneurs grow their own businesses, and as a longtime member and leader within Entrepreneurs' Organization (EO), he's well-suited for the task!

3 Simple Yet Effective Ways To Boost Employee Morale

Good employee morale is essential to any successful business. It's a reflection of company culture and has a direct impact on not just happiness but also productivity. Here are three surefire ways to improve morale within your organization:

1) Keep The Door Open. When supervisors or management vanish without a trace, it hits morale hard. It's crucial to be present and available to your team. Sometimes it's as simple as keeping the door open, but it also includes having transparent communication. Keep people looped in, especially when there are good things to report on. On top of that, have regular one-on-one chats with everyone on the team and make sure their needs are being met.

2) Emphasize Mental Health. Everyone should have their mental health acknowledged. Always take time to assess the mental health of everyone on your team. If they need to take a break or refocus, make sure they do. If they need a mental health day (or a vacation), encourage it. Be flexible and understanding.

3) Reward And Recognize. Make sure hard work gets recognized and people get credit for that hard work. Shout out star players during meetings and make sure everyone (including management) sees the good work that's being done. And don't hesitate to dole out rewards (lunch, gift cards, etc.) in recognition of that hard work, as well. *Inc., Nov. 4, 2020*

How Big Data Reveals The Humans Behind Your Users

The Internet is a data mine. From search engines to ad clicks, we can see what people are interested in. Big Data is accessible to just about every business, and it can tell you a lot about the people you do business with — or the people you want to do business with.

If you aren't tapping into Big Data (Google Analytics is an example), you're missing out. You can use data to hone in on the customers you want to acquire and reduce those costs at the same time. You can better develop products and services you know customers will love. And you'll be able to adapt to changing trends driven by real people. *Inc., Feb. 26, 2015*