

TECHNOLOGY TIMES

“Insider Tips To Make Your Business Run Faster, Easier And More Profitably”

Fun Facts!

Held every October, National Cybersecurity Awareness Month (NCSAM) is a collaborative effort between government and industry to raise awareness about the importance of cybersecurity and to ensure that all Americans have the resources they need to be safer and more secure online.



3 Ways To Prevent Your Employees From Leaking Confidential Information

A lot of businesses need to come to terms with the fact that their employees are their greatest IT threat. As a business owner, you may be aware of cyberthreats to your business, but your employees might not be. They might not know about the threat of cyber-attacks or malware. They might use unsecured WiFi on company equipment. As a result, your employees may be putting your business at serious risk.

What can you do to change that?

1. IT ALL STARTS WITH EDUCATION. One of the biggest reasons why employees put their employer at risk simply comes down to a lack of education. They don't know about the threats targeting businesses or that small businesses are a major target of hackers and scammers.

You need to do everything you can to train your employees. Give them the education and resources to be a line of

defense rather than a risk. Develop a consistent training regimen. If you need to bring in IT professionals to help, do it. Don't make assumptions about critical IT security training if you aren't sure. Professionals can answer your questions and make sure you and your employees have everything you need to know to keep your business secure.

Another important thing is to **hold this training regularly**. Threats evolve, and you need to stay ahead of the curve. Keep IT security on the minds of your employees. When they forget about it, that's when the risk is highest.

2. SAY NO TO UNSECURED, PUBLIC WIFI. This is a big problem for businesses with remote employees, employees who work from home or employees who use company technology outside of the business walls. According to a Spiceworks study, 61% of employees said they have connected to unsecured WiFi while working remotely.



October 2019



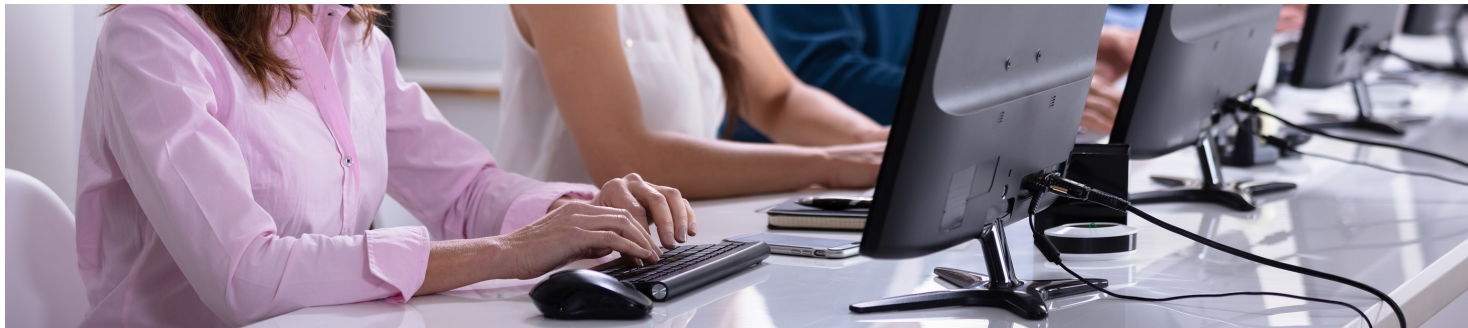
This monthly publication provided courtesy of Todd Clark President of DenaliTEK Inc.

Our Mission:

“Through our core values and technology, continually protect and enrich every organization we’ve been given the privilege to serve.”

Continued on pg.2

**Get More Free Tips, Tools and Services At Our Web Site: www.denalitek.com
(907) 865-3100**



This is cause for concern. Connecting to public WiFi is like leaving the front door of your home wide-open while posting on social media that you're going to be out of town for a week. You never know who is going to let themselves in and snoop around. Hackers use public hot spots to circulate malware and steal data. Sometimes they even set up fake hot spots with the same name as a legitimate hot spot to trick users into connecting to their WiFi, which makes data theft *even easier*.

Discouraging your employees from using unsecured, public WiFi is a good step to take, but don't be afraid to take it further. Don't let them connect company equipment to unsecured WiFi *at all*. And place a bigger focus on endpoint security – make sure your equipment has up-to-date software, malware

“It's all about understanding the threats and taking a proactive approach to security.”

protection, local firewalls, as well as a VPN (virtual private network). The more layers of security, the better.

3. PROTECT ALL OF YOUR DATA. Your employees should never save personal or business data on portable/ external hard drives, USB drives or even as printed material – and then take that data out of the office. The theft of these types of devices is a real threat. An external hard drive is a tempting target for thieves because they *will* search the drive for sensitive data, such as financial or customer information that they can use or sell.

If you have remote employees who need to access company data, put a method in place to do just that (it should be discussed as part of your regular company IT security training). They need to know how to properly access the data, save the data or delete it, if necessary. Many businesses go with a secure cloud option, but you need to determine what makes the most sense for your business and its security.

While these three tips are great, nothing beats helping your employees develop a positive IT security mindset. It's all about understanding the threats and taking a proactive approach to security. Proactivity reduces risk. But you don't have to go it alone. Working with experienced IT security professionals is the best way to cover all your bases – and to ensure your employees have everything they need to protect your business.

FREE Report: The Top 10 Ways Hackers Get Around Your Firewall And Anti-Virus To Rob You Blind



You will learn:

- The #1 threat to your business that even the BEST firewalls and anti-virus software can't protect against (and what you need to do now to remedy it).
- A common misconception about employee devices on your office network and exactly what you need to do now to shut this down immediately.
- The shocking facts about why small business are the #1 target of cybercriminals - more than half of the reported cyber attacks are focused on small business for this one main reason that is easily fixed.
- How to keep your network secure with the proliferation of mobile devices, cloud applications, e-mail, and social media sites connecting to your computer network.

Claim your FREE copy today at
www.denalitek.com/10ways

Shiny New Gadget Of The Month:



The Philips Somneo Sleep & Wake-Up Light

Research suggests that when you wake up naturally (that is, you aren't jolted awake by an alarm or radio), you feel more refreshed and energized during the day.

The Philips Somneo Sleep & Wake-Up Light puts this research to the test. It's designed to simulate a natural sunrise right in your bedroom. You can set it to your specific needs, and it will slowly and steadily brighten when you need to wake up. It can also simulate a sunset for the opposite effect when you're going to bed! You can even use the light as a reading lamp — and it has a built-in radio, too!

The Philips Somneo Sleep & Wake-Up Light is a versatile device, perfect for anyone who wants to get a better night's sleep. Find it at Amazon and many other electronic retailers.



How can you build your confidence as a CEO, investor or entrepreneur? New CEOs have imposter syndrome. Private equity investors who just raised another \$1 billion-plus fund read newspaper headlines about the coming recession and quietly gulp. Self-made billionaire entrepreneurs worry that their fortunes will take an embarrassing hit. Newly elected government leaders worry about whether their results will live up to their campaign promises.

We find that leaders are less confident when they obsess about things they can't control, rather than taking action in the areas they can control.

The *Wall Street Journal* reported the results of a new survey (6/16/2019) by the Conference Board regarding what is on the minds of 800 CEOs.

External Hot-Button Issues

1. Recession
2. Global trade
3. Politics

Internal Hot-Button Issues

1. Attracting and retaining top talent
2. Disruptive technologies
3. Developing the next generation of leaders
- 4.

What this survey says to me is this: it's good to be aware of issues that are outside of your control — recession, global trade, politics. But it's even more brilliant to master the things that are within your control — hiring and retaining top talent, developing digital capabilities and developing the next generation of leaders.

HOW MUCH CONFIDENCE DO YOU HAVE IN YOUR TEAM?

If you have a high degree of confidence in your team, then keep doing what you are doing to hire and develop them.

But if you don't have a high degree of confidence in your team, then you should focus on hiring, developing and retaining more of the right people who fit your strategy — who can achieve the results you seek. How?

There are three ways to build confidence in your team. You can invest the time to master the skills and best practices around hiring, developing and retaining top talent yourself. Or you can engage ghSMART to do it for you. Or, what most of our clients do is engage ghSMART to solve this problem immediately and build your skills in this area for your long-term success. (A quick side note — I'm very proud to report that my colleagues achieved 99% "high" client-reported satisfaction over the past 12 months. So, to go with this confidence theme, I have a very high degree of confidence that my team will help you solve your #1 problem!)

A great way to build confidence in yourself as a leader is to build your confidence in your team. If you are the CEO of a \$1 billion-plus revenue company or have raised at least a \$1 billion fund, please reach out if you would like my team to help you build confidence in your team to deliver the results you want to achieve for customers, employees and shareholders.



Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times best-selling book, *Who: A Method For Hiring*, and the author of the No. 1 Wall Street Journal best seller *Leadocracy: Hiring More Great Leaders (Like You) Into Government*. Geoff co-created the Topgrading brand of talent management. He is the founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in Economics with honors from Northwestern University, and an MA and PhD in Psychology from Claremont Graduate University.

Only 31% of Employees Get
Annual Training on Cyber Security

<https://smallbiztrends.com/2019/09/2019-cyber-security->

**DID YOU
KNOW?**

These Are The Biggest Privacy Threats You Face Online Today

Webcam Access – While it's rare, there are known exploits that allow others to access your webcam (such as malicious software or software security flaws). Putting electrical tape over your webcam isn't a bad idea, but more webcams are coming with kill switches and shutters for peace of mind.

Phishing Scams – Don't ever expect these to go away. People still fall for them. NEVER click links in e-mails from anyone you don't know (and even if you do know them, verify that they sent you a link – e-mail addresses can

be spoofed).

Web Browser Plug-ins – Vet every browser plug-in and extension you install. Many extensions collect your browsing history and sell it. Read the terms of service before you click install (a good rule of thumb for software in general).

Ad Tracking – Web ads (and web ad providers, such as Facebook and Google) are notorious for tracking users. They want to know what you like so they can cater ads directly to you in the hopes that you'll click the ad, which gives them ad revenue. It's one of the many reasons why people use ad blockers.

Device Tracking – If you have a smartphone, chances are it's being used to track your every move. Again, it comes back to delivering ads that are relevant to you so you'll click on them. For companies like Facebook and Google, users are the product. *Inc.*, 7/19/2019

Capitalize On This Strategy To Improve Your Bottom Line

Want to boost your bottom line? The answer may be in cashless payments. It's all about taking your current systems and updating them to current trends.

Outside of the U.S., particularly in Europe and much of Asia, cashless payments are king. More people are relying on smartphones as payment processing tools (both in the consumer and business worlds). Of course, you don't want to rely on cashless – you want to be able to accept any money your customers are spending, whether it's cash, card or electronic.

Look at your point-of-sale system – is it ready for cashless? If not, look into it, research your options, ask around and see what option makes sense for your business (and bottom line). *Small Business Trends*, 6/26/2019

