T. Daniels Consulting

THE T. DANIELS TIMES

Microsoft Partner
Silver Small and Midmarket Cloud Solutions

What's New

October is National Cyber Security Awareness Month

Cybercriminals are very good at getting personal information from unsuspecting victims, and the methods are getting more sophisticated as technology evolves. Protect against cyber threats by learning about security features available on the equipment and software you use.

T. Daniels Consulting's unique multi-factor authentication solution (MFA), **SecureFactor,** reduces network disruptions and data breaches arising from weak or stolen credentials. To learn more about **SecureFactor, call 810-629-0131 or e-mail us at info@tdaniels.com**

October 2019

This monthly publication provided courtesy of Timothy D. Ricketts, President of T. Daniels Consulting.

"Thank you for the confidence you have given our entire team to manage and protect your valuable assets. We take great pride with our goal to exceed your expectations every day!"

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.

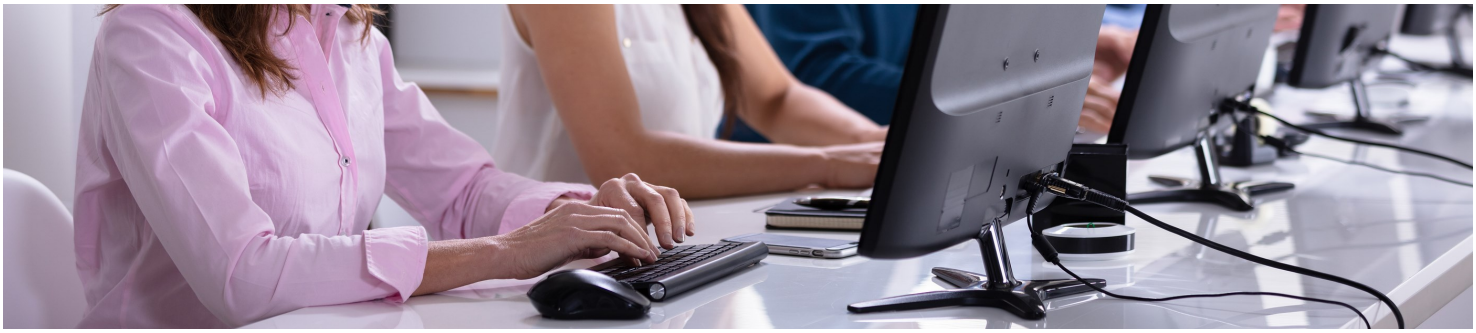
You need to do everything you can to train your employees. Give them the education and resources to be a line of defense rather than a risk. Develop a consistent training regimen. If you need to bring in IT professionals to help, do it. Don't make assumptions about critical IT security training if you 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

Continued on pg.2

Continued from pg.1



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.

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 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.

"It's all about understanding the threats and taking a proactive approach to 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 Cyber Security Audit 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 audit 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,
visit: http://www.tdaniels.com/cyber-security-1019
or call 810-629-0131.

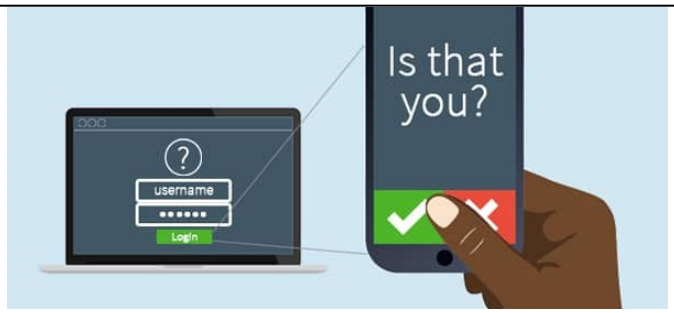
Shiny New Gadget Of The Month:

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.



Top 3 Reasons You Need To Enable Multi-factor Authentication

By: *Tim Ricketts, President*
T. Daniels Consulting

Multi-factor authentication (often referred to as MFA, 2-factor authentication, or 2FA) is an additional layer of security for the user accounts that you use to access applications including your email, client database, accounting software or remote access to corporate data. With little time and effort, it can massively increase the level of security protecting your sensitive data.

It may be that you already encounter MFA in your daily life and just don't know it. Take online banking for example where most institutions send a special code to your mobile phone or require a secondary form of password verification before you can access your account information. Working with MFA on your user accounts is no different and with apps from Microsoft and Google, it is even easier to enable and leverage in order to protect your sensitive corporate data.

Here are the top 3 reasons MFA should be enabled in your business today:

1. MFA is free.

Unbelievable right? Unlike other some other security protocols and applications, as long as the application in question supports MFA (which considering today's threat landscape, most of them do), it won't cost you anything.

Even if you have a legacy, proprietary application, as we know some of you do, there is likely a 3rd party MFA solution you can use (which may or may not have an associated cost) and you should strongly consider MFA because lets' be honest, the older less mainstream applications are already a target for cybercriminals.

2. MFA is super easy to use.

Assuming you have no troubles entering a username and password, you are well equipped to handle MFA. Most of the widely used platforms such as G Suite and Microsoft Office 365 use clever apps installed on your phone such as Google Authenticator and Microsoft Authenticator to help with your MFA access. For example, using the Microsoft Authenticator app to access your Office 365 services (eg: email) simply requires you to logon with your usual username and password, at which point the app on your phone will pop up with a request to confirm access. Simply tap on the app to allow, and your device will then successfully complete the logon process.

3. MFA is a vital layer in your security plan.

Digital security is like an onion – it must have many layers and each layer serves an important purpose. Firewalls and AV protection are as critical as ever, but in many situations, they simply will not offer all of the defense that you need to keep your information secure. MFA is an extremely effective method of protecting access to your user accounts and subsequently the sensitive data your business needs to protect in order to survive. Consider this, what if a hacker were to gain access to your CFO's email account, what do you stand to lose and can you afford to lose it? This is where MFA shines.

So, now that you know why MFA is so important and so easy to implement, the question you need to answer is no longer why should you enable MFA, but *why wouldn't you enable MFA*?

If you don't have a good answer that has been vetted by a security expert, then you need to get MFA setup on your systems today and keep your data safe. Need more info or help on getting MFA enabled for your business, contact us (810) 629-0131 and we will be glad to help.

The T. Daniels Difference

25 YEARS
1994 ~ 2019
T. Daniels Consulting

For over 25 years, T. Daniels Consulting has provided Small and Medium sized organizations with excellent customer service. Our Microsoft Certified Professionals and Engineers have an average 10 years' experience benefiting you by fixing problems quickly and correctly the first time. No other competitor comes close to our level of knowledge, experience and professionalism. We are continuously adding new and improved services to meet your ongoing needs. We never stop improving. That is the **T. Daniels Difference**. Thanks to all of our customers for making us one of Michigan's fastest growing IT consulting and service companies.

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*

Will You Be Able To Meet The Windows 7 January 2020 DEADLINE?

By now, you have likely heard about the upcoming deadline to move your Windows 7 devices to Windows 10 **prior to January 14, 2020.** Perhaps you have even finished the upgrade across your network and if so, congratulations!

However, if you are like 40% of the respondents in a recent Adaptiva survey and have started the process but are unable to complete the project due to the complexity, time, and/or resources required, we can help. Even one device left running Windows 7 after the end of life deadline leaves you **exposed to serious hacker attacks** aimed at taking control of your network, stealing data, crashing your system and inflicting a host of other business-crippling problems you do NOT want to have to deal with.

To learn more about how T. Daniels Consulting can help, simply call us at 810-629-0131 or e-mail us at info@tdaniels.com