DTS DanTech Services
Computers under control!™

Technology Times January 2023 Issue

"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "

What's Inside:

Got IT Problem? - Click Here!

Home Office Safety and Security Week—January 8-14, 2023

Home Office Safety and Security (HOSS) Week occurs in the second full week in January, and is from January 8 to 14 this year. During this week, stay-at-home workers are urged to assess the safety of their work environment. If you work remotely or are looking for such a job, we're using today's observance to highlight certain aspects you might want to consider including in your home office. Take out time to assess your workspace and pinpoint any security vulnerabilities that could jeopardize you or your data.

HOW TO OBSERVE HOME OFFICE SAFETY AND SECURITY WEEK

Take inventory. If you are a remote worker, you can take inventory of your workspace to celebrate HOSS Week. Make sure your list is detailed and remember to keep it handy at all times.

Check your antivirus and firewall protection. Are your system's antivirus and firewall software up to scratch? If not, you should do something about it quickly. Outdated security systems leave you vulnerable to attacks that could jeopardize your work.

Backup your data. Remote workers who work on local files on their computers need to have backups to avoid data loss. It's best to have both physical and cloud backups to ensure that in cases of fire or hacker attacks, your data is still accessible.

- Continued on page 4

NEW YEAR'S RESOLUTIONS TO IMPROVE YOUR CYBERSECURITY

PERFECT YOUR PASSWORD POLICY
Taking a look at your password policies is a perfect cybersecurity New Year's resolution. There is a lot of outdated information concerning password policies. One is recommendation to change passwords frequently. Not anymore. Scrap any policy that enforces frequent and unnecessary password changes. Instead, only enforce password changes when there is suspicion that passwords may be compromised. Focus your attention on promoting the use of long, strong, and unique passwords by using password managers. Top it off with the security measure in our next resolution.

ENFORCE MULTI-FACTOR AUTHENTICATION (MFA) While strong and unique passwords go a long way toward preventing attacks, they aren't foolproof. Make the attacker's job much harder by enforcing multi-factor authentication (MFA) on user accounts. App or token-based MFA methods are best, because SMS authentication is vulnerable to sim-swapping. When all of your users have strong passwords and MFA in place, attackers have to figure out their passwords and obtain their devices in order to circumvent these security controls. Multi-factor authentication adds another layer of security to your sensitive accounts.

REMOVE OLD USERS FROM YOUR SYSTEMS
This cybersecurity New Year's resolution is critical, because active user logins enable access to your systems. Having a large number of old users with valid credentials increases the number of weak points in your organization. An attacker only needs to figure out one set of login details to breach your systems. Unnecessary user accounts give hackers more opportunities to infiltrate your network.

CONDUCT A RISK ASSESSMENT The threat landscape is constantly changing. Most organizations are also in a state of flux, with changes to their systems, structural arrangements, technology and more. A yearly risk assessment is an important cybersecurity New Year's resolution. It gives your company a chance to take stock of all of these changes and analyze the threats to your data security.

QUARTERLY EMPLOYEE TRAINING Your employees have a lot of responsibility and it is easy to forget about critical cyberthreats. This is why it is important to have quarterly employee training. Not only do these sessions provide a good opportunity to remind them of policies, but they also allow you to update them on the latest threats. Your employees are often the first line of defense in a cyberattack.

5 Tips for Online Security in 2023

It's time to revisit your online security practices. Between remote workers logging into networks, to using public wi-fi or other online tools, you need to ensure that your data and information are safe.

This isn't just a lesson for businesses either. While data integrity is vital for companies, it is just as important to keep your personal information safe.

Here are 5 tips for online security in the coming year. And the good news is all of these things are relatively easy – and inexpensive – to do!

1. Connect Devices with Reliable VPN

Secure and connect your devices with a reliable VPN. A virtual private network allows you to extend a private network across a public network in a secure manner. For example, you can access your work computer from a home-based device.

Key benefits of a VPN include:

- Privacy protection to stop snooping ISPs and third-party trackers on all the devices you have
- Secure your identity to hide your IP address and sensitive data you send and receive
- Prevent tracking by companies, hackers, or bots when you are online

VPN services are quite affordable and will give you the peace of mind that you are safe online, wherever you are. When searching for a VPN, look for these features:

- Ability to connect unlimited devices
- 24/7 support
- Independent audit
- Ad blocker
- Two-factor authentication

2. Train Your Team on Safe Surfing

One of the biggest security threats online can be human error. Too often people will click on links that are malicious or harmful.

It's important to conduct annual training to help your team understand these risks, spot warning signs, and stay away from harmful links online.
IBM reported that 23% of all data breaches were a result of human error.

Set a date and talk to your team about the following:

- Why cybersecurity matters and the impact on your company
- How your company will monitor security, such as phishing tests
- How good practices at work can protect individuals, too

- continued on page 3

Shiny New Gadget Of The Month:

Best work-from-home Thunderbolt dock: Kensington SD5500T Thunderbolt 3 and USB-C Docking Station

Laptops are made to be portable, and they excel in that task. When you're spending all day hunkered down in your home office, expanding your laptop's capabilities can not only help you get more done, it can help you feel comfortable—staring at a full-sized monitor and typing away on a proper keyboard does wonders for ergonomics.

That's where a Thunderbolt docking station can pay dividends, despite their high prices.

We've tested a slew of Thunderbolt docks in 2022 and our go-to recommendation is the Kensington SD5500T Thunderbolt 3 and USB-C Docking Station, because of its smart compromises.

It sticks to the tried-and-true Thunderbolt 3 standard and includes a pair of DisplayPort options for external monitor connectivity, which helps keep the price around $260 in a field where most options go for north of $300.

With a smart mix of ports and 60W of laptop charging power, this is the best Thunderbolt dock for anyone living the WFH life.

- "5 Tips for Online Security in 2023"
- continued from page 2

3. Beware of Public Wi-Fi

While public wi-fi is great for accessing the web in a jiffy, it can leave you vulnerable to hackers. So how can you work on the go and protect your information?
If you are going to use public wi-fi, the best option is to connect through a VPN to provide an extra layer of security against hackers. This is just as applicable at a local coffee shop as when you are traveling around the country or abroad.

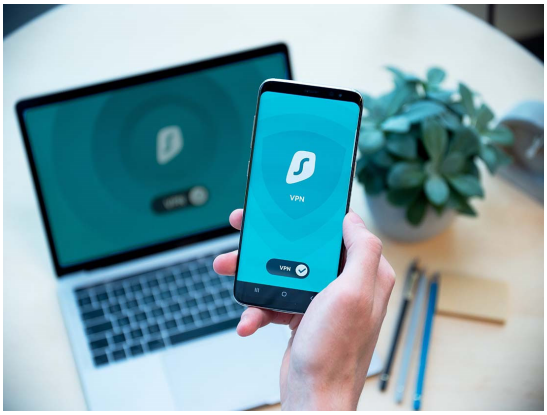
4. Enable Multi-Factor Authentication

Multi-factor authentication (MFA) or two-factor authentication (2FA) can be a simple tip that can save you from a lot of stress. MFA asks you to provide multiple verification methods to access an online account (2FA asks for two methods).

These additional verification steps are often tied to accounts that only you should be able to access to prove your identity when accessing information or tools.

After you enter a username and password, these verification steps may include:

- Answering security questions
- Entering a code that is sent to you via SMS or phone call
- Confirming access with an authenticator app
- Biometric verification, such as a fingerprint, voice, or face scan



Using MFA or 2FA can significantly reduce the risk of a successful hack or cyber attack. Often, MFA or 2FA is combined with other security measures, such as VPN, to make devices and data even more secure.

5. Secure Remote Workers

Remote work has become a reality for most companies. Even if your team works remotely only part of the time, it's important to maintain the same levels of security out of the office as in it.

Requiring remote workers to access networks via a VPN connection is the most effective way to maintain consistent security and protect company information.

If you aren't using VPN for remote access, here's why you need to start:

- Data is encrypted when accessed by employees to circumvent others from gaining access to information
- Keep company data off public wi-fi, which can be open to hackers
- VPN provides an authentication protocol to ensure you know who is on the network and you can control what information they must provide to access it
- It's a highly affordable option and can save your company in the long run (plus it is cheaper than paying mileage for commuters)
- For some employees, you may see increased productivity because they can get a jump start on work or projects from anywhere, when the creative inspiration strikes without worrying about security

New Year Computer Jokes

- Autocorrect can go straight to he'll
- Whoever said that the definition of insanity is doing the same thing over and over again and expecting different results has obviously never had to reboot a computer.
- Did you hear about the monkeys who shared an Amazon account? They were Prime mates.
- Q. What is the biggest lie in the entire universe? A. "I have read and agree to the Terms & Conditions."
- Q. How does a computer get drunk? A. It takes screenshots.
- PATIENT: Doctor, I need your help. I'm addicted to checking my Twitter! DOCTOR: I'm so sorry, I don't follow.
- Person 1: Do you know how to use Outlook? Person 2: As a matter of fact, I Excel at it. Person 1: Was that a Microsoft Office pun? Person 2: Word.
- Q: Why did the computer show up at work late? A: It had a hard drive.
- Anyone who thinks "talk is cheap"... obviously didn't pay my daughter's last mobile phone bill!
- I'm employed at a computer security company and have a colleague whose name is M. Alware. His e-mail address is malware@company.com. - My ex-boss's name is R. Stone. His e-mail was stoner@company.co.in. - My name is James Pan. Every other permutation of my name was taken (e.g., jpan, jamesp), so I'm stuck with japan@university.edu
- I can still remember a time when I knew more than my phone.

- "Home Office Safety and Security Week" - continued from page 1

5 FACTS ABOUT DATA SECURITY THAT WILL BLOW YOUR MIND

1. Bloodthirsty. A University of Maryland Clark School study is among the first to estimate the relentless rate of cyberattacks on systems with web access— an average of 39 seconds.

2. Target practice. According to the HIPAA Journal, in September 2020, over 9.7 million healthcare records were breached in cyberattacks.

3. Mind games. Resisting phishing attacks, according to Cofense, depends on user behavior, and recognizing this is the best approach to protect your company from some of the popular kinds of attacks.

4. The flaw in our stars. Over 95% of cybersecurity attacks are a result of human error.

5. Slow going. The majority of companies will take almost six months to identify

data breaches.

WHY HOME OFFICE SAFETY AND SECURITY WEEK IS IMPORTANT

1. Preventing property damage. It reminds us of the importance of workplace security. Creating a safe workspace is crucial for reducing the risk of damage to property in cases of assault and burglary.

2. Preventing data loss. The week preaches vigilance in issues such as antivirus and firewall software and creating backups for important files. These ideas will help keep data safe from theft and keep work running smoothly.

3. Creating awareness about remote work. The week aims to encourage more businesses to see remote working as a viable option. With safety and security measures put in place and the many benefits of a remote work situation, more businesses will be making the transition to more flexible work conditions.