DTS DanTech Services
Computers under control!™

Technology Times April 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!***

# How to Avoid Phishing Scams

Phishing scams are a type of cyber attack where scammers attempt to trick you into revealing sensitive information such as usernames, passwords, and credit card details. These scams can take many different forms, including emails, text messages, and social media posts. Here are some tips on how to avoid phishing scams:

**Be wary of unsolicited emails**: Be cautious of any email that you weren't expecting, especially if it asks you to click on a link or download an attachment. These emails may be disguised as coming from a legitimate source, such as your bank or a well-known company, but are actually sent by scammers.

**Check the sender's email address**: Scammers may use a fake email address that looks similar to a legitimate one in order to trick you. Always double-check the sender's email address to ensure that it's legitimate.

**Don't click on links or download attachments**: If an email contains a link or attachment, hover over it with your mouse cursor to see where it leads. If you're unsure, don't click on it. Instead, go directly to the website in question by typing the URL into your browser.

**Look for spelling and grammatical errors**: Many phishing scams contain spelling and grammatical errors. Legitimate companies typically have professional communication standards and don't make these types of mistakes.

*- Continued on page 4*

## Slow Computer Problem

One of the most common problems users have with their computer is that it is "running slow." This can be caused by many different things, however, typically it is referring to the time it takes to turn on the PC, open programs, or do just about anything. In some extreme cases, this can even mean input lag from your keyboard to what appears on the screen.

This issue can be incredibly frustrating, because it can affect multiple programs or areas on your computer and seriously reduce productivity. Nine times out of ten, the main reason for general PC slow-down is a lack of—or the improper distribution of—hardware resources. What this means is that specific programs or processes are using too much of your RAM, hard drive, or CPU.

Just running your operating system takes a base number of resources, so if you have a pesky program using too much of your computer, it can struggle to run the OS. This can cause common slowdown issues like input lag. An easy way to see what program is hogging your resources is by using Task Manager. To do this, right -click your taskbar and click Task Manager.

On the top of the Task Manager window, you will see a tab that reads "Performance." You can click this tab to see how much of your computer resources are being used at one time. Suppose these values are at or near 100%. In that case, you can close excess programs as needed until your computer is running comfortably again.

A good rule to remember is to only open programs you are actively using. This ensures your computer is running optimally at all times.

## Tips for Improving Your Social Media Security

Social media offers a convenient way to stay connected with friends and family, share your own updates and life stories, and even learn information quickly from professionals– but it's just as convenient for cybercriminals to get their hands on your private information and use it for their own goals.

Experts offer four tips to help you stay safe while getting the most out of social media.

**Tip #1: Be Selective About Sharing Personal Information**

A seemingly harmless post: "Two more weeks to fun & sun in Hawaii!" presents an open invitation telling a thief when it'll be easiest to break into your home. If you want to share details about your vacations, share them after you return. And the same goes for other places you attend. It won't make a difference to your network of friends to know that the pictures you posted from that fancy restaurant were from last weekend not today.
Even something as seemingly harmless as sharing your contact information on social media can backfire. Hackers have been known to use names, addresses, and phone numbers to open bank accounts or credit cards in someone else's name.

**Tip #2: Be cautious what links you click on**

Don't be too quick to click on a tempting ad, as it may link you to a fake site or contain malware that gets released onto your computer or phone.   Hover your mouse over the ad without clicking on the link to see what address the link will send you to. Sometimes fake sites are advertised that may open up your social media accounts to hackers. Also, once you get to the website, make sure the address is secure by looking for the lock symbol in the address bar.

Or better yet, research a company before clicking an ad. Access the company's site directly, rather than trusting a provided ad to ensure you know where you're going instead of being led blindly.

**Tip #3: Make sure each account has a unique password**

If one account's password is discovered, a hacker may try the same password on many different accounts.  Make your passwords strong with at least 12 characters, including uppercase and lowercase letters, numbers, and special characters, where possible.  By using a Password Manager to generate passwords, you'll be given long, complex passwords that are hard for cybercriminals to guess. And you don't have to remember.  All you need to remember is one main password to access this highly encrypted Password Manager, and it does the rest of the work for you.

**Tip #4: Update your privacy settings regularly**

By changing the settings on your social media accounts often, you control how secure your information is. Some platforms allow you to opt out of personalized ads, turn off data collection and prevent other users from seeing your demographics, among other options.  Privacy settings are crucial as a first line of defense for your online security.  But remember that the companies themselves and hackers may still be able to access your information.

## Shiny New Gadget Of The Month:

### Let's UnMix

Let's Unmix is a fully automatic music source separator.

It separates your music into Vocal, Drums , Bass and other instruments and can be used for Karaoke, DJ, remix, etc.

Separate music into vocals, drums, (percussion), bass and other instruments.

Separated tracks can be saved and exported to other apps such as DAW.

You can control volumes and panning of each track separately for playback and export. Playback speed also can be adjusted

You can cut specific region of the tracks for playback and export by defining the area of the waveform view.

Source music can be imported from Media Library, other apps or cloud  services such as iCloud, DropBox, Google Drive and so forth.

The supported file format as source music are mp3, m4a and wav. The supported output formats are m4a and wav. The optimal sampling rate of the source file is 44.1KHz(CD quality). The sampling rate of output file is always 44.1KHz regardless of the sampling rate of the source file.

## Your Home & Computer Security

Our consistent readers, we thank you, know that we value your security either at work or home. That being a steward of you & your families IT security can save you time, trouble, frustration, and money. Yet protecting your home devices and personal data from cyber threats doesn't have to be expensive. There are many no cost or low-cost IT security solutions that can help you stay safe online. Here are some of the best options:

**Antivirus & anti-malware software:** One of the most important things you can do to protect your devices from malware is to install antivirus software. There are many free antivirus programs available, such as Avast Free Antivirus, AVG AntiVirus Free, and Windows Defender. Malwarebytes Anti-malware has a free version as well. These programs provide basic protection against malware and can help keep your devices safe. While we continue to recommend paid versions, such as Webroot & Malwarebytes, something is better than nothing.

**Firewall:** A firewall is a network security system that monitors and controls incoming and outgoing network traffic. Most operating systems come with a built-in firewall that you can enable for free. For example, Windows Firewall is included in all versions of Windows and can be easily configured to provide basic protection against network attacks.

**Two-factor authentication:** Many online services offer two-factor authentication, which adds an extra layer of security to your accounts by requiring a second form of identification, such as a security code or fingerprint. This can help prevent unauthorized access to your accounts and protect your personal information. Two-factor authentication is typically free to use and can be enabled in your account settings. Consider Twilio's Authy.

**Backups:** Regularly backing up your data is an important part of IT security. This can help protect against data loss due to malware or hardware failure. There are many free or low-cost backup solutions available, such as Google Drive, Dropbox, and OneDrive. These cloud-based services allow you to store your backups online, making them accessible from any device with an internet connection.

**Password manager:** Using a password manager can help you create and manage strong, unique passwords for all of your online accounts. Many password managers offer a free version with basic features, such as Bitwarden. These programs can help you generate strong passwords, store them securely, and automatically fill them in when you log in to your accounts.

**VPN:** A virtual private network (VPN) is a tool that can help protect your online privacy and security by encrypting your internet traffic and masking your IP address. While some VPNs can be expensive, there are many free or low-cost options available, such as ProtonVPN and Windscribe. These programs can help protect your online activity from prying eyes and keep your personal information safe.

In conclusion, there are many no cost or low-cost IT security solutions that can help you stay safe online. From antivirus software to backups and VPNs, there are many tools available to help protect your devices and personal data from cyber threats. By taking advantage of these solutions and staying informed about the latest threats and best practices for staying safe online, you can help protect your digital identity and enjoy a safer, more secure online experience.

Dan Foote

## Microsoft Patch Tuesday

Microsoft released on March 14, 2023, a security update that fixes at least 74 bugs in Windows and other software. Hackers are already attacking two flaws, including a very serious one in Microsoft Outlook. Microsoft said that threat actors are taking advantage of this bug. It starts working automatically when a malicious email goes to an email server, even before it appears in the Preview Pane.

The flaw makes it possible for a threat actor to pose as a trustworthy person. This is the same as an attacker having a valid password and getting into an organization's systems.

### Action Plan for Business Owners

Windows is a staple in many businesses. Owners should take the following precautions to protect their clients and make sure their systems are safe:

- Install security updates quickly. Once there's a new patch, you should update you software to stop exploitation.
- Establish a regular update schedule. Check for and apply updates for your operating system, apps, and security programs on a regular basis.
- Get people to use strong passwords. Encourage employees to use strong, unique passwords and consider using a password manager.
- Enable multi-factor authentication. This provides an added layer of security.
- Always have a backup plan. Back up your data regularly and keep it in several places for quick recovery.
- Monitor network activity. Use tools for network monitoring to find strange behavior and possible threats.
- Develop an incident response plan. Plan for handling cybersecurity issues, including ways to deal with threats. Review policies on security. Regularly review and update security policies to adapt to new threats and technology.

*"How to Avoid Phishing Scams"*
*- continued from page 1*

**Check the website's URL**: Phishing scams may direct you to a fake website that looks like the real thing. Always check the URL to ensure that you're on the correct website. Look for the "https" in the URL, which indicates that the website is secure.

**Be cautious of urgent requests**: Scammers may try to create a sense of urgency in order to get you to act quickly. For example, they may claim that there's a problem with your account that needs immediate attention. Always take a moment to verify the legitimacy of the request before taking any action.

**Keep your software up to date**: Scammers may exploit vulnerabilities in your software to gain access to your computer or device. Make sure to regularly update your operating system and software to protect against these types of attacks.
In conclusion, phishing scams are a common type of cyber attack that can be difficult to spot. By following these tips, you can help protect yourself from these types of scams and keep your personal information safe. Always be cautious of unsolicited emails, check the sender's email address, and don't click on links or download attachments from untrusted sources. By staying vigilant and keeping your software up to date, you can help protect yourself from phishing scams and other types of cyber attacks.

## Do you know that DanTech Services helps its customers in websites support and design?