P.O. Box 95
Pine Grove Mills, PA 16868
814-206-0000
814-207-4323
mas@tekresults.com
www.tekresults.com

TekResults Newsletter (April 2022)

To unsubscribe send an email to UnsubscribeNewsletter@tekresults.com with unsubscribe to Newsletter in the subject line or click here UnsubscribeNewsletter@tekresults.com

Dear Clients and Friends

It looks like Spring has finally arrived in Central PA. It is the end of April, and the leaves on the trees are still in shock from all the cold weather, but they're finally peeking out and hesitantly proclaiming winter is over. Break out the grill, dust off your softball glove and go shopping for a new swimming suit. While you're thinking of warmer things, we'll dive into this issue of our newsletter.

This issue is all about security. We know that's not a particularly exciting topic, but we'll make it worth your while by keeping things on point and brief. We also have some important announcements, so you'll want to be sure to read to the end. With that said, here's this month's newsletter!

Referrals

TekResults owes much of its success to our loyal and enthusiastic clients. It's those of you who tell your friends about us that keep our company growing, and we'd like to say thanks. Just telling someone about us is all it takes. Just let us know you dropped our name and we'll drop a gift card in the mail. See, who said talk is cheap!

Businesses Who Need Our Referrals
Any business who has slow computer systems
Any business who has slow network
Any business needing a better disaster recovery strategy including backups for mission-critical devices (servers, essential PCs, etc.), equipment redundancy,
Any business requiring help upgrading existing IT infrastructure due to obsolescence
Any business that needs better email services
Any business that needs to migrate to a new software platform
Any business that needs help with its industry vertical market software
Any business that has employees and compliance questions
Any business that needs help with employees working from home
Any business that needs reliable IT service
Any business that is purchasing another business and needs IT help
Any business that is being sold or is being dissolved
Any business with human resource issues as they pertain to IT
Any business that wants to save money and improve functionality by utilizing a VoIP Business phone systems
Any business needing a better security infrastructure

Any business needing remote desktop applications
Any business needing help migrating to Microsoft 365
Any business that would benefit from monitoring of performance, security, etc. of their IT infrastructure
Any business that would like an IT department that will visit and report on each device on a scheduled basis
Any business that would like to read our newsletter or other mail tips and blasts

Is your technology secure?

Most people outside the tech world don't lie away nights wondering if their computers and other technology is safe from attack, but we would all benefit from giving this a little more thought. The old saying "The wolf is always at the door" has never been truer than today, when the "wolves" don't even have to come to your door - they can get you from an Internet café from on other side of the world. In this article we provide some time-tested tips for shoring up your defenses.

Keep your software up to date

We're going to talk about your Windows operating system here, but the lesson applies to all your technology including mobile devices, home security systems, even car computers. We'll talk about Microsoft because they are the most coveted prize in the entire bad-guy universe. Microsoft reports there are more than 1.4 billion monthly active devices running Windows 10 or Windows 11. That makes Windows a huge target. There are many whose life work it is to spend day after day trying to find weaknesses in Windows they can exploit for their own gains.

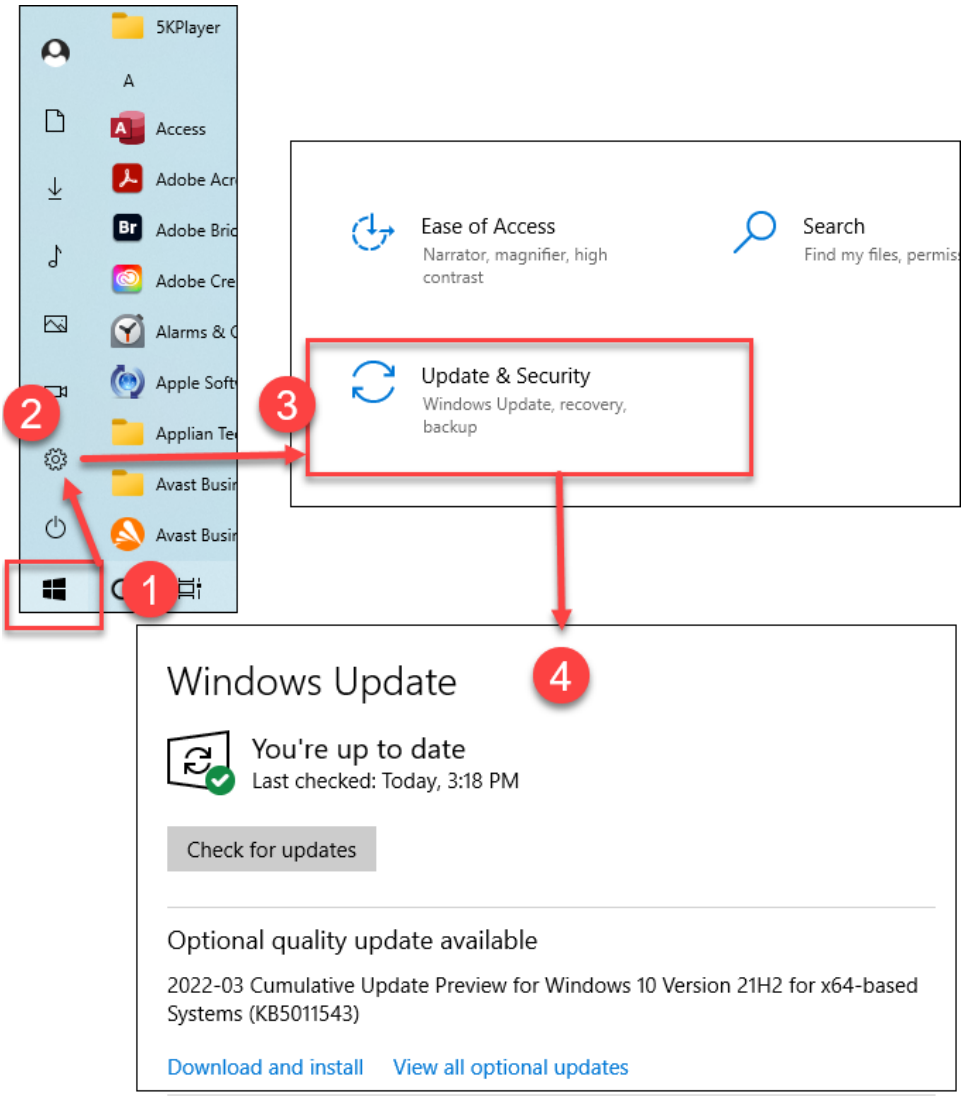
As users, we depend on Microsoft to remain vigilant and to fix security weaknesses when they are discovered. This is one of the chief reasons Windows performs updates. Windows is ever-evolving, Microsoft is steadfastly patching security breaches and preventing malware infections. Security patches, bug fixes, and new features are often included in software updates.

Unless someone has changed the settings in Windows, updates will occur automatically, but this is not always true of other software. Your apps normally will let you know if there is an update available. but you have to give the go ahead for the update. It's a good idea to do this for the same reasons you do Windows updates. iPhones, iPads, Androids, Google devices, Adobe products, QuickBooks, Sage, all the apps that run on your computer are vulnerable to the same bad guys that try to subvert Windows, and your first line of defense is keeping your software up to date.

How to check if Windows is up to date

It's easy to check for updates in Windows 10 and 11.

1. Click the **Start** button.
2. Click the **Settings** cog.
3. Click **Update & Security.**
4. View your update status.



What is firmware and why do I need to update it

As we just discussed, it's important to keep our smartphones, laptops and other connected devices updated with the latest version of the operating system. But what about the Wi-Fi router that's been sitting on the shelf untouched for the last couple of years? Does it need updating, too? The answer is yes, of course! The software that runs on your Wi-Fi router is known as "firmware", and even if your home Wi-Fi seems to be working well, regularly updating the firmware on your router is extremely important.

Firmware is the software that comes preinstalled on a device. Every router manufacturer has its own version of this software; so does your printer and your home alarm system. Anything that is automated will normally have firmware. And, like the operating systems that run on your smart phone or your personal computer, firmware controls all the inner workings of the device. For example, it's the firmware that makes it possible for your router to communicate wirelessly with your devices; it helps protect your network from malware, viruses and other threats; and it provides the administration software that you use to manage your router's settings.

When a manufacturer makes improvements to the way a device operates, or develops security patches, those improvements are usually rolled up into a downloadable software package, a file called a firmware update. Updating firmware usually requires a little tech savvy and some direction from the device's manual (online manuals are fine), but the general process is this.

1. On your computer, download the most recent firmware file from the manufacturer's website.

2. Open a web browser on your computer and type the device's IP address in the address bar. This assumes your device is connected to your network and you know the device's IP address.
3. Once you are on the device's web interface, you should be able to find an option to update firmware. There will be an upload button you can use to upload the firmware you obtained in the first step.

Although it would be best to read your device's manual for exact instructions, here is a good article that provides some general steps. While firmware updates are not as intuitive as operating system (OS) updates, they are still important. If you need help, TekResults will be happy to assess your devices and perform the necessary updates. Give us a call at 814-206-0000.
Also, it is strongly advised that you make a backup of your device's settings etc. before you attempt a firmware upgrade and you may want to talk to us about making sure that if you "brick" the device that we can get you up and running quickly with a replacement.

Invest in a good antivirus program

While keeping your Windows operating system up to date helps prevent weaknesses in the software from being exploited, most systems that are infected with viruses or malware get that way through some sort of user interaction:

- Sharing music, files, or photos with other users.
- Visiting an infected website.
- Opening spam email or an email attachment.
- Downloading free games, toolbars, media players and other system utilities.
- Installing mainstream software applications without thoroughly reading license agreements.

Viruses are still a huge problem in 2022. But it isn't only viruses you should be worried about. Criminals want your personal information - your identity, your bank and credit card numbers - so they can take your money.

And they're doing this in ever more elaborate ways, from fake apps (with download links often shared on social media) to fake websites that look like real ones but steal your login details and personal information.

Modern 'antivirus' software does a lot more than block and remove viruses. Many packages now include a VPN service to give you extra security and privacy while you browse the web, and warn you if malware is trying to access your device's camera and microphones. They also include password managers which remember all your logins so you can have different passwords for all your accounts.

Is Windows defender good enough?

Windows 10 and Windows 11 come with built-in antivirus protection called Windows Defender (AKA Microsoft Defender Antivirus). In past years, this program offered only the most basic protection, and many thought it little more than a joke. However, Microsoft has been making steady progress in making Windows Defender a legitimate tool. In 2022 it now has a solid reputation as being very good protection. But is it enough? Well, that depends.

The catch is that in order to get the best protection from Windows' built-in security tools and features, you have to stick to Microsoft products. So that means using Edge instead of Chrome or Firefox as your default browser, Microsoft Office 365 instead of Google Workspace or LibreOffice, and Microsoft Teams instead of Slack or Zoom.

As a result, if your Chrome or Firefox browser stumbles across a malicious website, you'll have to rely upon the browser's own protection, not Microsoft's. (To be fair, the protections on Chrome and Firefox are pretty good on their own.)

Microsoft does have browser extensions for Chrome and Firefox, but they're limited to machines running the Pro, Enterprise or Education versions of Windows 10 and Windows 11.

For the parental controls to work properly, your kids have to use Edge, and no other browser, on Windows. You can also put Microsoft Family Safety apps on your kids' Android and iOS devices, but that requires a paid subscription to Microsoft Office 365.

Does my Mac need antivirus?

Most antivirus experts agree that while Apple's security software is fairly good, it's not foolproof. XProtect (Mac's built-in antivirus program) does not identify as many types of potential malware as third-party antivirus software, and gaps in its library of malicious programs can leave users exposed. Part of the problem is that the software relies heavily on Apple identifying and tagging malware and viruses, and since Apple isn't a dedicated security company, it doesn't keep track of nearly as many threats as third-party products.

If you're willing to pay for the best security (and why wouldn't you?), TekResults partners with Avast to provide exceptional protection for our corporate clients, using Avast Business CloudCare. Because businesses have so much at stake, we highly recommend not leaving your protection to Windows Defender. Give us a call to discuss your specific needs at 814-206-0000.

Change your passwords

Your computers carry a lot of sensitive and important data, so keeping work data safe is a major priority. One security tip for computer users is to constantly change your passwords to something new, but it may not always be clear why you have to do something this inconvenient so consistently. Changing your password avoids a number of dangers -- including some that are less obvious, such as what happens to the passwords you have saved on computers you no longer own.

Limit Multiple Account Breaches

It can be tempting to use the same password on every account you have, whether for computers and network equipment or online accounts, as it's much easier to remember one. However, it also means that if someone figures out your password, he can gain access to every account you have. Changing your passwords to something different and unique to each account will make it so that even if someone does guess one password, he cannot use it for anything else.

Prevent Constant Access

Not all hackers take what they need and leave. Occasionally hackers may continue accessing your account, either to monitor your data or continue stealing information over time. It can be difficult to figure out if someone else is using your account, so by changing your password consistently, you reduce the risk that other people will have frequent access to your accounts. Consider changing your password every few months to be on the safe side.

Limit Guesswork

If you use the same password for long stretches of time, you increase the risk of someone guessing your password. Whether it's from someone watching you type in your password a number of times or someone repeatedly trying to guess it, the longer you have the same password, the longer people have to try to find out what it is. Don't let people watch you log in to your accounts, and avoid using short, easy-to-guess words or phrases.

Prevent Saved Password Abuse

If you ever switch computers with other people, or if you get rid of old computers without reformatting the hard drive, it's possible that anyone who uses your old computer will have access to your saved passwords. Giving someone a computer with saved passwords is like giving them access to your accounts. Consistently changing your passwords will mean that even if someone has found an old password of yours, it will no longer be relevant or useful.

Choosing a Good Password

When coming up with a new password, you want something that can be safe from guesswork and hacking attempts. You may be tempted to use a long password, but quality is much more important than quantity. Hacking programs are capable of guessing passwords by combining random words and phrases together, as well as any information relevant to you. To combat this, avoid using any personal information such as dates, addresses or names. Also avoid using simple words and phrases; if you do, make them grammatically incorrect to avoid guessing. Use random combinations of numbers, letters and symbols that can still be easy to remember. For example, instead of "password" -- which should never be used under any circumstance -- you could use "p4$$w0rD." It is still the same word, and still short, but far harder to guess either by human or program.

How to remember all those passwords

It's getting more and more difficult to keep up with all the passwords required to live in a web-based society. Gone are the days when you could use your dog's name or your childhood nickname to access your online banking or email. Today most website security policies require your passwords to contain a combination of capital and lower-case letters, special characters and numbers, and to use a specified number of characters. To make it worse, some of them also require you to change those passwords every couple of months and they won't let you use a password you've used in the past! The result is multiple, unrememberable passwords. And if you can't remember them, you must write them down. And if you write them down, they can be lost or stolen.

Much to our horror, some of our clients keep their passwords in a notebook next to their computers; some even have them on a paper, taped to their office wall. It seems the very security the password requirements are trying to implement are defeated by the complexity they impose. Fortunately, there's a relatively easy way to deal with this: Use a password manager.

A password manager (PM) is an app that allows you to store the URL (website address), username and passwords for all the sites for which you have accounts. They are a low cost, in some cases free, solution that offer these benefits

- Encrypted, safe storage for all your passwords
- The ability to use long, complex, secure passwords for all your sensitive sites – none of which you need to remember
- A management system that stores all those passwords allowing you to manage the system with a single password or phrase
- The option to automatically fill in the required usernames and passwords for sites you visit
- Initiate password resets automatically (for most of the more popular sites).

How much work is it to set this up?

This is the question most of us think first. Our days are all busy, and most days we are juggling 6 balls at a time; the last thing we need is another ball. The answer is: it depends.

The time it takes to set up a PM will be determined by the number of passwords you need to manage and by your level of expertise in doing password resets. If you only have a handful of passwords, you can expect to be done with the whole setup in an hour. If you have 50 passwords, it can take several hours.

Our recommendation

There are lots of reviews of password managers on the Internet, and from our experience, the most popular all have similar features and will get the job done for you. PC Magazine offers a roundup of the Best Password Managers for 2022, if you'd like to compare features. We like and have used LastPass Premium. Its ease of use, web-based password vault and its low cost ($3 a month paid annually) make it an easy favorite. Note, there is a free version available, but recent changes have made free LastPass less than desirable. You can read PC Magazine's review here.

Keep your backups up to date

If your hard drive crashes or you catch a ransomware virus, the only thing standing between you and lots of pain is a backup. At some point, all hard drives fail; maybe not tomorrow, maybe not next year, but someday. If you don't have a backup of your valuable documents and pictures, they will be lost when that day comes.

Document backups

Document backups back up anything in your Documents and Pictures folders. You can also specify additional folders if you are storing files somewhere else. This kind of backup is not designed to back up your programs (apps) or the state of your computer. If your hard drive dies, a Document backup will not help you restore the computer to health, however your *documents* can be safely restored to a repaired or replaced computer. Unfortunately, you will have to reinstall your apps – unless you have an image backup.

Image backups

In addition to the files, photos, movies, and videos you store on your computer, you also have other important data stored there too. This includes your operating system, applications, browser history, preferences, settings, bookmarks, device drivers, etc. If you lose these files, worst case is that your computer will not start. Best case is that you will spend time re-creating information.

With disk image backups, the software takes an image of the entire hard disk. This lets you restore the entire system to another computer, including the operating system, applications, browser history, preferences, settings, bookmarks, device drivers, and all the files you have created or downloaded. Image backups let you restore the whole system and get back to a previous state fast.

An image backup will only restore your documents and pictures to the state they were in when you made the backup, so if you have added additional files since then (of course you have!) they will be lost if you are not also backing up your documents.

We STONGLY recommend you create an image backup of all mission-critical systems. Explanation: if your business will grind to a halt when a specific computer goes down, that system is mission critical. It is required to keep your business running.

What we recommend

Document backup

For Document backups we recommend Microsoft OneDrive. With OneDrive, you can sync files between your computer and the cloud, so you can get to your files from anywhere - your computer, your mobile device, and even through the OneDrive website at OneDrive.com. If you add, change, or delete a file or folder in your OneDrive folder, the file or folder is added, changed, or deleted on the OneDrive website and vice versa. You can work with your synced files directly in File Explorer and access your files even when you're offline. Whenever you're online, any changes that you or others make will sync automatically. Here is an article (with video!) that explains how OneDrive can back up your Desktop, Documents and Pictures. Note: you will need **one** of these two things:

- A Microsoft account- If you don't have a Microsoft account, click the Create a Microsoft account link here. This provides 5GB OneDrive storage. Microsoft accounts are free.
- A Microsoft 365 subscription – This provides 1TB OneDrive storage. Not free, but there are many plans to choose from. Home users should look at Microsoft 365 Family (allows 6 users for $9.99 a month) or Microsoft 365 Personal (1 user for $6.99 a month). Business users have more options. TekResults sells Microsoft 365 business plans and we can help you find the right fit for your business. Give us a call to discuss your options.
-

One of the great things about using OneDrive to back up your documents is that you don't have to do anything after the initial setup. Changes you make or add to your docs back up automatically. Set it and forget it!
We understand the many Microsoft options can be confusing, but we are experts at negotiating these waters and will be happy to help you find the right plan. Give us a call at 814-206-0000 to get started.

Image backup

For image backups, we recommend Macrium Reflect Free for personal use, and
Macrium Reflect Workstation for business use: $75 one-time purchase – Support is free for 1 year, after that you have to pay to renew the optional support contract.

These two versions are essentially the same, but there are more restrictions on the free edition, and Macrium forbids the use of the free edition in a business environment, so if you're backing up a mission-critical computer at work, you'll need to cough up the cash. For server backups we recommend, and use, Macrium Server.

All editions of Macrium software allow you to schedule regular backups and to easily check to make sure those backups have run successfully. Once you create the backup schedule, Macrium will happily back up your system without you having to do another thing, although you should check the Macrium log once a week to make sure your backups are completing as expected.

Is your hard drive encrypted?

If your computer is lost or stolen, it's worth knowing that your username and password provide scant protection against a determined hacker trying to access your files. IT professionals and bad guys alike can break into a computer in less than five minutes using a Windows installation CD or some other specialized tool.

Laptop users are a special, high-risk group because their computers are typically on the go and vulnerable to loss and theft. It's much easier to snatch a laptop off a commuter bus seat than it is to break into an office and steal someone's desktop.

High-risk users can take some comfort in knowing that there is a feature built into Windows that allows them to encrypt their hard drive so that, even if the device is lost or stolen, unauthorized access will become nearly impossible.

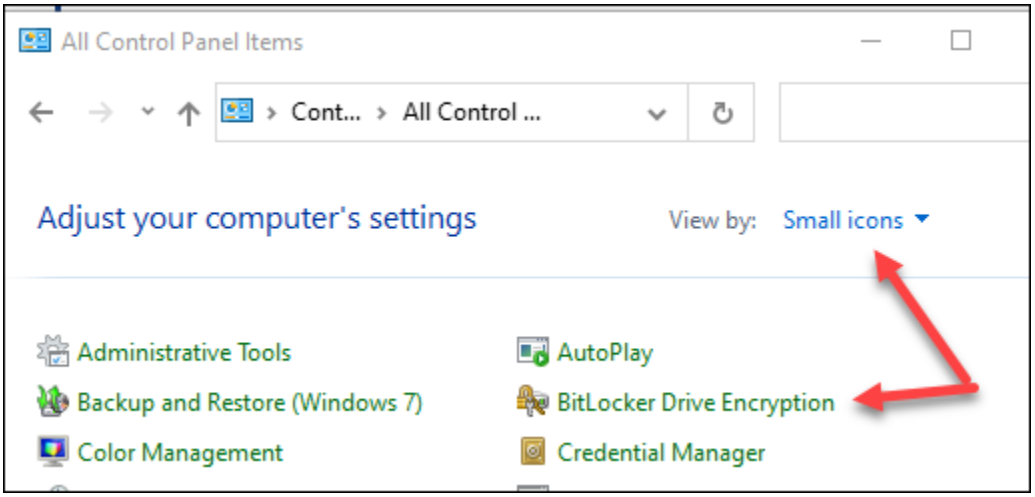
BitLocker is Microsoft's easy-to-use, proprietary encryption program for Windows that can encrypt your entire drive as well as help protect against unauthorized changes to your system such as firmware-level malware. Before you rush to find out how to enable Bitlocker, however, there are a couple things you should know.

- Bitlocker is easy to enable if you are logged into your computer with an administrator account.
- Bitlocker is easy to disable if you are logged into your computer with an administrator account.
- If you ever forget your username and password (used to log into your computer) and there is no other administrator account that can be used to log in, you're out of luck, because an encrypted hard drive cannot be broken into. Say goodbye to your files.
- If your user profile becomes corrupt and repairs must be completed on your hard drive, Bitlocker will need to be disabled first. This requires the use of a recovery key. Bitlocker generates a one-of-a-kind recovery key when it is enabled. It is up to the user to write it down and keep it in a remembered location against such an eventuality. If the key gets lost, there is no other way to disable the encryption. Microsoft can't even help with this.
- Your BitLocker recovery key is a unique 48-digit numerical password that can be used to unlock your system if BitLocker is otherwise unable to confirm for certain that the attempt to access the system drive is authorized.

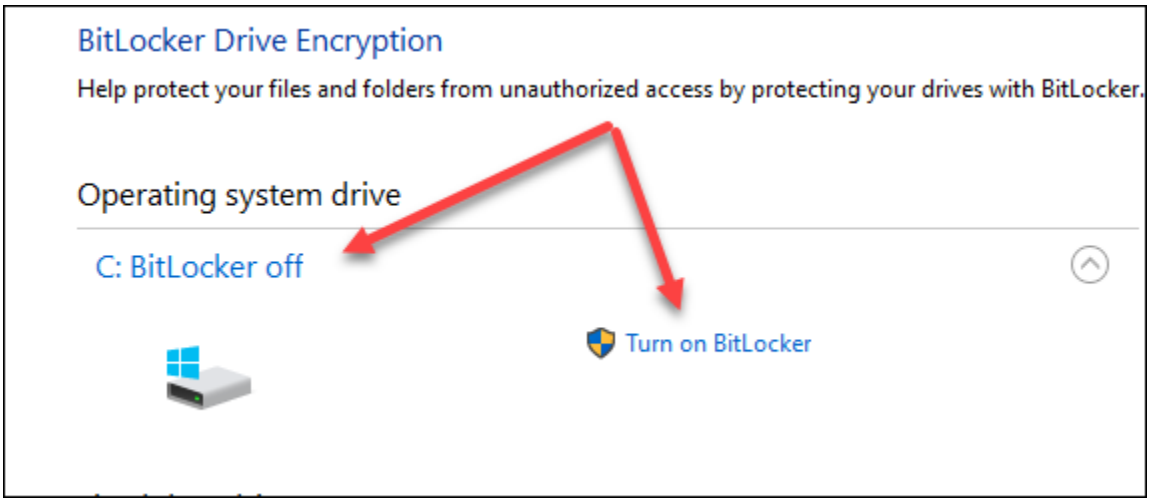
So, encryption can be a great protection tool, but it can lead to disaster if you forget where you put your recovery key. Here's what we recommend.

First, determine if Bitlocker is enabled on your computer.

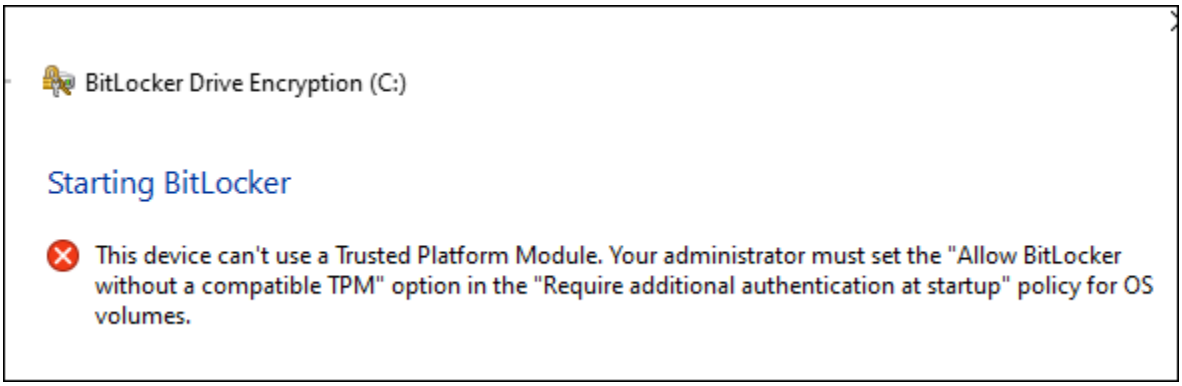
1. Sign into your computer with an administrator account.
2. Open the Control Panel and view the list by **Small icons**.
3. Open **Bitlocker Drive Encryption**.



In the Bitlocker Drive Encryption window, you can clearly see your status, and even turn Bitlocker on if your device meets the Bitlocker requirements.



If your computer does not meet the minimum requirements for Bitlocker, you may see this message.



4. If Bitlocker is turned on, determine if you know the location of the recovery key. Hopefully, you wrote it down at the time Bitlocker was enabled.
5. If you don't have the recovery key, turn Bitlocker off (from the Control Panel shown above). It may take some time for Bitlocker to remove the encryption from your hard drive, so don't be in a hurry.
6. If you want to turn Bitlocker back on, you may do so, but write down the recovery key this time!

Something else to note: if you are logging into your computer with a Microsoft account (this would be in the form of an email address), the new recovery key will automatically be saved to your Microsoft account and can be accessed by logging into Office.com with your Microsoft credentials. If you are logging in with a local or domain account (username and password instead of an email address), you are not afforded that luxury.

The bottom line

Encryption is good, but only if you know where your recovery key is.
If you have Bitlocker turned on and you don't know where the key is, turn Bitlocker off and, if after the disk is decrypted, you would like to turn Bitlocker back on again, write down the key.

When TekResults sets up a computer for a client, we never turn Bitlocker on. We feel it is up to the client to make the decision to encrypt their device and up the client to keep the recovery key safe. Many times we are unable to do any repairs on a system with an encrypted drive, and if the recovery key is lost, there's little we can do.

Changes at Google mean Outlook may no longer work with Gmail

Google has announced that after May 30, 2022 Google will no longer support the use of third-party apps or devices which ask you to sign into your Google Account using only your username and password. These include Outlook.

- If you do not open Outlook to get your Gmail, this announcement does not affect you.
- If you only go online to get your Gmail, this announcement does not affect you.
- You will be affected if you are one of the many users who have Outlook or another email client, such as Thunderbird, configured to send and receive your Gmail.
- This article will focus on Microsoft Outlook, however if you use an email client such as Thunderbird you will also be affected and should look for a solution (we can help).
- According to this post, Outlook 2016, Outlook 2019 and Outlook for Office 365 may not need an app password as described below (but will still require 2-Step Verification).
- For Outlook 2013 and previous versions, you'll need to use an App-Specific Password which you can create on the Google Account website.

On April 13, we sent out a news blast to our mailing list recipients that covers these changes in detail and outlines what you can do if you are affected. If you missed the email, you can read the entire article here.

TekResults and your home network

When the Covid pandemic hit everyone in March 2020, TekResults scrambled to help our clients work from home. This provided many challenges, because everybody's home network is different, and we have no control over the service in people's homes. Still, we did the best we could and got everybody up and running. And, although it's not our policy to include home networks in our preventative maintenance plans, emergencies require emergency action, and the beginning of a pandemic is no time to squabble over what is supported and what is not. We helped everyone one who asked, with no regard for whether their homes were part of their employer's PM plan.

Now it's April 2022 and things are slowly returning to normal as home workers return to their offices. With the emergency behind us, we felt this would be a good time to remind everyone that home networks and personally owned computers are not covered under any of our PM plans, and while happy to assist with issues, we will have to look at new home issues on a one-by-one basis; our regular hourly rate for support may apply. Thanks for understanding.

KnowBe4
Human error. Conquered.

KnowBe4 Second Chance

Many of our clients have showed an interest in working with KnowBe4 to provide online security training for their staff but were unable to do because their small number of associates did not meet KnowBe4's 25-person minimum requirement. We were disappointed to hear this because we know how valuable this training is, so we asked KnowBe4 if there was any way we could work around that requirement. As it turns out, there is! Those 25 people don't have to be part of the same company, and if we can gather enough interest from several clients to band together under a Knowbe4-TekResults umbrella, KnowBe4 will offer the training.

So, this is your chance. If you'd like to participate, let us know. If there is enough interest, we can get the training moving!

Want to read more about KnowBe4? Check out page 10 of our March 2021 newsletter here, or just visit KnowBe4's website.

Who We Are

TekResults is an independent company and will help you find the best solution at the lowest price. We have many years' experience finding the most cost-effective solutions to IT problems and opportunities.

We are a Microsoft technology partner but also have expertise in non-Microsoft software, Unix and other platforms. We can provide services in computer hardware, network, communications, third party software and we can create customized software for you.

We have a proven ability to work in all aspects of the systems development and implementation lifecycle and we are experts at organizing, planning, and creating cost effective solutions. Whether you want system upgrades, installation or complex programming projects, customer satisfaction with every project is the absolute commitment of TekResults. We believe this is essential for the long-term success of our client partnerships.

We are members of Centre County Bureau of Business and Industry, The Centre County Information Technology Consortium and the Association of Information Technology Professionals.

With offices located in State College and Altoona we are strategically placed to service clients throughout central PA.

We are Your Complete IT Partner.

Our Services and Products

- IT problem solving
- Office 365 sales and support
- Business phone systems (Comcast, VoIPLy, Vonage, Fortinet)
- Infrastructure design and implementation
- Pre-Sales consulting
- Capacity planning/ system design
- Network cabling
- Security compliance review HIPAA
- Security compliance review PCI
- System installations
- System upgrades
- System auditing / documentation
- Desktop, laptop and monitor and other sales
- Network administration
- Network troubleshooting
- Business consulting software testing and service
- 3rd party software setup and support
- Computer security solutions (including PGP, encrypted mail, secured transactions)
- Custom application development
- Legacy system migration and rewrites
- System integration
- Application integration
- Network installation and integration
- Training and staff development