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

TekResults Newsletter (December 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

As we bring 2022 to a close, the new year looks more promising than the previous 2 years. Businesses are open again; theaters are doing a brisk business and restaurants are coming back to life. As Barry Manilow said, “Looks like we made it”. At least, we want to think so.

In this edition of the newsletter, we will discuss some ways you can help keep your email from being hacked and then wade into how to speed up searches in Windows, using indexing. For Mac users, we have a preview of MacOS 13, Ventura. For Windows users, we’ll offer some reasons to upgrade to Windows 11 (and a couple reasons you shouldn’t). And finally, we’ll show you how to back up your personal documents in OneDrive so they are available from any computer you may use. Sounds like fun! Let’s get started!

Computer sale!

With Windows 10 quickly approaching the end of its supported life, now is an excellent time to replace those aging computers. We have many desktops and laptops in stock to help make your holidays bright! We specialize in refurbished Dell systems that look great and come nicely appointed with a solid state drive, at least 16GB memory and an Intel Core i5 or i7 processor. We bench test each of our systems to ensure they are working in top-notch order before presenting them for sale, and each one comes with our 30-day warranty. Most of our systems feature Windows 11 Pro, but we still have a few Windows 10 systems in stock – priced to sell. Drop us a line and we can help you find just the right system to put under your tree.

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

But I didn't send that email!

In the past year we've seen an alarming increase in the number of times we've heard this declaration. A client calls us to say that someone has been sending emails out, pretending to be our client. The client got a call from someone they know, asking if the invoice (request for a donation/request to resend account info, etc.) they just received was legitimate. Of course, the next thing the client wants to know is "Have I been hacked".

Hacked vs Spoofed

These two terms sound like they can be used interchangeably, but they are two different things. They get confused because both are unsolicited and are usually part of a bulk email campaign, commonly known as spam. Email spam, also known as junk email, refers to unsolicited email messages, usually sent in bulk to a large list of recipients.

- Spoofed is when someone pretends to be you and sends out emails using your email address in the FROM part of the email. This does not require the spoofer to gain access to your email account. Anyone can pretend to be anyone with a little effort.
- Hacked is when someone has obtained your password and signed into your email server as you, which enables them to send out emails that really do come from your account. This is the more serious of the two. Once someone gains access to your account, they normally don't stop at sending a thousand spam messages from the account, they usually always create an email rule that delivers all new incoming messages to the deleted items or RSS folder, where you won't look for them. If you happen to be a global administrator for the email's domain, the bad guy can also wreak havoc on all the other users in the domain (change their passwords, delete their accounts, send spam out from their accounts, read their sensitive email, etc.).

How to prevent being hacked

Prevention from someone gaining access to your account is simple. Have your email administrator enable multifactor authentication (MFA) for your account. With MFA enabled, each time there is a sign in on a new device, the email server sends out an authentication code to your phone and you must enter the code into your device to gain access. This process is very effective at keeping your account from being compromised. If you are an email administrator, it is even more important that you do this! By the way, you will sometimes see multifactor authentication referred to as two-factor authentication (2FA). MFA and 2FA are the same thing.

How to prevent being spoofed

To prevent being spoofed, an email needs a way to prove that it came from whom it says it did. If the email can't prove its pedigree, it either gets sent to the spam folder or just plain ole doesn't get delivered. The technology that makes this

happen is called **DKIM**. DKIM must be set up at the domain level and therefore will require an email administrator to make it happen. Once it's in place, DKIM protects all email accounts in the domain.

DKIM is an email authentication protocol that the mail servers on the receiving end of your messages can use to verify you are the true sender of a message. It ensures that nobody has used your domain or other identifiers to impersonate you or your company. DKIM has become an authentication standard in the email world. A message sent without DKIM and/or SPF can be considered suspicious by the receiving email servers.

Why is DKIM important?

DKIM provides protection for the reputation of your organization as well as the integrity of its email program. It offers domain protection against phishing and "spoofing" scams, especially when used with DMARC and SPF. DKIM is difficult to spoof since it detects inconsistencies in email headers. DKIM helps ensure deliverability; without a DKIM signature and valid records, recipients' SMTP servers are significantly more likely to block your emails and mark them as spam (or just reject them outright).

Read more about DKIM here.

How to identify bogus emails

Is this email for real?

We hear this from clients all the time. When you receive a message that looks suspicious, there are some steps you can take before you call in the professionals (us).

1. Look at the sender's email address
   At first glance many spam emails may appear normal, as they might mirror a legitimate company's branding and seem on the up and up. One of the easiest ways to determine if the email is spam is to look at the sender's email address. A legitimate email from a business shouldn't come from a free email service address such as Yahoo, Hotmail, or Gmail, and there shouldn't be a bizarre string of numbers in the email address either. Also, check the spelling of the sender's domain. There's a big difference between services@microsoft.com and services@micorsoft.com. Can you spot the difference? A spammer will hope you can't.

2. Look at the information the sender is requesting
   Your bank should never request sensitive financial information through email. Be wary of emails that ask you for sensitive information. So, if you get an email that asks you for personal information, no matter how legitimate it might seem, ignore it. Bad guys may try to trick you into giving away your username and password by providing a link that takes you to a logon page. For example, you might receive a message from "Netflix' saying there's a problem with your account, asking you to click the link to sign in to resolve the issue. If there's ever a doubt, don't click the link. Instead, open a web browser and go to the site directly. That way you know you haven't been fooled into giving away your credentials.

3. Look at the greeting
   If a legitimate company, like your bank or your credit card company, wants to reach out to you via email, they will have your personal details so will normally address you with your first name. Spam emails will likely begin with a generic, 'valued customer' greeting or even just a 'good morning'.

4. Look at the content of the email
   Many phishing emails are rampant with grammatical and spelling errors – always a bad sign. Many bad actors from foreign countries struggle with American grammar and spelling. Here is an example. You can see others here.

5. Analyze the headers

This step is a little more advanced than the previous steps, but well worth taking the time to learn. An email header is a code snippet that consists of essential details to authenticate an email message. It precedes the email body and contains information about the sender and recipient.

An email header is more than the to, from, date, and subject section that precedes an email body. Headers also play an essential role in recording an email's route since every email message has an email header.

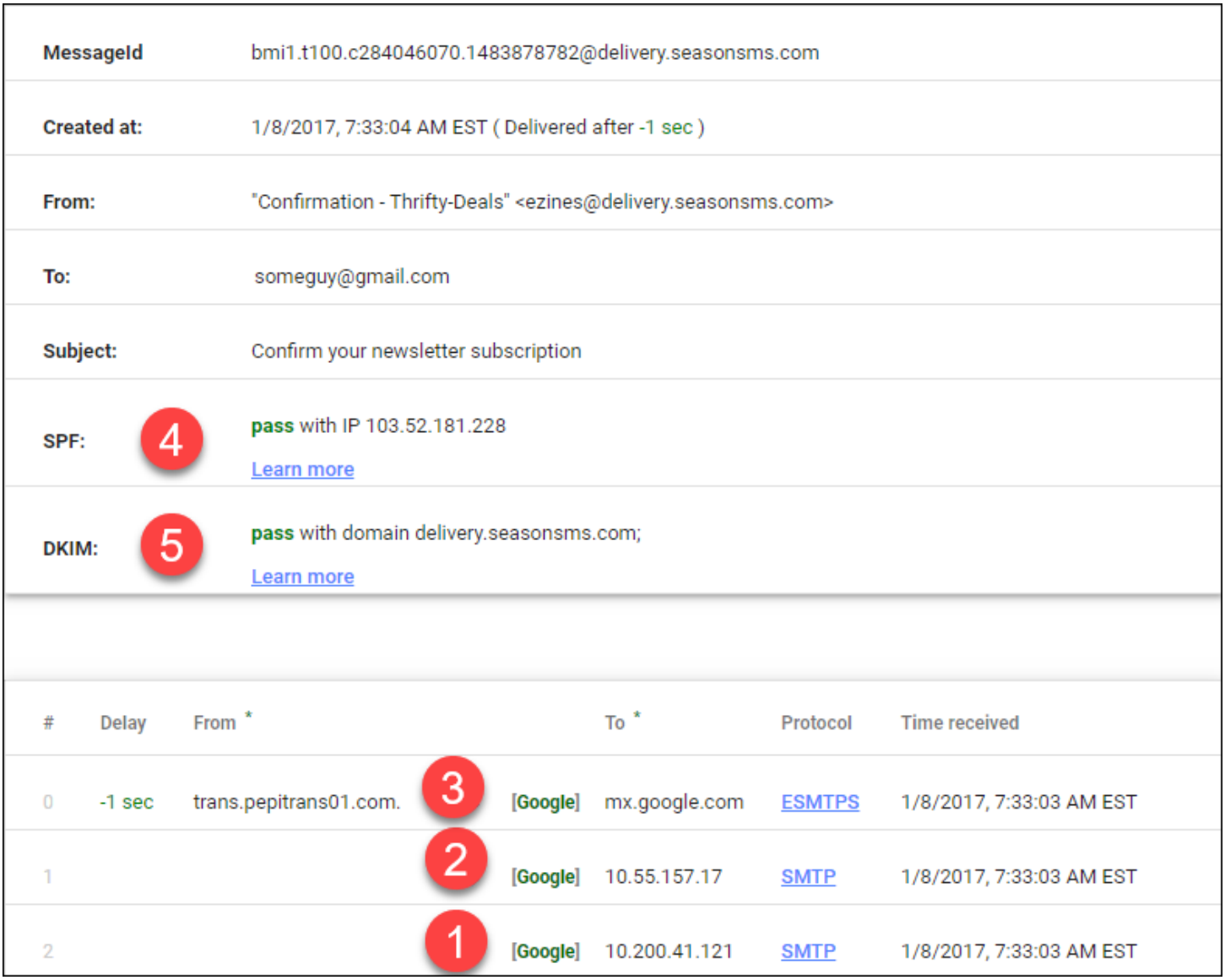
When an email is sent from one address to another, the message will go through mail transfer agents (MTA). So, email headers will show If the email was sent to other addresses before reaching its final destination. If the header information looks suspicious, users can avoid engaging with the email.

Headers use metadata to provide information about the transmission process. Here's an example of part of a header. It seems to be mostly gobbledygook, but everything here means something.

```
Delivered-To: someguy@gmail.com
Received: by 10.200.41.121 with SMTP id z54csp461727qtz;
       Sun, 8 Jan 2017 04:33:03 -0800 (PST)
X-Received: by 10.55.157.17 with SMTP id
g17mr82034336qke.122.1483878783846;
       Sun, 08 Jan 2017 04:33:03 -0800 (PST)
Return-Path: <0-1111323-gmail.com@delivery.seasonsms.com>
Received: from trans.pepitrans01.com
(trans.pepitrans01.com. [103.52.181.228])
       by mx.google.com with ESMTPS id
94si44473076qtb.140.2017.01.08.04.33.03
       for <someguy@gmail.com>
       (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256
bits=128/128);
       Sun, 08 Jan 2017 04:33:03 -0800 (PST)
Received-SPF: pass (google.com: domain of 0-22228-
gmail.com@delivery.seasonsms.com designates 103.52.181.228
as permitted sender) client-ip=103.52.181.228;
Authentication-Results: mx.google.com;
      dkim=pass header.i=@delivery.seasonsms.com;
      header.i=@delivery.seasonsms.com;
      spf=pass (google.com: domain of 0-22228-
gmail.com@delivery.seasonsms.com designates 103.52.181.228
as permitted sender) smtp.mailfrom=0-22228-
gmail.com@delivery.seasonsms.com
```

The good news is that you don't have to understand all the data in the header. You can use an email header analyzer to parse the "gook" into English. A Google search for *email header analyzer* will return hundreds of sites that offer this (free) service. We like Google's analyzer because it's easy to understand. Just copy and paste the header into

the analyzer, click the **ANALYZE THE HEADER ABOVE** link and out comes the result. Here is the analyzed (full) header from the example above.



MessageId	bmi1.t100.c284046070.1483878782@delivery.seasonsms.com
Created at:	1/8/2017, 7:33:04 AM EST (Delivered after -1 sec)
From:	"Confirmation - Thrifty-Deals" <ezines@delivery.seasonsms.com>
To:	someguy@gmail.com
Subject:	Confirm your newsletter subscription
SPF: 4	**pass** with IP 103.52.181.228 Learn more
DKIM: 5	**pass** with domain delivery.seasonsms.com; Learn more

#	Delay	From *		To *	Protocol	Time received
0	-1 sec	trans.pepitrans01.com. 3	[Google]	mx.google.com	ESMTPS	1/8/2017, 7:33:03 AM EST
1		2	[Google]	10.55.157.17	SMTP	1/8/2017, 7:33:03 AM EST
2		1	[Google]	10.200.41.121	SMTP	1/8/2017, 7:33:03 AM EST

What the results mean

1 and 2 tell us the IP addresses of the servers where this message originated. The ones here don't help us because IP addresses that begin with 10, (like 10.200.24.12) are public-use addresses, usually used for the individual computers on the *inside* of a business or a home network. The business/home firewall assigns these addresses to the computers they service and those address are not visible on the other side of the firewall (to the public).

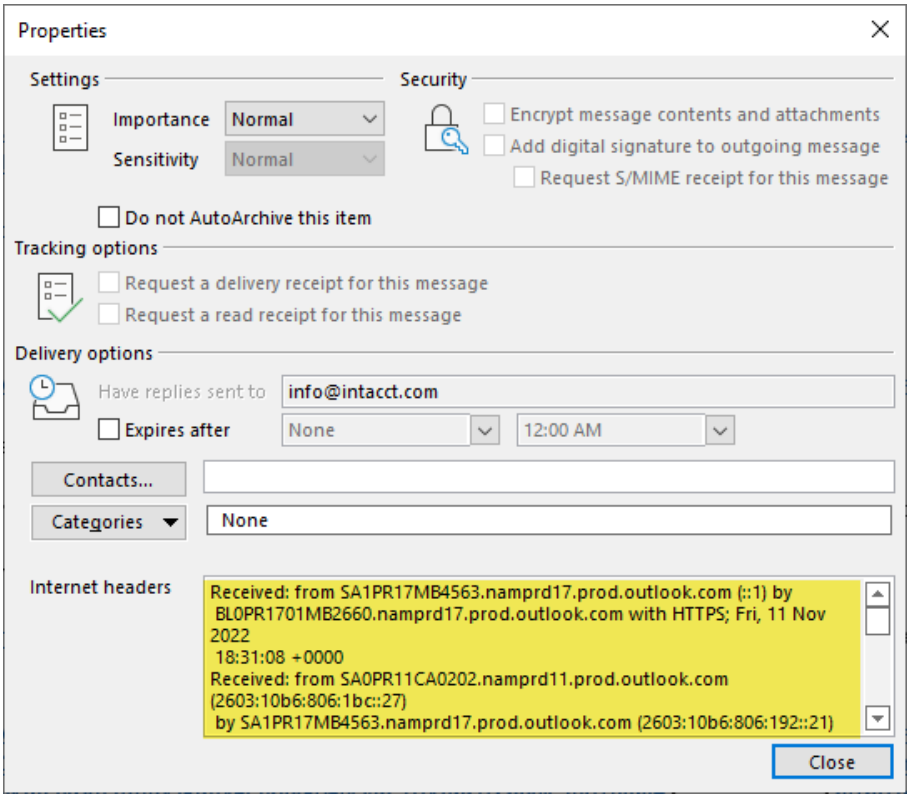
3 tells us the third server to handle the message was a Google server. This also is not helpful since Google's servers handle millions of emails a day. If one of these three IP addresses had been the public address of a service provider, we could have looked up the IP address and known the country or even the city of origin.

4 and 5 are more helpful. They don't tell us anything about the message's originating location, but they do tell us the message was sent from a domain that has taken the time to set up DKIM and SPF (we covered this in the previous article), something that bad guys don't do. The passed SPF and DKIM tests indicate this message came from where it says it does – seasonsms.com. This doesn't confirm the validity of the message, but it's a good indication.

How to find the email header

Here is how to find an email header in Outlook. If you use a different email client, like Gmail, Thunderbird, iCloud or AOL, there are helpful instructions here.

1. In Outlook (this example uses Outlook 365).
2. Open the email in its own window (double-clicking the email should do it).
3. In the opened message, go to File > Properties.
4. Look for the box to the right of **Internet headers** and copy the contents to the clipboard. Hint: You can click in the box and type **Ctrl+A** on the keyboard to select the contents and then type **Crtl+C** to copy.
5. Once you've copied the headers you can just paste them into your chosen header analyzer.



Can an email header lead me to the person who sent the message?

Usually, no. At best, you might be able to find the IP address of the first mail server to have handled the message and then look up that server's IP address using an online search tool such as MXToolbox. However, as we see in the example above, the originating addresses (1 and 2) are non-searchable addresses and 3 is a Google address, none of which will lead us to a person or a specific sending device. Occasionally, in the case of an actual spam email (which this one is not), the originating IP address can be traced to a city or country, but probably not to a specific device or individual. That's OK, though, because the email header gives us enough information to make an informed decision as to whether or not the email is legitimate or spam (DKIM and SPF passed).

We will be happy to do the email header analysis for you, but we will need to see the actual headers, meaning you will have to copy the headers and paste them into an email to us for us to analyze. It won't work for you to forward the suspicious email to us.

Here is a complete breakdown of the header used in the example, if you would like to do some more study.

Best practices to avoid being compromised

Of course, the best way to deal with a compromised email account is to avoid getting compromised in the first place, so let's start with some tips on how to stay safe.

Use a password manager and multifactor authentication (MFA) wherever possible

Use a reputable password manager to change all of your online passwords to strong, unique ones for each login. We can't stress this enough. Hackers today use a tactic called credential stuffing, whereby they literally cram previously stolen usernames and passwords into as many online services as possible. Why? Because a lot of usernames and passwords are identical across accounts. We know that it's hard to remember multiple passwords, so we recommend using a password manager. We like and use LastPass.

If signing up for a new email service, check for MFA support

Not all email providers provide MFA. So, when signing up with an email provider, check to see what layers of security are available such as MFA either through SMS (less secure) or app-based such as Google Authenticator or Authy.

The main benefit of MFA is that it provides a second layer of security such as a text message sent to a smartphone with a one-time password. Only the person with your device can ostensibly complete a new login. Not to mention, it can inform you when someone is trying to log into your email account.

Don't click suspicious links in email or texts

We covered this in the previous article, but it bears repeating.
Phishers often send links via email or text that look legitimate, but once clicked, the links allow the phishers to steal your information. Email attachments that contain malware are also popular vessels for cyber mayhem. The easiest way to avoid these scams is by not clicking the links or attachments. Instead, open another tab and go to the website of the company in the email or link to see if the information presented matches the official source. As a general rule, never open links or download attachments from unknown senders. Emails from known senders that contain links or attachments without any context are also bad news.

Don't use public Wi-Fi or public computers to work with sensitive information online

When you're traveling or not at home, try to use the internet only through your own computer and your own mobile hotspot. Public computers at hotels, for example, are accessible by other people who can put keyloggers or other malware on them, which can come back to haunt you. The public Wi-Fi provides a target-rich environment for someone who knows how to access the data being transmitted.

If you must use public Wi-Fi, use a good VPN service

VPN stands for "Virtual Private Network". When you use a VPN, you connect to the internet through one of the VPN's servers. In doing so, your device's traffic is encrypted, protecting you from some of the security threats coming from public Wi-Fi hotspots. Here is some more information about VPNs, including recommendations and reviews. For our PM clients that use Avast CloudCare, Your Avast subscription includes Avast SecureLine VPN, which is perfect for use when you're away from home. If you are not already an Avast customer, we'd be happy to set you up.

We should point out here that many of our clients use VPN to connect their home computers to their work servers and/or computers. VPN in this instance provides an encrypted tunnel between their home and work. The VPN in this article is used for a different purpose and you most likely can't use your work VPN client for that purpose.

Get a strong antivirus

Speaking of Avast CloudCare, which is a great antivirus…
A good antivirus raises the bar on securing your information, with real-time protection from phishing attacks and threats like malware, ransomware, and more. Windows comes with its own antivirus (Windows Security), but we don't think that's enough. We recommend Avast CloudCare to all our clients.

Help! I've been hacked!

It starts like this: your inbox starts receiving messages from people you haven't corresponded with for a while asking, "Did you really send this message". Your phone calls now include people asking the same question. Someone has been sending out emails, claiming to be you. What do you do now?

Change your password. Do it NOW!

You probably have no idea if you've been hacked or spoofed (see our earlier article in this newsletter explaining the difference), but regardless how someone is pretending to be you, your first action must be to change your email password. You can't take back the bogus emails that have already gone out, but you can prevent someone who may have gained access to your account from continuing unimpeded. If you are a TekResults email client, and need help getting your password changed, call us right away.

Determine if you've been hacked or spoofed

You may have trouble doing this on your own. Best to call us and ask us to investigate.
It may be difficult to obtain the email headers from one of the bogus messages; asking someone who received that message to forward it to you won't work, because the forwarded message has its own headers and the headers from the bogus message won't be included.

Run a message trace

Most email servers have the ability to run a message trace on your email address to see if the bogus emails were actually sent from your account. We can assist with this. It's possible someone has spoofed your account and did not actually use it to send out those emails. If your account was compromised and was really used to send the emails, a message trace will list every email that was sent, the delivery address, the time, and whether or not it was delivered. If you were spoofed and your account was not used to send the messages, other than changing your password, there's little else to do.

Check your inbox rules

One of the hacker's favorite tricks is to gain access to your mailbox and then create rules to do unexpected things to your incoming mail. Most often we've seen rules that move all incoming messages to the Deleted Items or RSS folder, where you wouldn't think to look for them.

Run a Microsoft 365 Security Audit

We have the ability to run a security audit when one of our clients has been compromised. The security audit reveals who all the users are in a domain, which users have administrator privileges and what rules are in place for each user. This information is extremely helpful in spotting problems, especially unexpected inbox rules.

Windows indexing

Have you ever used the Windows search tool to look for something on your computer? Windows uses an index to help you quickly find what you're looking for. Indexing the contents of your PC helps you get faster results when you're searching for files, documents, and email. Here's how it works.

What is indexing?

Indexing is the process of looking at files, email messages, and other content on your PC and cataloging their information, such as the words and metadata they contain. When you search your PC after indexing, it looks at an index of terms to find results faster. Think how difficult it would be to find something in a textbook or reference manual if there was no index in the back of the book. The index makes finding a specific subject relatively easy. The same principle is at work on your computer. A fully built index can return answers to searches such as "Show all songs by Taylor Swift" in a fraction of a second, versus the minutes it could take without an index.

When you first run indexing, it can take up to a couple hours to complete. After that, indexing will run in the background on your PC as you use it, only re-indexing updated data.

What information is indexed?

By default, all the properties of your files are indexed, including file names and full file paths. For files with text, their contents are indexed to allow you to search for words within the files. Apps you install may also add their own information to the index to speed up searching. For example, Outlook adds all emails synced to your machine to the index by default and uses the index for searching within the app.

Which apps use the index?

Many of the built-in apps on your PC use the index in some way. File Explorer, Photos, and Groove all use it to access and track changes to your files. Microsoft Edge uses it to provide browser history results in the address bar. Outlook uses it to search your email. Cortana uses it to provide faster search results from across your PC. One Special case is PDF's. You will need to use an Adobe indexing tool to get this to work. Adobe used to provide search function with iFilter. It can still be downloaded but doesn't work with windows 11. There are third party options such as Mythicsoft that will do the job.

Many apps in the Microsoft Store also depend on the index to provide up-to-date search results for your files and other content. Disabling indexing will result in these apps either running slower or not working at all, depending on how heavily they rely on it.

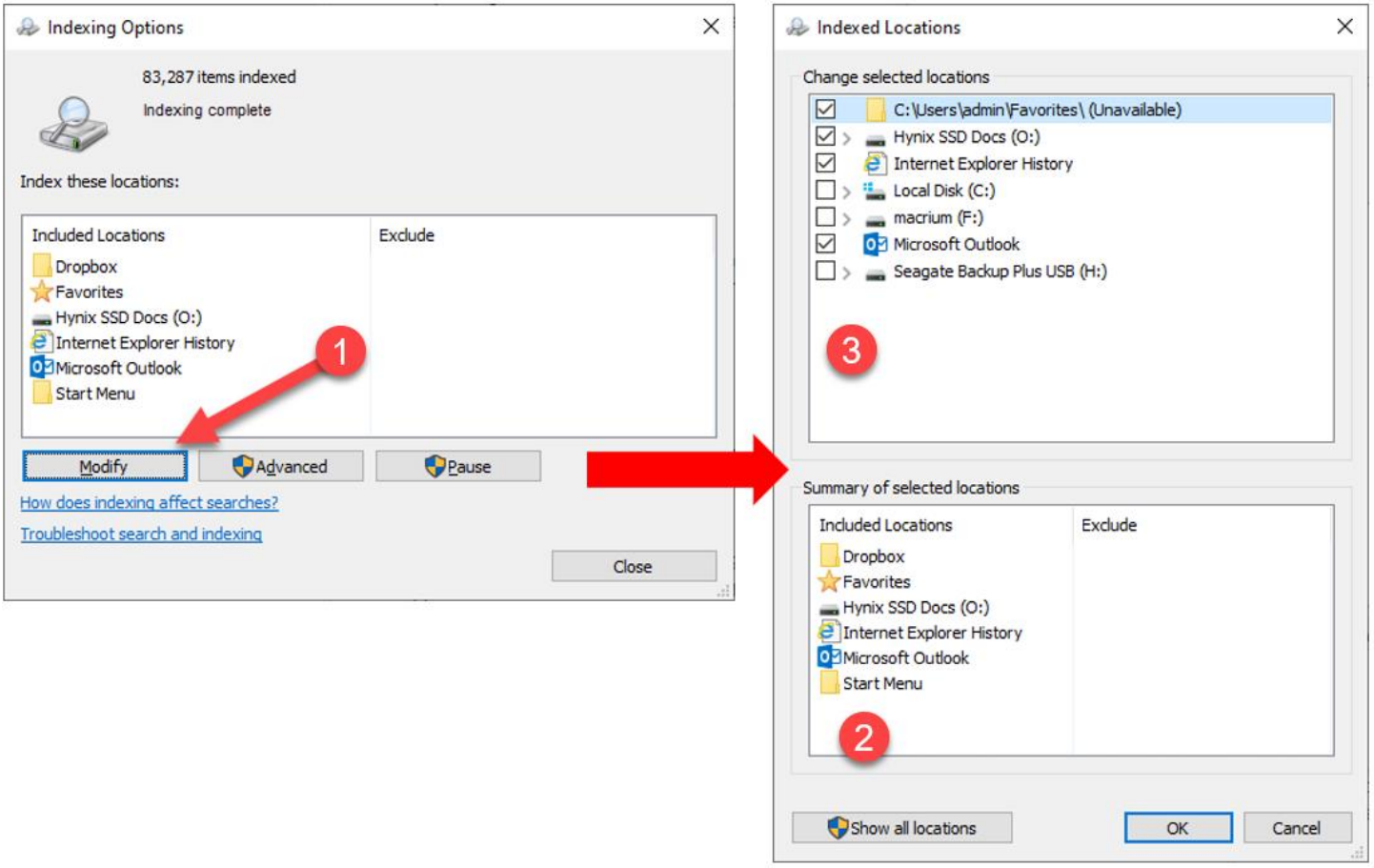
Indexing best practices

Indexing is a great tool, but if it's not managed the index can easily become bloated and filled with indexed locations that you don't care about or will never need to be searched. A bloated index will slow down searches and take up additional space on your hard drive.

How to manage your indexed locations

Amusingly enough, Windows Search is the easiest way to get to the settings you need. Just click the **Start** button and type **indexing options**. Click on **Indexing Options** when it appears in the search results. Or you can open Control Panel and access **Indexing Options** from there.

The Indexing Options window gives you a quick view of the locations Windows has indexed. Of these locations you will want to make sure your Documents and Outlook are indexed, but everything else is arbitrary, based on how often you think you might search those locations. To modify the locations, just click the **Modify** button (1).



In the **Change selected locations** (3) part of the resulting dialog box, you can uncheck the locations you don't want to index. Notice that some of the locations have an expand button **>** to the left of the location, which will allow you to see the folders in that location that are being indexed. If so desired, you can uncheck folders to your liking. Note, the locations shown will be different for you.

The **Summary of selected locations** part of the resulting dialog (2) shows the top-level locations for the choices you've made above in 3. If you click on one of the locations here, it will highlight the folder in 2 and display the location with its check box. This is helpful if your summary has a lot of entries and want to quickly navigate to the check-boxed location in 3.

Uncheck the locations you don't want to index and then click OK. Windows will immediately begin to reindex. You can then close the Indexing Options dialog box. You can use your computer while the index is updating, but searches will be slow until it's complete.

You will find more information about indexing here.

Upgrading your Wi-Fi

In 2023 there will be more devices using Wi-Fi than ever before. Multiple TVs, phones, tablets, games, it seems that everything can now be controlled using Wi-Fi. Earlier in 2021 we presented a newsletter highlighting the uses of home automation and noted that you can even buy a single light bulb that can be controlled by a Wi-Fi enabled app! With all this wireless connectivity going on, we need a better standard of Wi-Fi connectivity. Fortunately, the powers that decide these things, the Wi-Fi Alliance, is on the case.

What Is Wi-Fi

The term "Wi-Fi" was created by the nonprofit Wi-Fi Alliance and refers to a group of wireless networking protocols that are based on the IEEE 802.11 network standard. Wi-Fi has been around since the late '90s but has improved dramatically in the last decade. The most recent standard (802.11ax) is more commonly called Wi-Fi 6.

How Is Wi-Fi 6 Different?

Wi-Fi 6 is a substantial upgrade over previous generations, though the differences may not seem immediately obvious to the average user. These changes might not dramatically change the way we use wireless routers or wireless networking but instead consist of many incremental improvements that stack up to be a substantial upgrade.

The first big change is that Wi-Fi 6 allows for potentially faster connection speeds. Faster Wi-Fi means better upload and download speeds (or throughput) due to the increased bandwidth afforded by Wi-Fi 6. This is becoming increasingly important as file sizes continue to increase, along with the higher data demands of streaming high-quality video and communication-heavy online gaming. Playing a multiplayer game while also streaming to Twitch requires large amounts of bandwidth and a reliable and stable connection.

How much faster? Theoretically, the maximum Wi-Fi 6 speed is 9.6 Gbps. This is the maximum throughput of Wi-Fi 6 across multiple channels. By contrast, Wi-Fi 5 offers a maximum of 3.5 Gbps. Keep in mind, in real-world situations, local networks may not reach this top speed, but when that maximum is shared across multiple devices, devices with Wi-Fi 6 can enjoy significantly faster speeds even if they don't reach the maximum potential.

Other differences

Increased speed is just one of the benefits of Wi-Fi 6. Other features help improve network congestion by using Overlapping Basic Service Sets (OBSS) and employing Beamforming technology to detect where a device is requesting data and transmitting the data in the device's direction in a localized data stream, as opposed to just broadcasting data in all directions. Besides speed and signal optimization, Wi-Fi 6 also offers better security and increased battery life for your wireless device (by activating the device's radio only when needed). Pretty amazing stuff!

Our recommendation

Let us know if you want us to look at your WIFI and make recommendations – we are already doing this for our PM clients

MacOS 13 Ventura is here

If you're a Mac user, say goodbye to Monterey and hello to Ventura—MacOS Ventura, that is. Also known as MacOS 13, Apple's latest operating system is finally available for download. The latest version packs a variety of new capabilities into desktops and laptops, including updates to Messages, Safari, the Mail app, and Continuity, among others. Here are five of Ventura's new features.

iCloud Shared Photo Library

Instead of using AirDrop to send batches of photos or manually sending them to a group chat, you're now able to share a collection of images in a shared iCloud library with up to five other people. You can share all the photos and videos in your library or customize specific content that you want automatically added based on people in the images, the date they were taken on, or even the proximity—like if you wanted to share all your vacation photos with others on the trip with you. Anyone in the Shared Library can edit, delete, and favorite photos, and this will all sync to everyone's devices.

Useful Message Features

We've all sent regrettable texts before. With MacOS Ventura, you can edit messages up to 15 minutes after sending them and delete them up to two minutes after. You can also recover deleted texts for up to 30 days. Meanwhile, those

who have read receipts can mark a message as unread, which will hopefully ease the pressure to respond right away. Since Messages runs on many of Apple's devices, these features are also available on iOS 16 and iPadOS 16. You can now take advantage of SharePlay via Messages too. Instead of FaceTime, you can watch a movie or listen to music with friends and family in a group chat. With access to shared playback controls, everyone's content is always in sync.

Live Captions

Apple is introducing Live Captions for those who are deaf and hard of hearing to Macs with an M-series chip. The feature automatically transcribes audio for media, calls, and in-person conversations. When using Live Captions during a call on a Mac, you can also type what you want to say via Type to Speak and have your response spoken out loud for others in real time. The feature will work in the FaceTime app, too—with the addition of speaker attribution.

Mail App Features

The native Mail app in MacOS has received some usability enhancements that bring it up to par with Gmail and other modern email clients. Ventura users can now unsend emails shortly after firing them off and can schedule emails to be sent at a later time. You'll receive nudges to follow up on emails sent a few days ago that haven't yet received a response. And, if your email mentions an attachment or a person who's been CC'd but you forgot to attach a file or CC someone, you'll get an alert. Finally, searching your inbox is more convenient. Click on the search box within Mail and it will show a list of your recent contacts, documents, photos, and emails before you even start typing.

PassKeys

Apple is on a mission to kill traditional passwords, and it's teamed up with the FIDO Alliance to create a secure passwordless sign-in system called Passkeys. Passkeys are stored on only your device and never on a web server, so they are virtually immune to phishing attacks. Instead of typing in a password when you land on a login page, you'll be prompted on your Mac's screen to pick up your iPhone or iPad and use either Touch ID or Face ID to verify your identity. The two devices talk to each other, and with that, you're logged in.

Passkeys will sync across all your iCloud-enabled devices, including iPhone, iPad, and Apple TV, in addition to Mac (with end-to-end encryption). On non-Apple devices, you'll have to sign in using your iPhone. However, Google and Microsoft are part of the same group working with the FIDO digital identity organization, so similar functionality is coming to Windows and Android soon.

A larger list of new features and this full article are available here.

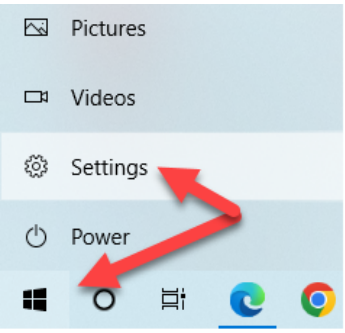
6 reasons to upgrade to Windows 11 - And a couple reasons you shouldn't

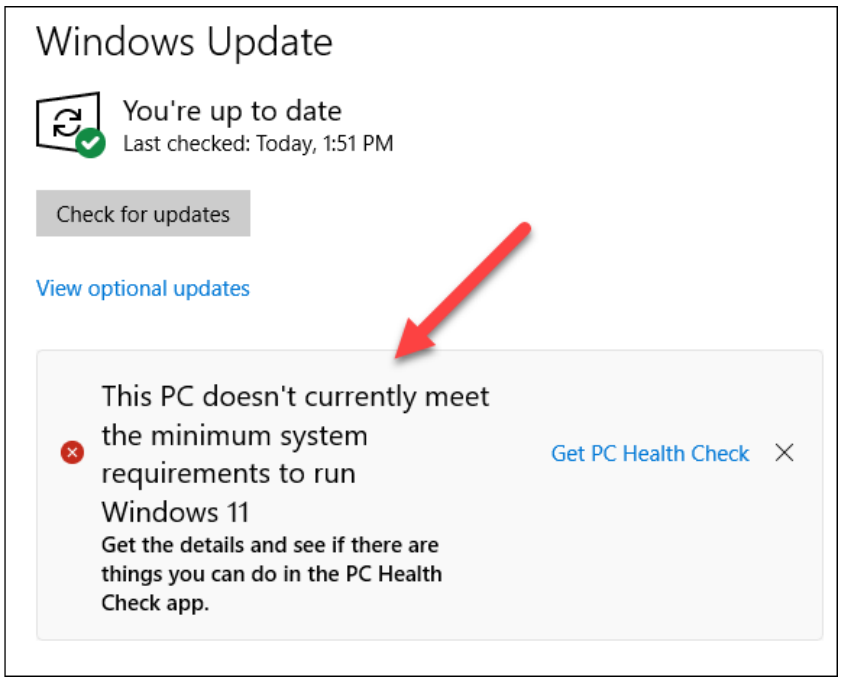
Windows 11 has been available since October 2021 and many of our clients have already taken advantage of the free upgrade from Windows 10. This article contains some reasons you should consider the upgrade – and a couple reasons you shouldn't. Normally, we would say that there is no hurry since Windows 10 will continue to be supported until October 14, 2025, however the developer of your favorite software may feel differently and stop supporting Windows 10 before Microsoft does, making Windows 11 a requirement to run their software.

Why shouldn't I upgrade?

If you're considering the upgrade for a home computer, there is little reason not to upgrade, but if your computer is used in a business environment, someone in your company should make sure that all the business apps employed on your computer are compatible before making the leap. Many companies use specialized software, which may include accounting, audiological, medical, industrial and banking apps that have not yet been proven to work with Windows 11. We have encouraged all our clients to thoroughly vet all apps used in their businesses before upgrading. The vetting process should include a discussion with the software developer's customer service or IT department.

Your system may not be able to upgrade to Windows 11 due to hardware limitations. By now, most systems that can be upgraded to Windows 11 will tell you so if you go into the Windows 10 Settings. Click Start > Settings > Update & Security.





Alternately, you can download and use Microsoft's PC Health Check app to give you a definitive evaluation.
After downloading the app,

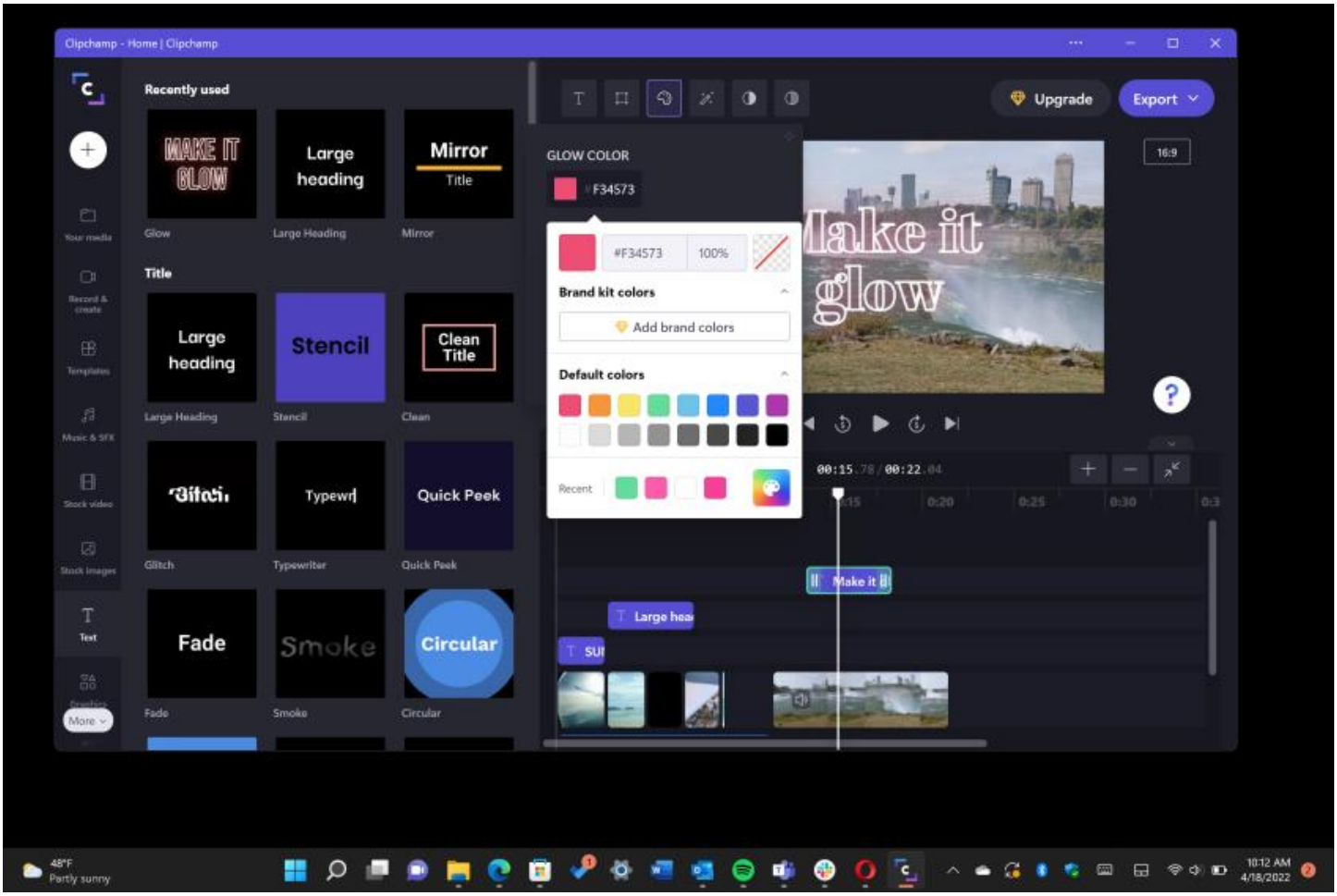
1. Press Windows logo key + S or select **Search**, type **pc health check**, and select **PC Health Check** from the list of results.
2. Select **Check now**.

With the reasons NOT to upgrade out of the way, here are a few reasons you SHOULD upgrade.

A More Consistent Interface

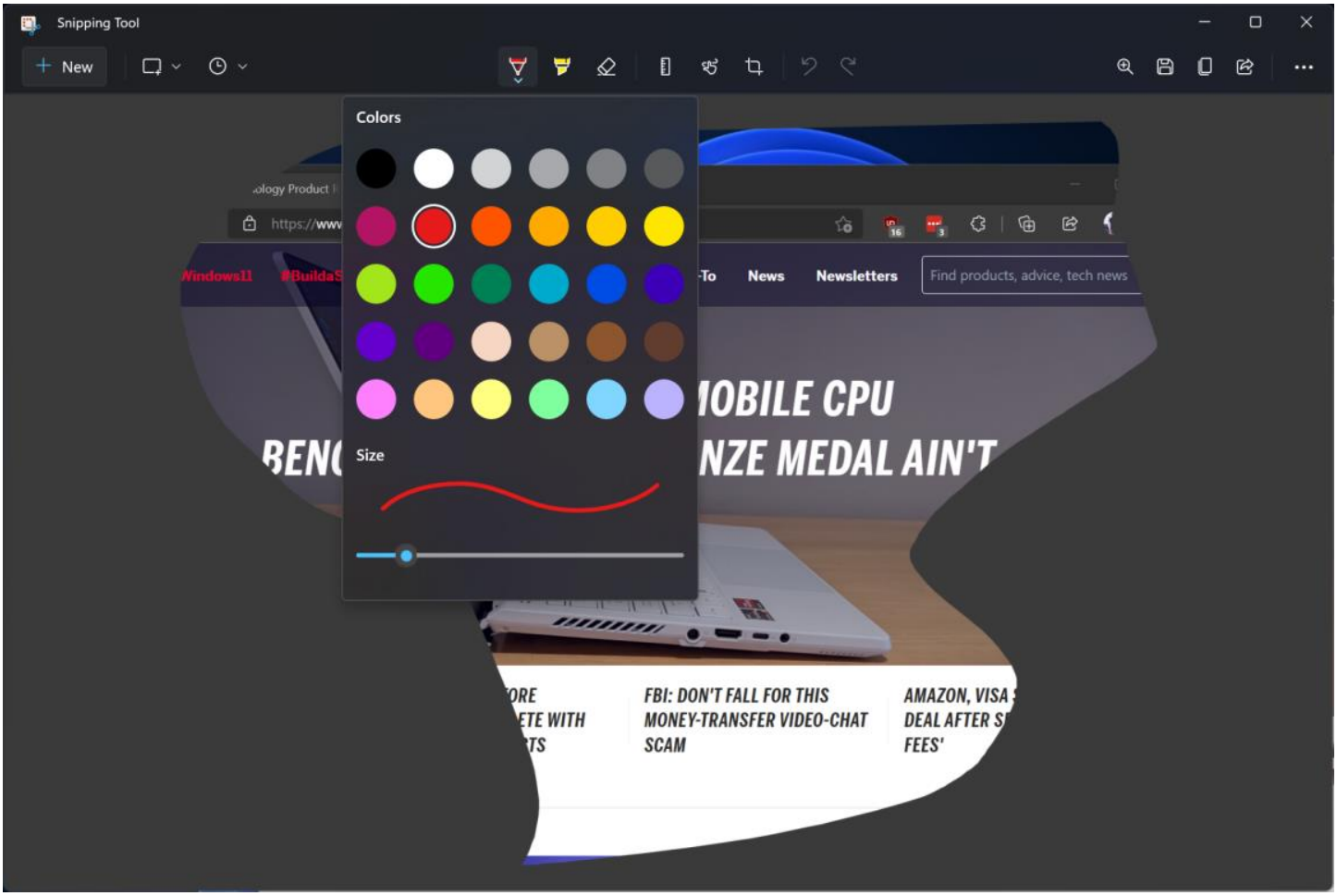
PC users no longer need to hang their heads when friends show them their slick macOS and Chrome OS user interfaces. Windows 11 is every bit as slick, aside from the occasional old-school Control Panel dialog box. The rounded window corners, compact Taskbar, and touch-friendly (sorry, Apple) design is easy on the eyes. It just looks nicer. Let's not forget the understated and pleasing new system sounds (Opens in a new window), too.

Improved Included Apps



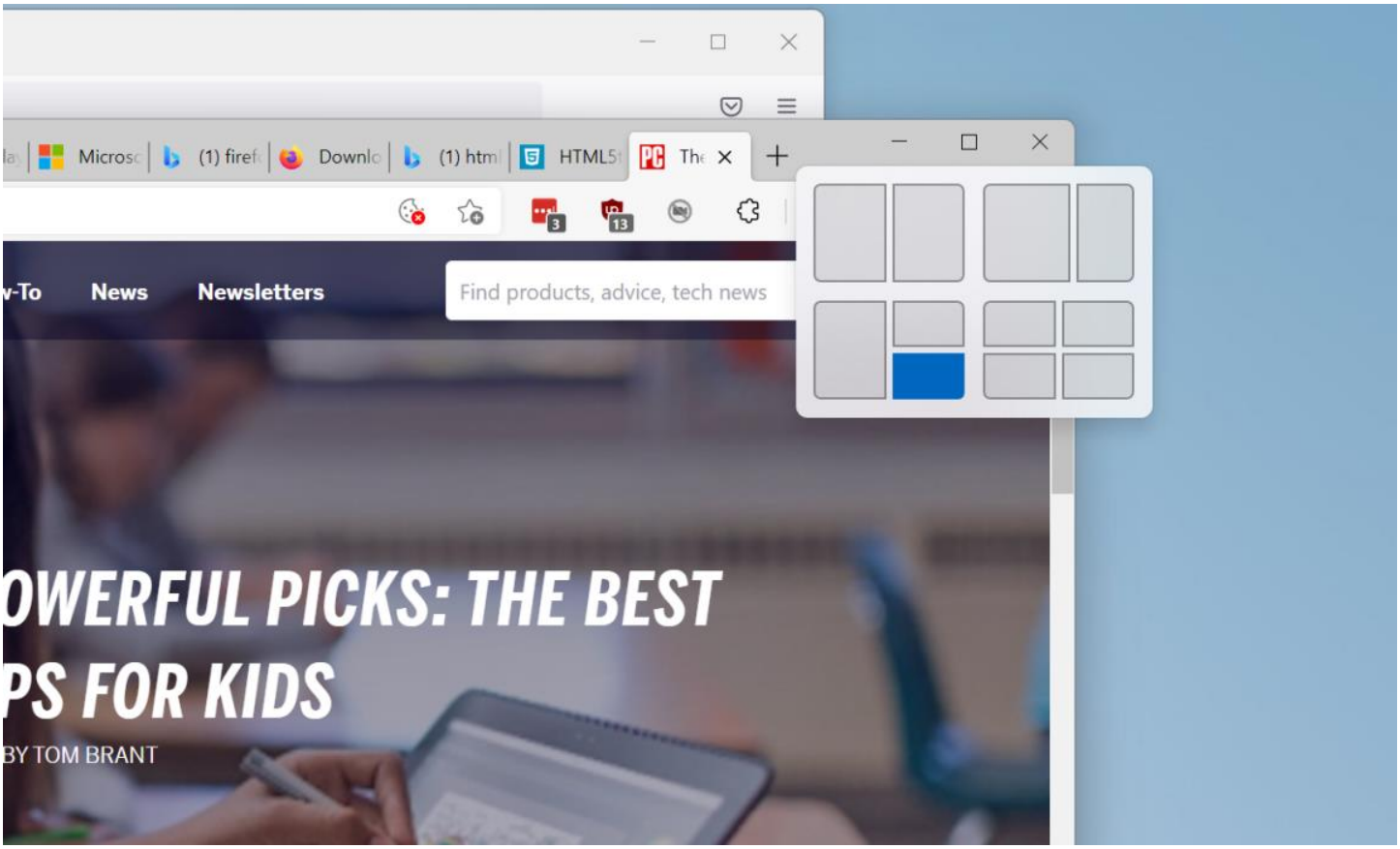
The included apps in Windows 11 are better than those in Windows 10. An all-new Media Player app makes watching videos and listening to music and podcasts a better experience. Windows 11 users will also get Clipchamp, a simple template-based PWA video editor suited to small business making videos for marketing and advertising. The Windows 11 Clock app deserves special mention because of its useful new Focus Sessions feature that helps you concentrate on projects. The Photos app also includes surprisingly capable video editing, with some features not even found in Clipchamp. The Notepad, Paint, and Calculator apps have all been updated as well.

A Better Screenshot Tool



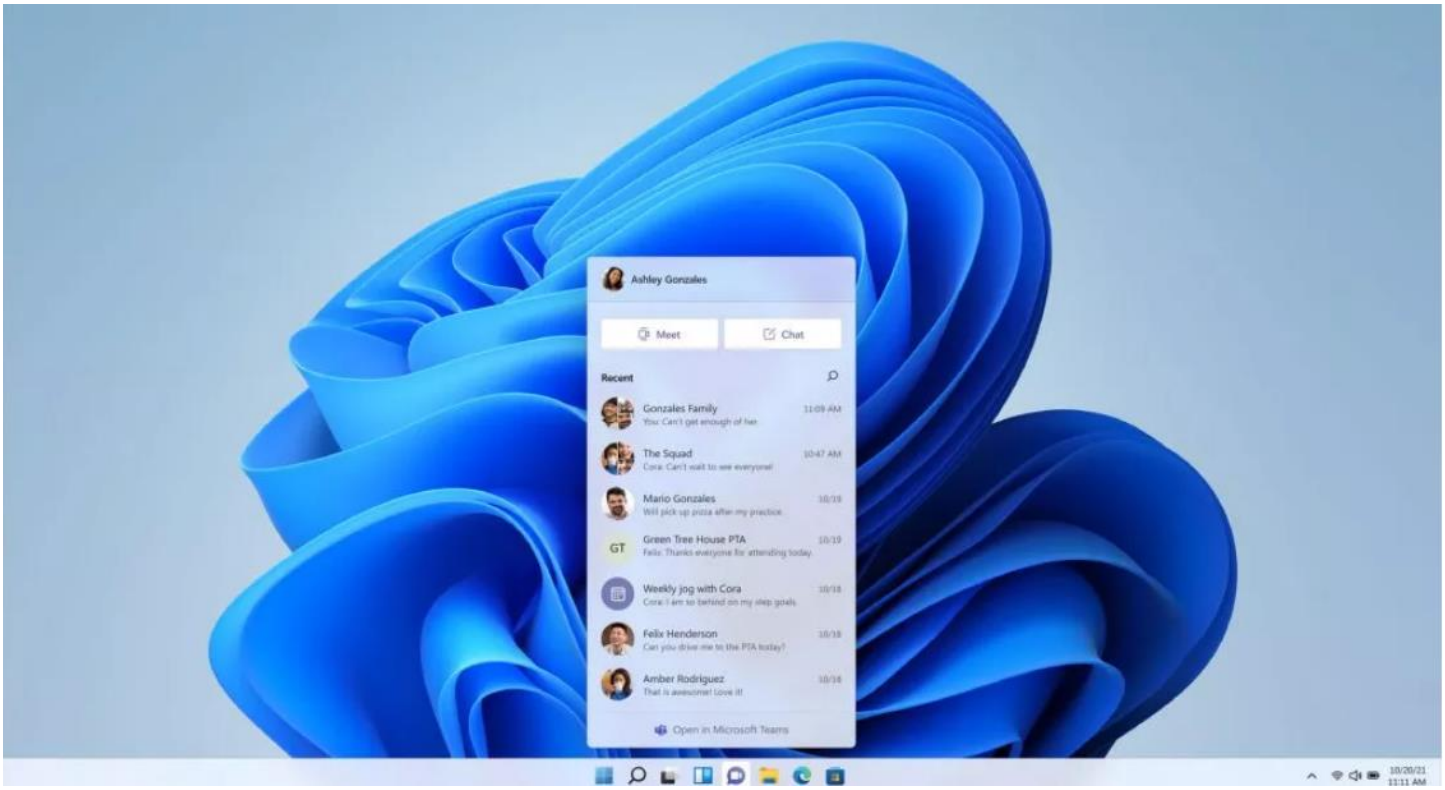
Taking screenshots in Windows 11 continues to improve, with many good options. Microsoft has updated the clunky old Snipping Tool (accessible with Windows Key-Shift-S), which competes with the similarly named and superior Snip & Sketch app. The Snipping Tool lets you select rectangular or freehand areas, program windows, or the whole desktop. It then opens a mini-editor for cropping and markup. The screenshot tool also has a delay timer and built-in options for saving and sharing. You can still use the tried-and-true PrtSc key to save a screen image file to the clipboard or to OneDrive.

Snap Layouts for an Organized Desktop



In Windows, you have always been able to arrange windows on the desktop just the way you want them. Just when we thought it wasn't possible to improve the already great capabilities in Windows 10—which lets you snap a window to the side to fill exactly half the screen or to a corner for an exact quarter of screen real estate—Microsoft comes up with another window layout trick called Snap Layouts. When you hover the cursor over the maximize icon at the top right of any window, you get multiple layout choices in a thumbnail view. You can even save a layout for a group of apps you want to reuse later in a single taskbar icon.

Collaboration and productivity



One of Microsoft's main focuses with Windows 11 has been the new level of interoperability with collaboration platform Teams, which has been built into the core of the new OS (and has also received a Windows 11-flavored visual overhaul).

In Windows 11, users can launch directly into Teams chats and meetings with a single click or touch, via an icon that takes a front-and-center position in the taskbar. The new system tray also hosts a mute button for easy access, addressing one of the most common pandemic faux pas.

Performance and security

During the development of Windows 11, Microsoft homed in on performance and security, two qualities that will top the priority list for any business. Microsoft claims Windows 11 boot times are significantly faster, and so is authentication service Windows Hello. Navigating the web and web-based services is also said to be much snappier, and not just on Edge. The new OS uses less energy too, which should translate to longer battery life when employees are working on their travels.

Separately, Microsoft has made a point of highlighting Windows 11's security credentials, with new protections added at a chip and cloud level to ensure company assets remain secure no matter where employees are located.

"Key security features like hardware-based isolation, encryption, and malware prevention are turned on by default. We have also made going passwordless easier by simplifying the steps to deploy Windows Hello for Business," explained the firm. "And all these components work together in the background to keep users safe without sacrificing quality, performance or experience."

With security front of mind, Microsoft has also introduced a strict new set of hardware requirements for Windows 11. For example, all Windows 11-compatible CPUs must feature an embedded TP, and support secure boot, virtualization-based security (VBS) and specific VBS capabilities.

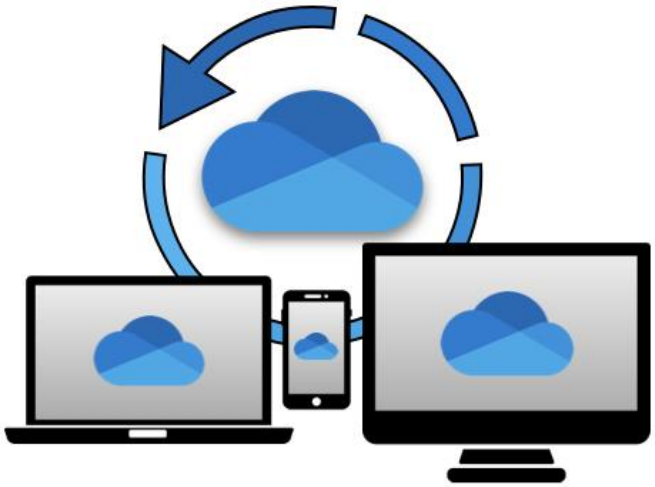
It’s for this last reason (hardware requirements) that many older systems will not be able to upgrade to Windows 11.

OneDrive Backup: How It Works, Benefits, Limitations and More

Cloud storage has become one of the most common ways of storing data due to its multiple benefits, including convenience, efficiency and cost-effectiveness. Unlike local/physical storage like hard disk, memory card or pen drive, when you upload a file to the cloud, it is saved on remote computers (also known as servers) in data centers that are located across multiple regions all over the world. With cloud computing, you can access these servers from anywhere and on any device via the internet.

One of the main advantages of cloud storage is that it enables users to share files and collaborate seamlessly, even while on the move. With the majority of workers around the world either working from home or in a hybrid environment, cloud storage is in high demand. One such popular cloud storage solution is Microsoft OneDrive. If your organization uses computing devices with Microsoft Windows, you must have surely encountered the term “OneDrive.”

In this article, we will discuss what OneDrive is, whether OneDrive is a viable backup solution or not, and how to better protect your OneDrive data.



What is OneDrive backup?

OneDrive backup is a cloud service by Microsoft that allows you to store, sync and share files over the internet. OneDrive is a part of the Microsoft 365 productivity suite and comes preinstalled on Windows 10 and Windows 11 PCs. You can access OneDrive using a web browser or directly through the OneDrive app. Let’s take a closer look at some of its important capabilities.

OneDrive backup for PC folders

OneDrive allows you to back up your PC folders, including documents, images, music and other important files to a cloud storage. This helps in protecting your data and allows you to easily access it on other devices as well. You can back up a maximum of 5GB of files in OneDrive for free, or up to 1TB with a Microsoft 365 subscription.

How to set up OneDrive backup for PC folders

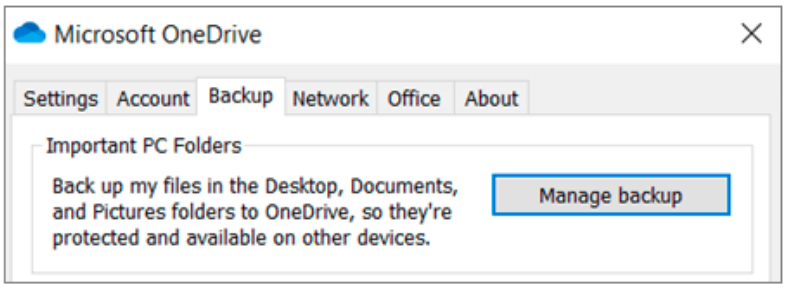
Setting up OneDrive backup for PC folders is simple and easy. Follow these steps to set up OneDrive:

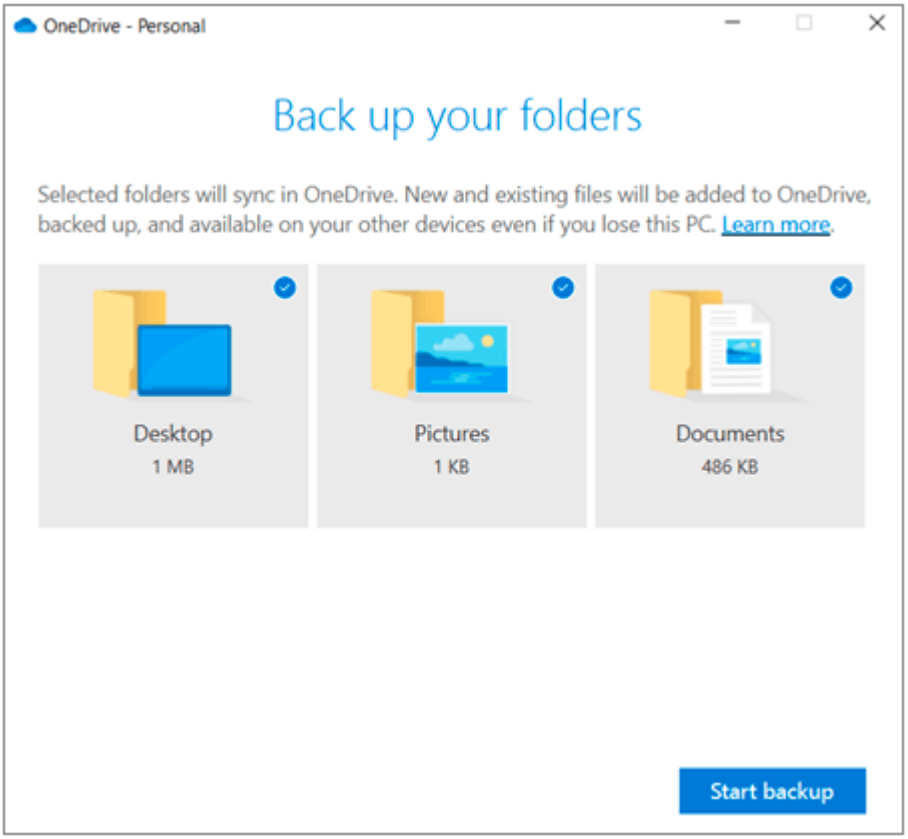
1. Select the blue cloud icon in the Windows notification area.

Don’t see a blue cloud?
Click the start button and type OneDrive to search Windows for the app. Launch the app. You will be prompted to sign in. Not sure how to sign in? Read on.

If the cloud icon is grey or has a line through it, that means you need to sign into OneDrive. How you do that depends on whether you are using a personal OneDrive account or OneDrive for Business. If your email is hosted with Microsoft 365, you would use your work email credentials to sign into OneDrive. If you are not using a work account, you can sign into OneDrive using a personal account. Personal accounts use a Microsoft ID. If you don’t have one of these, you can sign up for free here. Once you are signed in, continue to step 2 to configure OneDrive backup.

2. Select Help & Settings > Settings, then Backup > Manage backup.





3. Select the folders you want to back up.
4. Select **Start backup**.

When you start the backup, everything in your Documents, Pictures and Desktop folders will be moved to a new location on your hard drive. That location will be inside a new OneDrive folder; anything in that folder will sync with OneDrive in the cloud and, thereafter, anything you save to Documents, Pictures or your Desktop will be synced and available from any PC anywhere in the world.

Benefits

OneDrive provides easy accessibility to your backed-up files and folders from any device. In the event your device is lost or stolen, you can download the files from your OneDrive backup or access them via a web application. OneDrive also allows you to customize your backup preferences. You can choose to automatically save photos and videos to OneDrive whenever you connect a camera, phone or other device to your PC. You can also choose to automatically save screenshots to OneDrive.

You can access your files even on mobile devices by syncing them between your PC and OneDrive cloud storage. Syncing works automatically as long as you are signed into OneDrive. It also allows you to work on your files directly in File Explorer and access them even when you are offline. Any changes made to your files when you are offline will be automatically synced once you are online. You can also share OneDrive files with your colleagues using a shareable link for easy collaboration.

Is OneDrive a backup solution?

OneDrive allows you to store important files and folders in the cloud and protects your data to a certain extent with security features like AES 256-bit encryption and multifactor authentication (MFA). However, in terms of a backup solution, it falls short in some critical areas. For instance, being able to identify important documents that need to be backed up, based on a set policy.

Since the sync and share capabilities work only for files and folders, in the event your hard drive crashes, you cannot restore apps, operating system settings, user profiles and so on.

Cloud storage and backup may seem like the same thing, but their scope and functions are different. Cloud storage services, such as OneDrive, help free up space on your local device by saving copies of your files and folders in the cloud. However, they do not offer comprehensive protection or restore capabilities like cloud backup solutions. On the other hand, cloud backup solutions are designed to secure your data and enable quick recovery in the event of data loss or a breach.

For backing up your systems, we recommend and use Macrium Server Backup for all our clients' servers and Macrium Workstation Backup for select client PCs. We are a Macrium partner, so if you are interested in either of these products, let us know. We'll be happy to help.