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

TekResults Newsletter (Dec 2021)
To unsubscribe send email to UnsubscribeNewsletter@tekresults.com with *unsubscribe to Newsletter* in the subject line or click here UnsubscribeNewsletter@tekresults.com

Dear Clients and Friends

The Holiday Season is here once again. We hope you have survived Black Friday and found all the great deals you were looking for. We are grateful for the support we've enjoyed from our clients and friends this year. Some of you have taken the time to say thank you for our help, and that makes it all worthwhile for us. We wish you all a wonderful Holiday Season.

In this newsletter we'll bring you up to date on the Microsoft products that are reaching (or have reached) the end of their lives. We'll tell you about an exciting new tool we've invested in to help support our Preventative Maintenance Plan clients better, and we'll provide some tips on how to avoid having your email hacked. Finally, we'll discuss the need to upgrade your network equipment, and point you in the right direction.

If you are looking for last minute holiday gifts for loved ones or for yourself, we have lots of new HD monitors, including gaming curved monitors. We also have Windows 11 laptops and desktop computers and lots of other peripherals that would even make Santa smile.

Referrals

TekResults owes much of our 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 for you to enjoy a great meal at any of Dante's restaurants in Central PA. 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 disolved
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

Here's this month's newsletter!

How long will my Microsoft software be supported

We know it may seem like Microsoft is always announcing that one of their products is reaching the end of its supported life, but in reality, Microsoft products typically have a ten-year life cycle. The problem is there are so many Microsoft products that every year something reaches the end of its life.

With the release of Windows 11 in October this year, many users are concerned that their Windows 10 systems, released in 2015, are going to stop being supported by Microsoft. However, be of good cheer, Windows 10 is only six years into its ten-year life cycle and will be supported for another four years yet, until October 14, 2025.

What Does Microsoft End of Support Mean?

This means that once a product reaches its 'Extended Support End Date' there will be no patches, security updates or support from Microsoft. If you're using any of these products and do nothing, it's almost certain that your risks around security and compliance will increase, which may also impact productivity. These risks will only grow over time, so it's vital you act sooner rather than later.

Why Does Microsoft End Support for its Products?

In brief, so that they can focus their investment on supporting newer and better technologies and improved user-experiences. It also helps their bottom line.

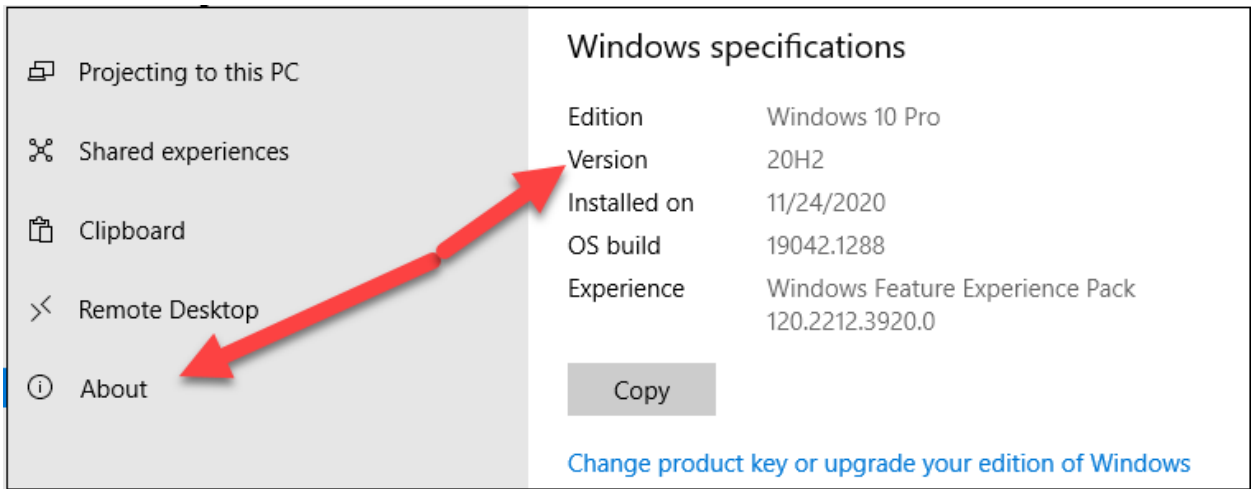
Here's a list of some of the most common products and their end-of-life dates. You'll notice some of these have already passed their "use by" date. Clients using these products really need to either update (if possible) or replace these systems. You will find a complete list, by year, on Microsoft's website here.

If you are a TekResults Preventative Maintenance Plan client, you already know we access all your systems every quarter and make suggestions for updates and replacements as needed.

Product	**Date Support Ends**
Windows 7	Jan-20
Server 2008 / 2008 R2	Jan-20
Internet Explorer 10	Jan-20
Share Point 2010	Oct-20
Office 2010	Oct-20
Lync Server 2010	Apr-21
SharePoint Server 2010	Apr-21
Project Server 2010	Apr-21
Windows 10, version 1809 & 1909	May-21
Skype for Business Online	Jul-21
Internet Explorer	Jun-22
SQL Server 2012	Jul-22

Note that the Windows 10 in this list is for versions 1809 & 1909. Hopefully, your version of Windows is not that old. If you have not disabled Windows update, and updates happen with regularity, you won't need to be concerned about this, but if you want to check which version of Windows 10 you are using, follow these steps.

1. Click **Start**
2. In the far-left panel of the **Start** menu, click **Settings**.
3. Open **System**.
4. Scroll to the bottom of the left panel and click **About**.
5. In the right panel, under **Windows specifications**, look for **Version**.



Here is the list of Windows 10 feature updates in order. If your version is older than the 2004/20H1 version, your version of Windows is already out of support. By the way, **2004** does not represent the year 2004. It stands for the year and month the update was released 20**20** and **04** (April). And as if this wasn't confusing enough, the marketing name calls it *May* 2020 Update and not *April* 2020 Update. Don't try to figure it out, just go with it. Thanks Microsoft!

Version	Codename	Marketing name
1803	Redstone 4	April 2018 Update
1809	Redstone 5	October 2018 Update
1903	19H1	May 2019 Update
1909	19H2	November 2019 Update
2004	20H1	May 2020 Update
20H2	20H2	October 2020 Update
21H1	21H1	May 2021 Update
21H2	21H2	November 2021 Update

I thought you said

When you see that the 1809 and 1909 versions have reached the end of their life, you may protest "I thought you said Windows 10 will be supported until 2025".
We did, and it will. However, Microsoft factors in the Windows feature update version as part of the equation when supporting Windows 10. The current version of Windows 10 (21H2) is not the same

Windows 10 as the 1909 version. Frequent and ongoing updates has distanced the current version from the version of 2 years ago so much so that Microsoft will no longer support the 1909 version.

Windows 10 feature updates vs quality updates

Microsoft releases quality updates about 4 times a month. These updates contain bug fixes and vulnerability fixes, among other things.

Microsoft releases feature updates twice a year. These feature updates are the ones that get the fancy designations like 21H1 and 21H2 (see the list above) and typically include new features, visual improvements, and significant enhancements to improve the overall experience and security of the system. Microsoft only supports a feature update for 18 months. That's why you still have Windows 10 being supported till 2025 and systems running the 1909 feature update now out of support. Here's a great article with more information about feature and quality updates.

We're investing in tools to serve you better

At the beginning of the Covid 19 pandemic TekResults decided to invest in a solution that would allow us to monitor the health of all our Preventative Maintenance Plan client's servers, workstations and laptops remotely. We knew it would be increasingly more difficult to visit our clients in person due to the limited visitation rules most businesses were beginning to enforce, and we were unwilling to be sidelined in our commitment to outstanding service by a little thing like a global pandemic!

As we began to look for a system to aid us, we had three clear objectives. The perfect system would:

1. Display the health of each system we service (and there are hundreds of them) in an online dashboard.
2. Send automated alerts to us if there are issues with any of these systems.
3. Allow us to connect to each system remotely to fix problems clients might be having and to perform routine maintenance.

In short, what we were looking for was a good **RMM** system. The platform we decided on was **Atera**.

ATERA

Atera is an IT management solution that enables monitoring, management and automation of hundreds of IT networks from a single console. Atera provides RMM services.

What is RMM

Remote monitoring and management (RMM) is the process of remotely monitoring and maintaining IT infrastructure. RMM software is mostly used by managed service providers (MSPs), like TekResults, to manage their clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agents. It enables them to control their clients' IT operations without setting foot on-premises.

How does RMM work

Deploying RMM requires an agent, which is lightweight software installed on client servers, workstations, networking devices, laptops and all other devices connected to the network.

This agent allows technicians to get real-time insights on the health of the client's IT environment. It also enables them to control and monitor remote devices.

The RMM agents can connect without VPN and firewalls, hence when you install an RMM agent onto a device, the RMM platform can recognize it from anywhere, allowing technicians to control devices remotely.

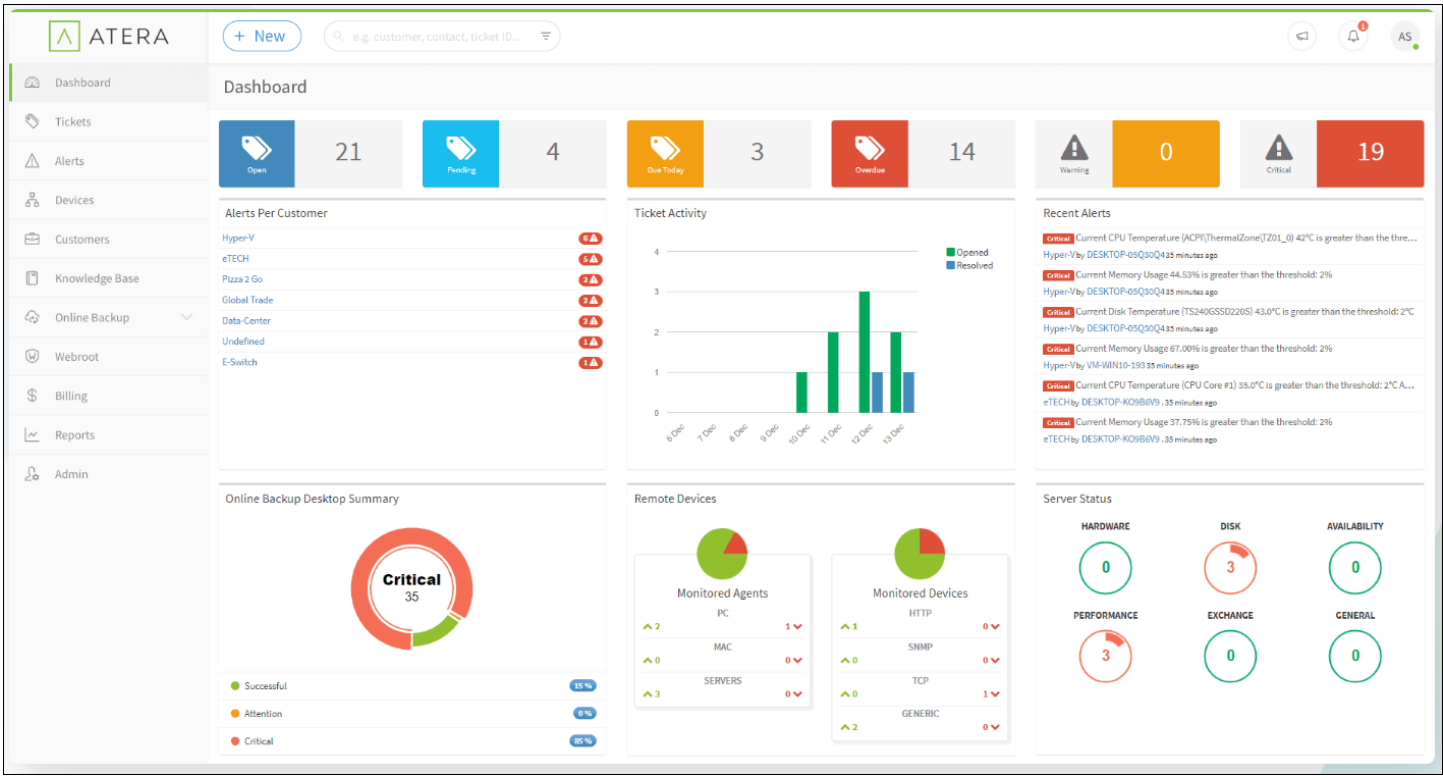
What Does RMM Software Do?

Here are few core functions of modern RMM tools:

- Real-time monitoring and alerts management
- IT automation and scripting
- Reporting and analytics

Real-time monitoring and alerts

We believe our clients shouldn't have to wait for something to break down before the support team spots a problem. Atera allows us to know about potential problems so that we can fix them before they grind the client's business to a halt. The screenshot below shows the Atera dashboard as it monitors all the systems belonging to multiple clients and presenting recent alerts, server status and hotspot areas.



This screenshot shows the details for a single Atera-managed system.

☆ DESKTOP-[redacted] Home Laptop

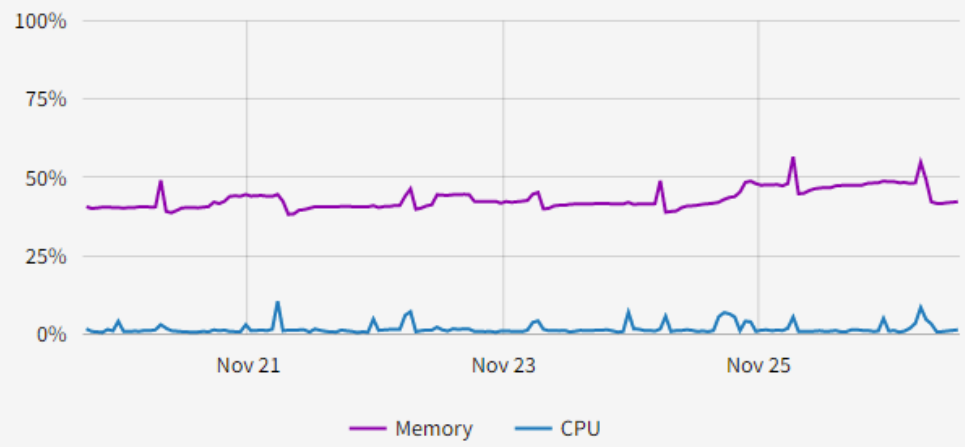
Online | Connect | Manage | Edit | Create ticket

Machine Name	DESKTOP-[redacted]
Workgroup	WORKGROUP
Availability Monitoring	Disabled Edit
Last Seen	Nov 26, 2021 12:58:43 PM
Last Logged User	DESKTOP-[redacted] (Since: Nov 10, 2021 11:31:27 PM)
Last Reboot Time	Nov 10, 2021 11:31:00 PM (2 weeks ago)
IP Address	[redacted]
Customer	[redacted]

0	0	0
0	8	0

Metrics

Memory Average: 43% | CPU Average: 2% | Last week



Profiles

Threshold Profile Manage
TekResults Client PC

IT Automation Profile Manage

Alerts Pause alerts

No alerts to display

Software

OS Edition	Microsoft Windows 10 Home x64
OS Version	20H2
OS Build	19042.1348
Office Version	Microsoft Office 365 Business x64, Build 16.0.14527.20276

Security

Antivirus
Active — Avast Antivirus

Anti spyware
Active and Updated

Hardware

Vendor	LENOVO
Model	81TE
Serial Number	R90[redacted]
Motherboard	LENOVO LNVNB161216
Processor	Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz - 6 cores
Memory	16 GB
Video Card	Intel(R) UHD Graphics 630
Sound	Intel® Smart Sound Technology (Intel® SST)
System Drive	C
MAC Addresses	A4:B1:C1:D[redacted] (Primary) A4:B1:C1:[redacted]

Disks

Total Capacity (17%)

IT automation and scripting

Atera provides both automation and scripting tools. Some automated tasks include:

- System Restore Points
- Temp Files Deletion
- Internet History Deletion
- Reboot
- Shutdown
- Defragment (all disks)
- Run Checkdisk (all disks)
- Run Scripts

Most of our clients enjoy a TekResults service contract (AKA Preventative Maintenance Plan), which includes, among many other services, a quarterly check up on all servers, laptops and desktop systems. In the past, we would visit each business quarterly and check the health of every system manually. Now, with many people working from home, these personal visits are not always possible, however using Atera's tools, we have been able to automate many of the things we used to do onsite.

Reporting and analytics

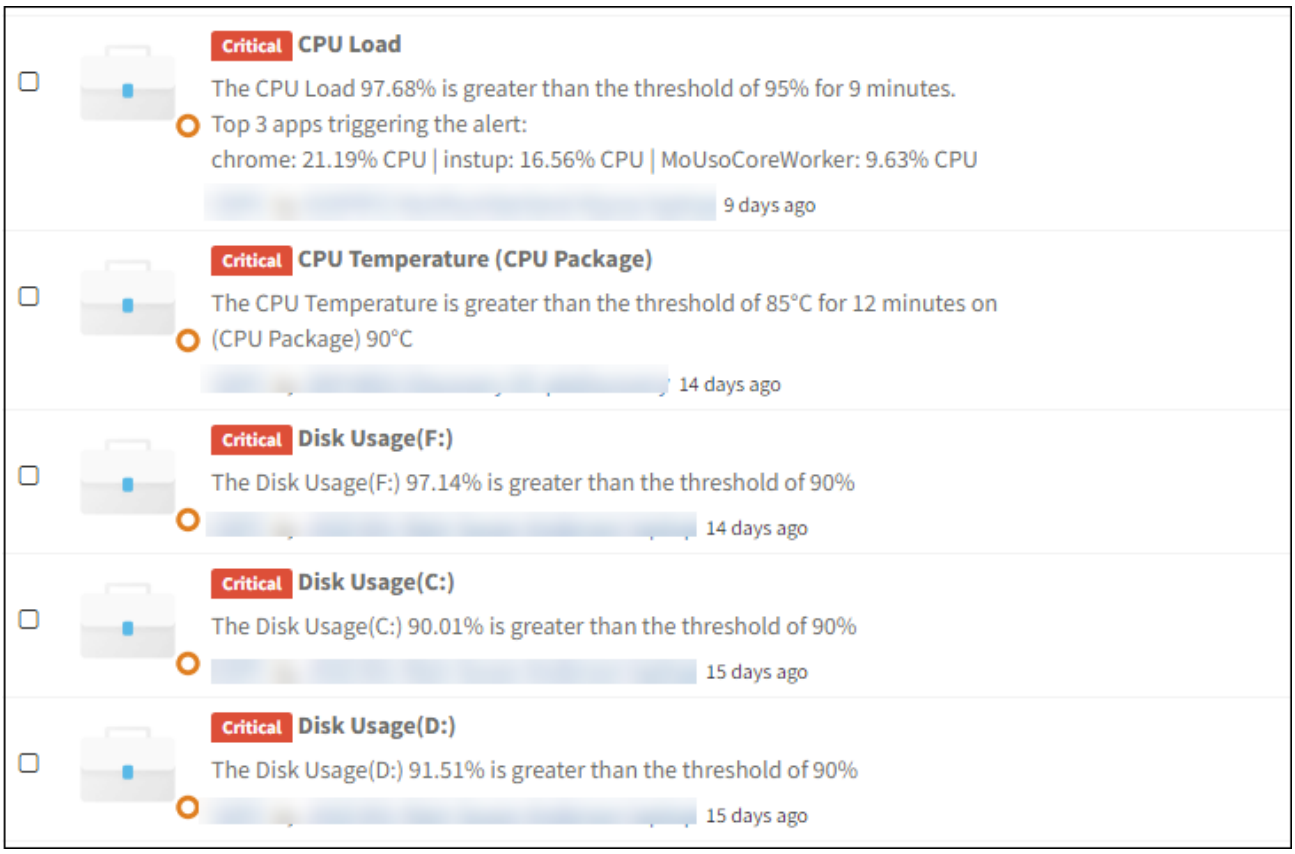
Atera doesn't just perform monitoring tasks, it also includes extensive reporting options such as:

- System health at a glance
- Specific customer health
- Agent health
- System inventory audit
- Microsoft licensing
- Software inventory
- Patch and automation feedback

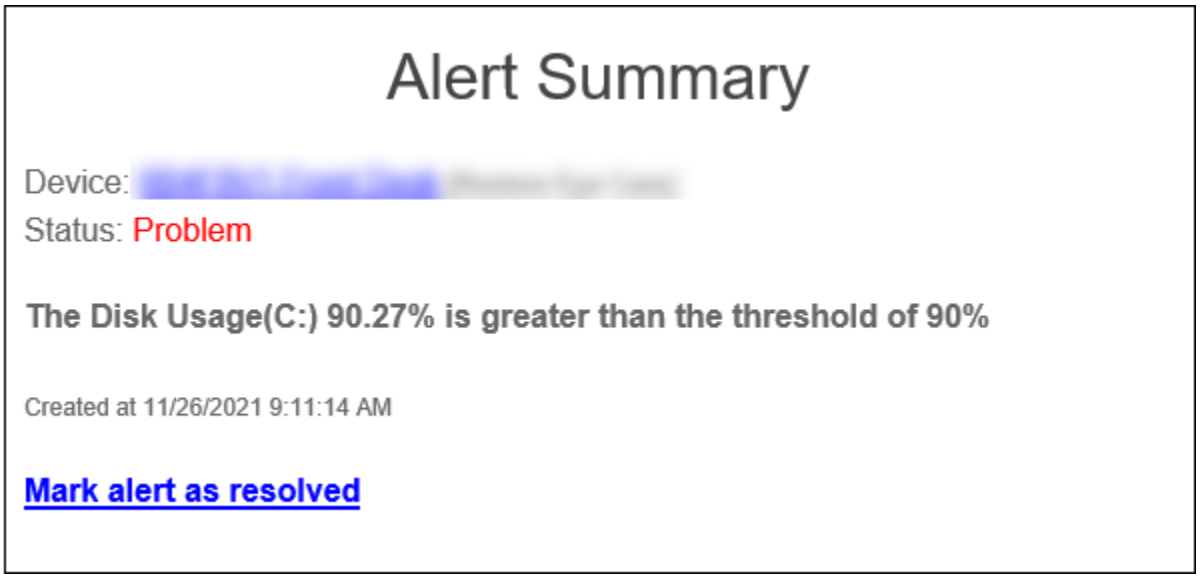
Alerts

Atera sends alerts to TekResults's technicians on a variety of issues that help us stay ahead of problems instead of simply reacting after the fact. Each day we receive these alerts both as email notices and within the Atera dashboard. These alerts let us know if a computer we manage is overheating, using a lot of memory, has a full hard drive, as well as many other issues that, if left unattended could cause problems. By now, many of our clients are familiar with these alerts because, when we receive one, we pass it on to the client along with our recommendations.

Below we see a list of alerts as presented in the Atera dashboard.

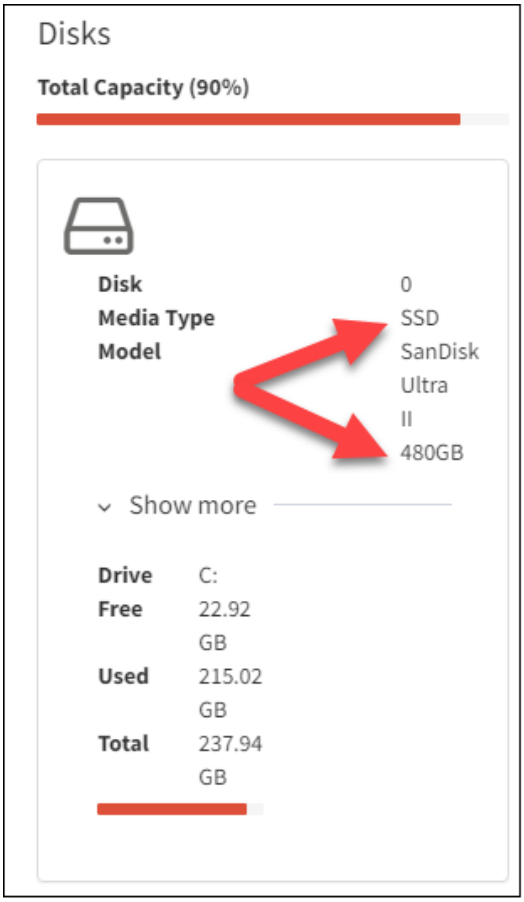


And here we see a disk usage alert for a single system as it was sent to us through email. It tells us percentage of the hard drive that is used (90.27%). The device (blurred out) tells us the name of the device and the client it belongs to. This alert came in as this article was being written.



Looking this system up in the Atera dashboard, we found the system is the receptionist computer at a small office and the disk in question is a 480GB SanDisk solid state drive (SSD). That's a relatively large

drive and we have to wonder what is causing it to fill up. Our next step is to reach out to the client and ask them if there are some large files that are candidates to move to external storage or to the server. If not, do they need a larger hard drive.



Remote access

Many of things we do to keep our clients' systems healthy can be done right from within the Atera dashboard, but sometimes we need to actually sit in front of a client's computer to do some old-fashioned troubleshooting. In these cases, Atera makes it possible for our technicians to "remote in" to the client's system and see what the client sees. The ability to fix problems remotely ensures that clients don't have to wait for us to schedule a visit to the workplace. Help is only minutes away. This arrangement allows the user to demonstrate whatever problem they are having and for the technician to be able to work with the user directly.

All this functionality does not come for free. However, we have been able to squeeze the extra cost into our Plan pricing with no extra costs to our Preventative Maintenance Plan clients.

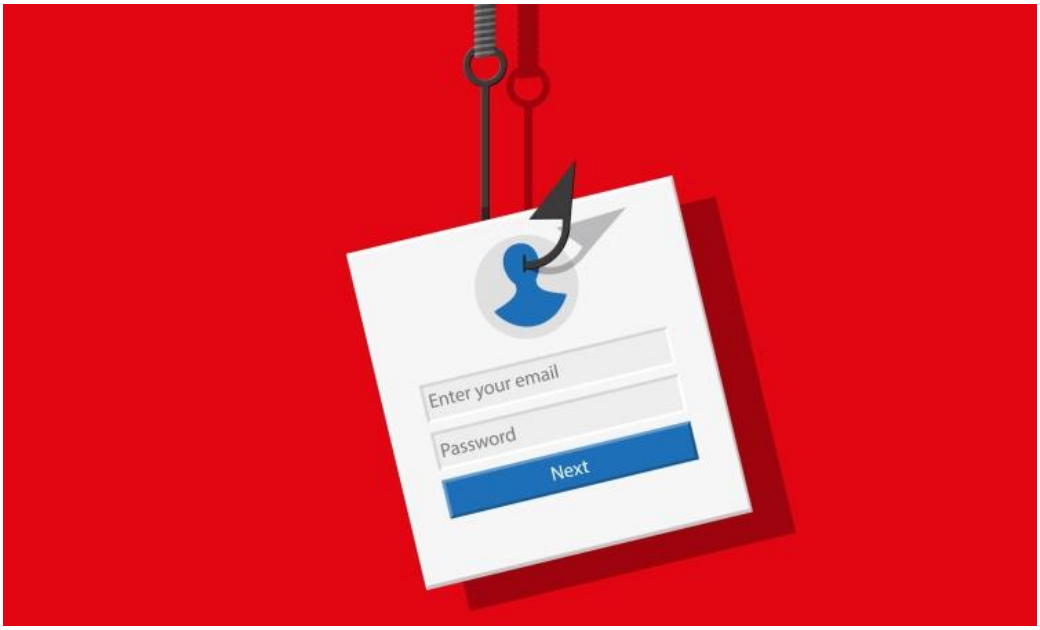
Atera has made it possible for TekResults to continue to provide the same excellent service we delivered before the pandemic and then some. With the powerful Atera monitoring and reporting tools, we are

now able to offer a proactive approach to potential issues and a faster solution for the home workforce, making us an even better IT partner for you.

Currently only TekResults clients with a Preventative Maintenance Plan are eligible for use with Atera, but if you'd like your business to become a service customer, we'll be happy to discuss it with you. Give us a call at 814-206-0000 or email us at info@tekresults.com.

Phishing lessons

How to avoid accidentally giving away the keys to your online identity



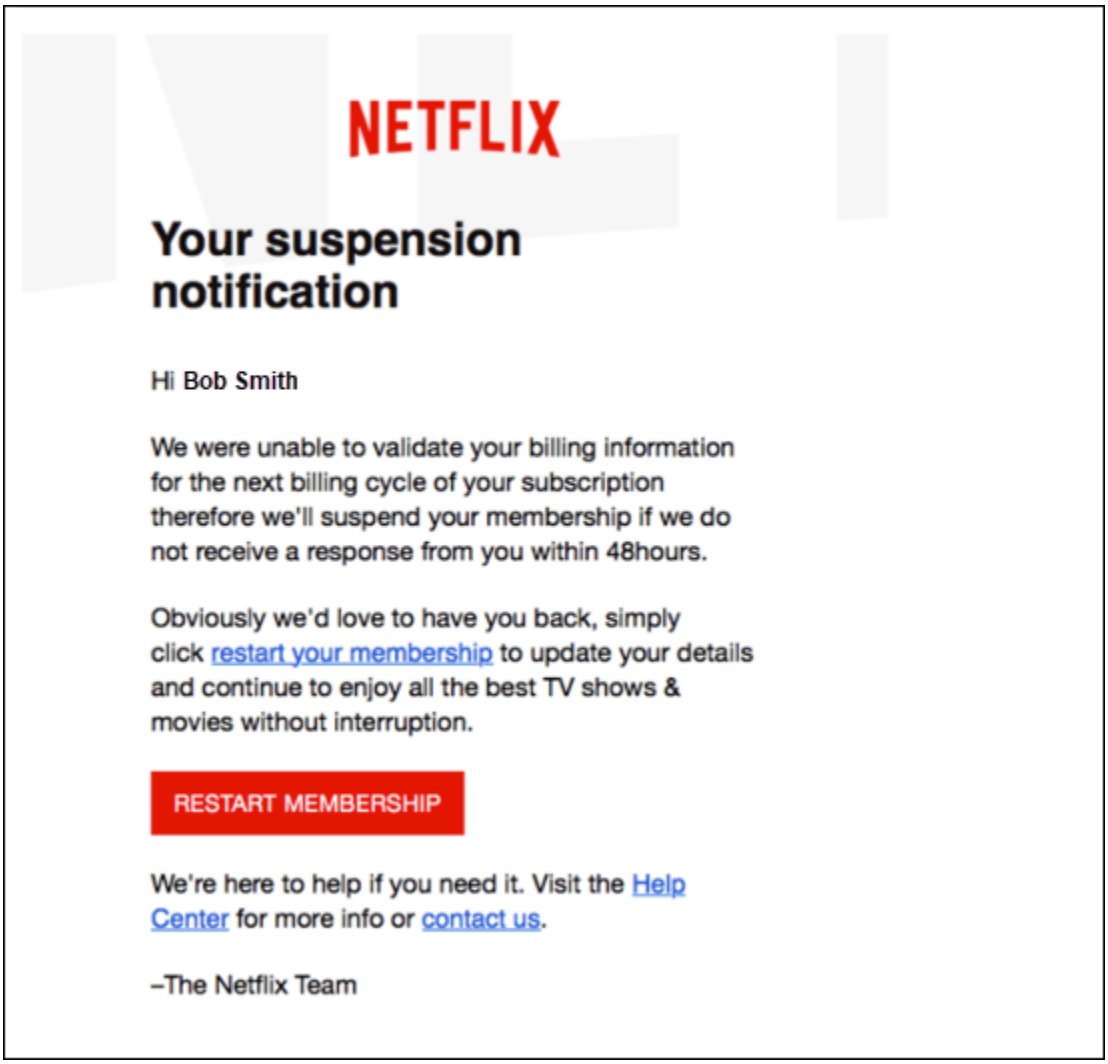
Many of us have seen movies and TV shows that feature computer hackers using elaborate methods to gain access to someone else's data. They sneak through firewalls, trap passwords, use hidden cameras and fancy key cards and keep us entertained with their antics. However, the sad truth is that all these dramatic efforts are rarely necessary. Most cyberattacks depend more on the frailty of people than the weakness of security devices and are much more easily implemented using email and texts that contain malicious content.

Attacks that use this method are referred to as *social engineering* - the deception and manipulation of human beings to convince them to willingly provide sensitive information or click on a corrupt link. Social engineering employs many methods, but the most common is phishing.

As its name implies, cybercriminals send malware to email addresses in hopes that someone will respond. The bait they use is typically in the form of a message that appears to come from a legitimate source, such as a bank or a security company or, every often, Microsoft. The messages contain a reason to catch your interest (Your account is overdrawn, your computer has a virus, etc.) and a link to log into "your account" to get more information or to resolve the issue. The link, of course, does not really go

where advertised, and instead takes you to a website that convincingly looks like the site you expect to see. Once you "log in", the bad guys have your credentials.

If you are a Netflix subscriber, wouldn't you be tempted to respond to this message? This is a copy of an actual phishing message sent out by cybercriminals. It was reported by Today as a warning to Netflix subscribers. Email recipients received personalized notices informing them that their billing information needed to be updated and they must "restart their membership." The bogus email includes a link to a fake Netflix website that asks users to log in and then enter various types of personal information.



Why is phishing so successful

The FBI reports that in 2020 there were more than 241,000 reported phishing victims. It's important to note that many victims of cyberattacks don't report these crimes to the FBI or any other agency, so this figure is surely lower than the actual number.

One of the reasons phishing is such a pervasive type of attack is it exploits universal psychological vulnerabilities. Who would not be tempted to respond to these subject lines?

- Official Data Breach Notification
- Your password expires in less than 24 hours
- Attempted login to your account
- Billing information is out of date
- Dropbox document shared with you

Here is a list of others you and your coworkers should be aware of.

In addition to tempting subject lines, cybercriminals typically try to intimidate victims by presenting themselves as representatives of a legitimate entity. Here is a 2020 report from F5.com that finds that 55 percent of phishing sites used recognizable brand names and identities in their URLs. For example, what's wrong with these URLs?

https://login.micorsoft.com
https://freeoffer.capitalone.zza.com

In the first example, **Microsoft** is misspelled and who knows where this will actually take you. In the second, the domain is **zza.com**, so even though it has *capitalone* in the address, it is not associated with Capital One. Sneaky.

Case study

Three weeks ago, one of our clients reported a break in. A cybercriminal had gained access to his email account at Microsoft 365 and had sent out email invoices, as the legitimate user, to that user's business associates. Because the hacker had complete control over our client's email account, he also set up inbox rules that moved messages that were received from those business associates to a folder, where our client would not think to look. This way if the hacker got a reply from the messages he sent out, our client would not tumble to them easily.

Our client caught this pretty quickly, because one of the business associates the hacker targeted worked for the client and she asked him about the bogus message. In taking emergency action, the client had to close his bank accounts and set up an audit of those accounts. Although he acted quickly enough to avoid losing money directly, the time and inconvenience of having to scrutinize all his financials made this a costly attack. And, of course, it could have been much worse if not caught right away. Kudos to the employee who questioned the bogus email and to the client for taking immediate action. He called us.

Steps taken to mitigate the damage

1. When the client notified us of the possible break-in, we immediately changed his email password, cutting off the hacker's access to his account.
2. We launched a security audit of his account. One of the things that makes Microsoft 365 such a great product is their focus on security, and to that end, they provide great security tools. Using 365's tools, we were able to do a message trace for the client that showed all messages that had been sent from his account, who they were addressed to and whether or not they were delivered. This provided the scope of the attack.

3. Next, we used 365's tools to audit the login log for the account. This showed the IP addresses from which all logins originated. We could see most of the logins were from the client's own IP address, but several addresses originated in Nigeria.
4. We checked with the client's customer service provider to make sure his email hadn't been blacklisted because of suspected spamming activities. It hadn't been because the hacker did not use the client's email to send thousands of spam messages, as is usually the case. This bad guy targeted just a handful of the client's business associates, not enough to cause a red flag.
5. Finally, with the client's permission, we configured his company's domain to not allow anyone with an IP address originating outside the US to log into any of his company's email accounts at office.com.

How did this happen

These steps were all good, but they were reactive steps and couldn't fix what had just gone before. Naturally the client felt violated and probably a bit overwhelmed. He asked us "How could someone have guessed my password".

We don't think someone guessed his password. According to an article published by LastPass "When hackers are trying to get passwords, they don't guess them one by one in a password field. Instead, they have a toolbox of software programs and databases to help them figure out credentials that might work.

First, most passwords that hackers have access to are stolen in large data breaches from popular online services. When popular services like LinkedIn, eBay, and Adobe have millions of records leaked, the passwords stolen in those breaches are compiled in large databases. Less well-known websites are also regularly hacked due to poor security protocols. So, what do hackers do? They use these "dumps" of data to perform "credential stuffing", where they use software (or "bots") to automatically test every username and password combination in the database to see if any successfully log on to another website (like a bank).

Or, if a hacker knows an email address for a user's account, they can use "password spraying" where they test known passwords (like 12345 and asdf) to see if any work with that particular email address. Again, bots are running these tests, and only if a match is found does a hacker then use the valid credentials to try taking over the account."

We explained to our client that if the hacker didn't use one of these methods, it's possible he, the client, had responded to a phishing campaign and didn't realize he had revealed his credentials.

If you'd like more information about phishing, the Federal Trade Commission has a good site here.

One of the things you can do to protect your company from phishing attacks is to provide professional training for your employees. Our partners at KnowBe4 offer security awareness training that helps your users know how to respond to today's sophisticated phishing and ransomware attacks. If you would like more information or would like to schedule a KnowBe4 demo, give us a call at 814-206-0000 or email us a info@tekresults.com.

Is your network gear as good as it should be?

Not so long ago, maybe 10 years or so, all a home network had to do was allow your phone and tablet to connect wirelessly to the Internet, a modest requirement. But, boy have times changed!

Today we need enough bandwidth to power Netflix, Disney+ and other streaming TV services, video calls on Zoom, laptops, smartphones and tablet Wi-Fi, video gaming, smart-home devices (doorbells, smart thermostats, lights), voice assistants like Alexa, and more. According to Google's Connected Consumer Survey, US households own an average of 11 connected devices.

If you live alone, you probably still don't have as large a requirement as a large family, but if you start seeing the buffering message when you're streaming movies, and if your downloads take a long time, it's time to beef up your home network.

Here are some tips for making things go faster!

The devices on your home network are only as fast as your Internet connection

People who live in the country and outlying areas may not have as many options as those in more metropolitan areas, but many towns have more than one Internet service provider. Many places offer Verizon and Comcast, or even a local cable company. Shop around and see what plans these companies offer. Most providers change their plans every year or so as the technology improves and they invest in faster equipment. See if you can upgrade or switch your current plan. Chances are your current company will increase your Internet speed and even give you a reduced rate for the first few months as you move to a new plan. It is usually easier to do this if you are at the end of a service agreement period.

Get a faster modem/router

Your modem is a box that connects your home network to the wider Internet, usually given to you by your ISP (Internet Service Provider).

A router is a box that lets all of your wired and wireless devices use that Internet connection at once and also allows them to talk to one another without having to do so over the Internet. Often, your Internet service provider will give you one box that serves as both modem and router, but they're still different technologies; not all modems include routers and not all routers have modems. You need both, integrated or not, in order to provide an Internet connection for all the devices in your home.

If the box your ISP gave you does not provide Wi-Fi, then you most likely have had to purchase a wireless router from a third party such as Amazon or Best Buy. If you modem and/or router is older than 7 years, it is most likely outdated and should be upgraded. We have modern routers and other equipment that will allow access from many devices.

Mesh networks help spread the load

If you have a larger home, if you have lots of smart devices in addition to your computers and phones and streaming boxes, or if your router has to sit far away from the center of your home, a Wi-Fi mesh-networking kit is the way to go. Good ones start around $250 and go up from there. These kits usually come in two or three pieces, with one piece that functions like a stand-alone router and one or more pieces that act as satellites. Place each satellite in between your router and an area of your home with a poor Wi-Fi signal, and it will act as a go-between, increasing the range and improving the quality of your entire wireless network. One of our clients, whose ISP is Atlantic Broadband, recently upgraded their service plan and AtlanticBB sent them a new mesh networking kit as part of the upgrade (at no additional cost). But if your ISP isn't that generous, you can still buy a Mesh kit. We can help you with this purchase.

Businesses need to be aware of changing technology too

We've been talking about home networks, but business should also look into upgrading aging network gear. Many of the best advances are offered to businesses first and a quick call to your ISP to find out what upgrades are available would be a great idea. Most business ISPs now offer gigabit speeds and will provide the modem/router (usually referred to as a gateway) to bring those speeds into your business.

Of course, once you have gigabit speeds coming into the building, you will also need to assess the gear that spreads those speeds through your business. Many older routers and switches are not capable of providing speeds faster than 100Mbps (megabits per second); gigabit speeds are 10 times faster than that. Typically that means investing in some new gear, but the cost of these changes is not normally prohibitive. A new router and switch can normally be purchased for around $1500. Used devices are considerably less costly.

The point is that better, faster Internet is available, and a few phone calls could make all the difference to your business. You can start by calling us at TekResults. We will be happy to assess your network and make recommendations. Our assessment is free. We'd be happy to visit your business at no charge and help you find the perfect fit between speed and cost. Our preventative maintenance clients are already enjoying this benefit and we'd be happy to provide references for you to talk to.

Give us a call at 814-206-0000 or email us at info@tekresults.com. We'll be standing by!

Our partners

TekResults doesn't just work with networks and computers; through our partners, we also provide security training, phone sales and other vital services.

KnowBe4
Human error. Conquered.

KnowBe4 is the world's largest security awareness **training** and simulated phishing platform that helps businesses manage the ongoing problem of social engineering. When business managers and IT

departments are busy tending to day-to-day operations, who has time to train the staff how to avoid the many phishing scams and security risks that target them each day? This is where KnowBe4 comes in. With their award-winning, on-demand, engaging, interactive browser-based training, KnowBe4 trains at each staff member's pace by providing online simulations and fun quizzes, all designed to keep the workforce sharp and on the lookout for the bad guys who would take advantage of them.

As ransomware attacks become more common (see our article elsewhere in this newsletter), TekResults is no stranger to dealing with the aftermath of these devastating attacks. We know the best first defense against ransomware viruses, or any virus, is a great antivirus program. Avast, a global leader in digital security and privacy, has recently released new versions of its security products to address the recent global surge in coronavirus-related ransomware.

In recent years, Avast has monitored a rise in attacks specifically designed to exploit Remote Desktop Protocol (RDP) in order to execute widespread ransomware attacks. In March 2020, at the peak of the pandemic lockdown, Avast observed a 20% increase in these types of attacks globally. With millions of workers around the world using RDP daily to remotely access their business network, this tool has become a strong cyber-attack vector.

As our client's come to the end of their subscriptions with other antivirus products, we will be recommending they change to Avast. If you have a preventative maintenance plan with us, we will notify you a couple months before your current antivirus expires. If you don't have a plan with us, not to worry. We'll still be happy to discuss making the change with you.

With much of America's workforce working from home, finding the right product to safeguard our client's from instability introduced by home routers has become a priority.
SonicWall delivers Boundless Cybersecurity for the hyper-distributed era in a work reality where everyone is remote, mobile and unsecure. SonicWall safeguards organizations mobilizing for their new business normal with seamless protection that stops the most evasive cyberattacks across boundless exposure points and increasingly remote, mobile and cloud-enabled workforces. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide.

Voiply provides simple and reliable phone solutions to business, allowing the cost-conscious manager to replace their old analog phones with Internet phones that are feature-rich and affordable.

In 2012 VoIPLy was founded with a big agenda. They saw the market change and that companies were going to need to communicate in a faster and more efficient way. They understood then that the "Cloud" was not a phase but in fact was the way of the future. So they developed a cloud based unified communication system that utilizes the latest technologies. They wanted to be not only a part of the change but in the forefront of servicing SMB's around the globe. Their hard work has paid off. Over 5,000 companies now trust VoIPLy Cloud Phones and they have just begun. With VoIPLy, businesses can simply operate and migrate over to a powerful, feature filled, and compliant phone system. You don't have to be an expert to set up one of our hosted phone systems. They've made it easy and affordable.

TekResults has helped many of our clients cross over from expensive POTs (Plain Old Telephone) systems to Voiply and we'd be happy to provide our expertise to you as well.

If you'd like to discuss revolutionizing your phone system, or would like to discuss any of the other products we've mentioned, please call us or shoot us an email.

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 administration
- Network troubleshooting
- Business consulting software testing and service
- 3rd party software setup and support
- Computer security solutions (including PGP, encrypted mail, secured transactions)

- Network cabling
- Security compliance review HIPAA
- Security compliance review PCI
- System installations
- System upgrades
- System auditing / documentation
- Desktop, laptop and monitor and other sales
- Custom application development
- Legacy system migration and rewrites
- System integration
- Application integration
- Network installation and integration
- Training and staff development