BLUE BEAR TAX

Team Member IT Playbook

Best practices for support

Every computer at BLUE BEAR TAX is well looked after by ITGuys Team. Normally, we work in the shadows keeping your technology doing its thing without you having to hear from us. But every now and then something comes up that requires more hands-on attention. Below is a list of guidelines and information about your technology and how we provide support!

Computers:

While we don't view what you're working on, we do keep track of your computer's vitals (e.g. available updates, security patches, system usage, battery life expectancy, serious alerts, EOL data, and extended warranty information). If your computer isn't performing the way you're expecting it to, let us know and we'll perform a health check.

NOTE: Even though there may be extra computers at the office, it's not a good idea to use a different one without a thumbs up from a manager first, even for short-term use. Most computers that have been previously decommissioned are not being regularly maintained, and as such are vulnerable to security issues.

Labels:

Each computer has a label, and each associated power cord has a label. The label on your computer identifies the machine you're using and has a website address for your team to get support for that computer when needed. If your label falls off or wears out over time, that's okay, just let us know and we'll print a new one. Your label has the asset number of your computer, and the address of your support portal.

Power Cords:

The specific power cord that came with your computer is like your computer's lifeline, the wrong one can lead to chaos. While other power cords may fit physically, a mismatch in voltage can make the computer act funky or damage it over time. Need an extra cord? Let us know and we can order one for your specific computer. Also, it's a good idea to unplug your computer during a lightning storm. Lighting strikes can affect electronics up to 3 miles away, even on fancy surge protectors.

Getting Support:

Getting support is a breeze. The label on your computer has a website address that leads to a support portal for your team to submit trouble tickets and book appointments. You can also submit a ticket by emailing support@itguysteam.com or if it's urgent, please give us a call at 303-578-6256 (9-5 Monday – Friday). After-hours support is available upon request as well.

Support Portals:

Support portals are customized around the way your team works best. On your portal, you'll find important documents, training videos, ticket submission portals, etc. If you'd like a change made to your portal, please let your office manager know. Support portals are also where you will book remote or onsite appointments at your convenience.

Submitting Tickets:

Computer issues generally break down into a few categories; hardware, software, internet gremlins, and fire. Most times you will be experiencing software woes (e.g. email challenges, Windows freezing, slowness, etc.) However, some issues can be early indicators of something else. For example, if something only happens occasionally it may not seem that big of an issue. It's important to note that small issues can indicate much larger problems that aren't always easily detected and can become catastrophic if not remedied. Your best bet when encountering an issue in most cases is to first try a restart if possible and then submit a ticket through your support portal if the problem persists. We'll often be able to resolve most non-emergency tickets remotely if they're received before noon on the same day. After noon, tickets are generally resolved by the next morning.

Submitting tickets to our team directly is generally more efficient than asking a manager to help resolve a technical issue. When a ticket is submitted through your support portal or by emailing support@mynewitguys.com, you should receive an email verifying the ticket has been received, plus updates via email on the status of your ticket. Email is our preferred method of communication, however sometimes the email can end up in SPAM if a flag is triggered. If you haven't had a response to your ticket in a while, check the SPAM folder.

Magic Words:

We generally work as fast as we can to resolve your computer challenges in addition to all the other companies we help around the World, but nothing gets us moving like the 4 magic words. Those words are:

"This is an emergency"

Saying those 4 words, in that order, stops all other support tickets for everyone on our team, and puts all hands-on deck to focus on whatever issue is going on for you. We try to handle most issues before they blow up, but that doesn't mean something unexpected can't happen at the last minute.

Remote Sessions:

We're committed to providing fast and efficient support that works best for you. If it's determined that a remote session is necessary after a ticket has been submitted, we'll arrange a time with you to work on your computer (with you present unless otherwise specified). It's a good idea to allow at least 30 minutes per remote session. Even though a request may seem like a "small problem," it's general policy for us to look through the event log of every machine we touch to look for issues and apply maintenance scripts just in case.

NOTE: If you see your mouse moving randomly as if someone is performing a remote session you weren't prepared for, shut down your computer and contact us at 303-578-6256. (This is not common.)

On-site Support:

While on-site support is available to anyone at any time if requested, we have general maintenance scheduled every week (currently Thursdays) to provide preventative

maintenance for communal computers, perform non-time sensitive repairs, check on inventory if needed, and note any issues that we find for future maintenance. Feel free to flag us down if you have any questions or need anything.

Monthly Projects:

Each month we have a different scheduled IT maintenance project. Sometimes these projects are performed on- site at the BLUE BEAR TAX offices and they're generally performed by different technicians than the dedicated support professional you're used to (we'll give you a heads up if that happens, so you're not surprised.) These "other technicians" are normally assigned to a specific task and while they may be able to assist with an IT issue, largely they're focused on performing whichever operation they've been assigned and may not be prepared to assist with general issues. It's always best to submit a ticket.

Wi-Fi:

We take information security very seriously. That said, please don't use free or public Wi-Fi. This includes planes, hotels, airports, coffee shops, or conferences. That's how bad things happen to good accounts. If you need access to the internet, most phones are equipped with hotspot access. For frequent flyers, a cellular modem might be a good investment. We also have cellular modems available to borrow for extended stays. If it's an emergency, try to refrain from logging into any systems where a username and password is required (e.g. email, bank info, etc.). The reason being is that it's terrifyingly easy to scrape username and password info from a public network.

Lost/Stolen Computers:

Each computer is encrypted with bit-locker, so your data is safe (for now.) And our tracking software gives us the ability to locate the machine once it pops up online that can be used in a police report, and/or remotely wipe it. Just let us know as soon as possible if you notice your computer is gone and we'll set an alert.

Passwords:

Passwords to important systems should be changed every 90 days and ideally not written down. Also, if it can be avoided, it's best not to use the same password for multiple accounts (that's how most hacking happens). For those that have many passwords to keep track of, password keepers like LastPass and 1password work greatly. We also have a SOC2 secure password tracking system included in your support for all covered users available on request.

It's also a good idea to use 2FA wherever possible.

Training:

Computer software keeps changing all the time, and not just from one version to the next either. With online platforms, features and functionality can be moved or taken away in a moment and you may find yourself needing a refresher course on a program to restore functionality back to a smooth workflow. Don't hesitate to reach out if you have any questions.

Secure File Sharing:

When it comes to sharing important files. We want to keep data locked down tighter than a bank vault. OneDrive is fine for sharing most company files, but for sensitive information that you wouldn't want to end up in the wrong hands, it's best to use a secure transfer system like share file (available in your support portal.) USB drives are not a good idea to share files with, but if you absolutely must, they can be encrypted and decrypted with BitLocker to secure them during transit.

Updates:

Our software keeps track of your computers and lets us know when there are mission critical updates or security patches available. When an update is needed, we get an alert ranging from mild to critical and apply patches and updates via PowerShell as necessary (so you will never see us working on your machine.)

You may see an update pop up for a software or hardware device on your computer, but it's important to note that not all updates are beneficial. In some cases, an update is released

too soon and can cause more harm than good. Other times an update is released that takes away features than the previous version. Most automatic updates for windows are generally safe. Issues with hardware can crop up when an unexpected glitch is found after a driver update is applied where one wasn't needed. It's best to leave that part of life to us.

Smart Monitor:

The software on the smart monitor in the networking closet lets us know if there's any unwanted malicious activity on your network and pings us if the network is offline for more than 5 minutes. In that case we'll swoop into action and work with the ISP to get the internet back online. In very rare circumstances where the internet will be down for an extended period (e.g. a scheduled maintenance, serious outage, etc.), we have cellular modems available that will keep your network online (minus printers).

Firewall:

The firewall on the network sends us reports of possible attacks and provides VPN access to the office from outside the network perimeter if you need to access an office resource. (e.g. if you wanted to print something at the office from home.) The VPN for your network can be set up at any time upon request.

Microsoft 365:

Microsoft 365 reports when there is a spike in reported SPAM, however it doesn't keep track of spoofed or fake emails. The security for BLUE BEAR TAX is turned up as high as it goes on Microsoft 365, but spoofed or fake accounts can still get through on occasion (nothing stops it entirely). BLUE BEAR TAX is a sizable target for tricksters (for various reasons) and every now and again a message of sorts will get through. This can be in the form of a free email account with someone from BLUE BEAR TAX's name on it. Sometimes a hacking attempt can come in the form of a text message (it's shockingly easy to spoof a phone number.) In very rare circumstances the email will look like it came from someone with an BLUE BEAR TAX email account (NOTE: this is not common). Often the people will be making an odd request for gift cards, or an invoice payment. The unfortunate price of having access to digital communication is constant vigilance. Methods of social engineering change all the time (read: getting more effective) and it's best to double check with someone verbally if you're unsure about something. If you receive an email like this,

please don't delete it. Just let us know and we'll take the necessary steps to prevent others like it from getting through.

Google Workspace (formerly G-Suite):

Google Workspace alerts us when there's a spike in reported spam, but it doesn't fully track spoofed or impersonation emails. While we've configured BLUE BEAR TAX's security settings to the highest possible level within Google Workspace, fake or spoofed emails can occasionally slip through (no system stops them entirely). Due to BLUE BEAR TAX's visibility, we are a frequent target for phishing attempts.

These fraudulent messages may appear as:

- Free email accounts (Gmail, Yahoo, etc.) using an employee's name.
- Text messages from spoofed phone numbers (which are surprisingly easy to fake).
- In rare cases, emails that look like they came from an actual @[yourdomain] account (though this is uncommon).

Common red flags include unexpected requests for gift cards, invoice payments, or urgent financial transactions. The reality of digital communication is that social engineering tactics constantly evolve, requiring ongoing vigilance. If you receive a suspicious message, don't delete it—report it to us immediately so we can strengthen defenses. When in doubt, verify requests verbally with the sender. Let us know about any suspicious activity, and we'll take action to minimize risks for the team.

Popups:

At random times you may see a pop up saying your computer has been hacked or calling some number to reach a Microsoft representative to resolve your issues. These popups sometimes make noise or look very official. At times they can even stop you from doing work. Keep in mind that no one from Microsoft will ever contact you for any reason at all. In these rare cases, it's best to restart your computer and contact ITGuys for a virus scan.