



TOP 5 IT IRRITATIONS

How to Identify Them And How To Fix Them

Rely On IT

2053 Grant Road, #147
Los Altos, CA 94024

Phone: 650-961-1300
Email: sales@relyonit.com

The Top 5 IT Irritations

How to Identify them and How to Fix them

In my 30+ years of IT experience I have observed many of the common IT irritations my clients face when working with their IT day to day. Here's a list of the top 5, how to figure out if you have them and what to do about it.

1) My Printer is Gone / My "S" drive is gone

Symptom: Your team member cannot work because their shared drive is no longer available on their PC "S" drive or similar.

Solution: Your IT team may not be using industry standard ways to ensure your shared drives and shared printers are showing up on your desktop when you login. This is something that your IT folks can set up so that everyone has a consistent set of printers and shared drives based on group memberships and privileges.

2) WIFI doesn't show up /work consistently

Symptom: Cannot consistently connect to corporate WIFI or WIFI drops suddenly, or you're setup is insecure because you don't offer visitors/vendors a guest WIFI access.

Solution: Wireless access points and routers are not made equally and it largely depends on both the equipment in use and the configuration of that equipment based on its capabilities. Most enterprise grade equipment can separate corporate from guest networks to ensure your guests and vendors don't have ready access to your confidential data and internal resources. Some organizations need to have 4 or more wireless networks separated for various compliance reasons or for security reasons to separate network access to needed resources. Guest access should only be granted access to internet on a metered amount of bandwidth.

3) Staff doesn't know where to find documents

Symptom: Your staff is constantly complaining that they cannot find key business documents in your business day to day.

Solution: Standardizing your shared file repositories is essential to your team/employees finding the right information with little effort in order to get their work done on time without road blocks. IT setup should include a review of your business operations and logical work groups for file storage.

4) Software displays errors that it is unlicensed or needs activation

Symptom: Employees complain that they cannot open Microsoft office/Word/Excel, Adobe Acrobat, etc.

Solution: Software licensing has evolved over the years such that many products are now licensed on a monthly basis instead of the old annual model. This user centric licensing model can cause many issues if not managed properly where users will get errors that their software needs activation. Sometimes it outright stops the users from productivity and other times it continues to work for up to 30 days grace until it shuts down. There are strategies on the IT side to ensure this is well managed on the network and that every user gets licensed software with less hassles.

5) Data goes missing or suddenly becomes encrypted or corrupted

Symptom: You come into work one day to find the important document you need for a court case or a client presentation only to find that your data is missing or encrypted or corrupted. Now What?

Solution: Have you ever walked into work to find all your data was encrypted, or data suddenly goes missing? Malware crooks are engineering more and more sophisticated threats that can force all of your data to encrypt or get moved or deleted for a ransom of usually several thousand dollars in a non-traceable currency like Bitcoin to get your data back. These threats normally enter your company through an email phishing attempt. Most users identify with common emails from companies like UPS, Fedex, or banks or other trusted services. The Phishing attempt usually masquerades as an innocent email from one of your common trusted vendors, except for the link in the email goes to a server on the cloud that downloads the infection or ransomware to your PC and then launches against any attached/shared drives on your server you have access to until it has encrypted all of your most important business data. In this case the only way to recover is to have regular onsite/offsite backups of all your data to avoid paying their unreasonable ransom to a crook in another

country. Having the right multi-tiered security in place along with regular onsite/offsite backups are key steps in being ready for any future threats.

If your company is experiencing any of the above issues its time to seek out professional help from a qualified IT company who can truly make your IT experience effortless. Don't put up with excuses from your current IT provider. It is time for a change. For more information please call or email us to schedule a free consultation to see if our effortless IT services are a good match for your business.

Phone: (650) 961-1300

Email: sales@relyonit.com