White Paper: Most Common IT Questions

Part 1 of 2: Sharing the support love…

Introduction

We resolve literally thousands of support queries every month for our customers, and while each customer is unique there's always trends to be seen - as well as good solid advice that we can provide based on our experiences over the years helping hundreds of organizations, their staff and computers.

In this paper we cover five common questions (in no particular order), and give you some advice on how to deal with each. Next month we will do five more. Further information and help on lots of these topics are, as always, freely available on our Ethical IT Knowledgebase

1. What does Malware do?

Everyone knows viruses are bad, but a lot of people don't know how they differ to malware. Viruses are programs that copy themselves and infect a computer, spreading from one to another—just like, well, a real life virus. A virus will cause your PC to behave erratically, and when you browse the web you might type in one web address and end up on a completely different, often dodgy site. Malware, on the other hand, can manifest itself as a real application, installed on your computer. The Malware program will most likely encrypt your ordinary data and then will ask you to pay a fee to release the files, and there is no way round this other than to wipe your PC completely and restore your files from a backup – assuming you have one!

Both malware and viruses do have one thing in common: they require the user to mistakenly allow them into the system and fire up. Often this is by opening a spam email attachment which runs the required processes to install the nasties, but it can also be triggered by visiting the "wrong" web pages that trigger a fake "your computer is at risk" message which you then click "ok" on and give the program the permission it needs to wreak havoc. We highly recommend reading this explanation for more detail on the different types of malware, and as always, make sure you're running a good antivirus program.

2. Look after your laptop or phone battery

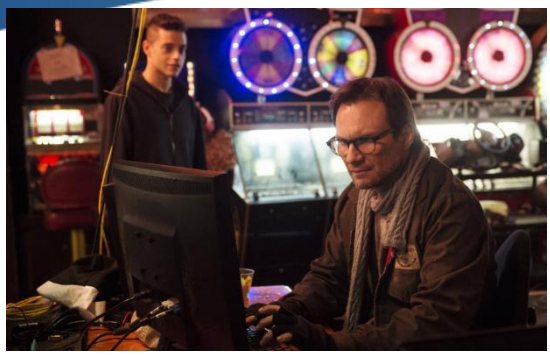
There are lots of guidelines and advice about batteries and how to manage them. These days with the strain we put on our devices, it's a wonder they work at all, but whilst hardware and tech in general keeps evolving at break-neck speed, batteries are really a couple of generations behind. We just haven't found a more effective way to store power yet than the Lithium battery. Some people say you should drain your battery completely before charging it, or that you should keep it between 40% and 80% all the time to make it last longer. Most of these rules are obsolete; modern devices running Lithium batteries will turn themselves off when fully charged and manage their power better. The general advice is: perform shallow discharges (not all the way to 0%) and keep them cool. Batteries have a finite life no matter what you do, so your efforts will only go so far— you can expect about 1.5 years maximum life, then you should replace them with a new one from a reliable retailer (there are lots of fakes out there so go genuine!)

3. Spam email and how to spot it

Some spam is obvious – just a name and a link to click, or an advert for a pill or a lottery win. But other messages are very, very sophisticated; an email from your PayPal account, or from eBay, or UPS saying you have a package. This is known as "phishing," in which a spammer will try to make their email look like it's coming from a legitimate source in order to get your information. They may tell you to click a link that looks like it's going to paypal.com, but if you hover over it, you'll see that it's really going somewhere else—likely a PayPal-disguised site where you willingly type in your information. There are a couple of simple tricks you can learn which will enable you to spot a fake within a few seconds; have a read of our Spam Email guide to find out.

4. Do I really need to "Eject" USB Drives?

Ever wonder why your computer warns you about ejecting those USB drives before you remove them? It's because computers use something called write caching to improve performance: if you copy something to your drive, it'll tell you it's completed the task, but it's actually waiting until it has a few other tasks to perform so it can do them all at once. Efficient, right? When you press eject, your PC finishes anything in the queue to make sure you don't



incur any data loss. Windows does a better job of avoiding problems than OS X and Linux, but we recommend ejecting all your drives anyway. It's small price to pay for keeping your data safe.

5. One of the sites I use has been reportedly "hacked"

It can cause a real shot of adrenalin then a sinking feeling when you read on the news that a site like LinkedIn has been hacked. The thought of your personal details in the hand of a criminal is horrifying. What those hackers are after is your username and password – that combination is valuable to them for sale on the dark web. It's likely that the data stolen from those hacked is encrypted, so uncovering the username and password combinations is often impossible, but sometimes hackers manage it. The advice here is obvious: 1. Change your password immediately. 2. If you use the same password for other sites, go and change those too. And 3. In future don't use the same password for multiple high profile sites. Of course the other way you can be hacked is by automated robots guessing your username and password combination. These robots bombard all the big sites every day looking for these weaknesses, so all the advice about using a proper, secure password is very sensible, and so is having a backup of all your files too.

Would you like to discuss any of this further?

At Ethical IT we are always here to help with these sorts of subjects too, so don't hesitate to get in touch with us to discuss this – on a personal level or for your organisation – we're all ears. Our Twitter feed also contains regular tips and tricks about these sorts of things, so please follow us @ethicalituk