Top Ten Cyber Security Tips

When you hear the words malware, adware and spyware, do you understand their meaning? Is a Trojan horse something you associate with Greek history or the modern-day world?

These are all potential threats and unfortunately for us, they are only getting more advanced. Keeping it simple and forgetting the jargon; here's our top ten cyber security tips here:

1. Realise that you are an attractive target to hackers. Don't ever say *"It won't happen to me."*
2. Practice good password management. Use a strong mix of characters and don't use the same password for multiple sites. Don't share your password with others, don't write it down and don't write it on a post-it note attached to your monitor, *ever!*
3. Never leave your devices unattended. If you need to leave your computer, phone or tablet for any length of time, no matter how short, lock it up so no one can use it while you're away. If you keep sensitive information on a flash drive or external hard drive, make sure to lock it up as well.
4. Always be careful when clicking on attachments or links in email. If it's unexpected or suspicious for any reason, don't click on it. Double check the URL of the website the link takes you to. **Think you can spot a phony website? Try this Phishing Quiz.**
5. Sensitive browsing, such as internet banking, should only be done on a device that belongs to you and on a network, that you trust. Whether it's a friend's phone, a public computer or a cafe's free Wi-Fi—your data could be copied or stolen.
6. Back up your data regularly and make sure your anti-virus software is always up to date.
7. Be conscientious of what you plug in to your computer. Malware can be spread through infected flash drives, external hard drives and even smartphones.
8. Watch what you're sharing on social networks. Criminals can befriend you and easily gain access to a shocking amount of information; where you went to school, where you work and when you are on holiday. This could help them gain access to even more valuable data.

9. Be wary of social engineering, where someone attempts to gain information from you through manipulation. If someone calls or emails you asking for sensitive information, it's okay to say no. You can always call the company directly to verify credentials before giving out any information. Never openly give information out if you don't feel comfortable with who you are speaking to.
10. Be sure to monitor your accounts for any suspicious activity. If you see something unfamiliar, contact your in house IT department or Managed Service Provider straight away. That's what they are there for!

Please feel free to call our helpful and knowledgeable team on 01843 572600 if you would like any advice about cyber security. You can also email us at hello@365itsupport.co.uk – we are always happy to help and provide advice for your IT requirements.

bcs
business computer solutions