Keeping your computer safe

1. Why do I need to read this?

Yes, I know this is a bit technical but stay with it. You only have to experience that awful feeling that all the stuff on your computer has gone, to appreciate how important this is. If you can't face this, then get someone who knows to sort it for you.

2. Keep your computer safe.

Obvious really, but how vulnerable is your computer to being stolen, dropped or breaking down – or someone else using it without your knowledge. Do you take your laptop out of your home? Leave it in a car? Or an unattended room?

3. Back Up Your Data

Backing up your data protects you in the event of a computer crash or electrical outage or surge, caused by a lightning storm. It also helps if you get caught out by ransomware, which stops you accessing everything and demands a payment to free it up.

You can do your back-up manually by transferring important documents to an external hard drive, (cost about £50) or using a "cloud" backup service. Apple provide this for their Macs and Microsoft OneDrive is built into the latest Windows 7-10.

If necessary, get help to set this up.

4. Operating System and other programme Updates

It is very easy to ignore these but they are essential in keeping your computer safe. Microsoft regularly issues updates to deal with vulnerable issues.

Make sure your PC has auto updates switched on.

Always ensure you have the latest update for Adobe flash (assuming you have this on your PC) which is vulnerable to hackers. Go to www.adobe.com/software/flash/about/ to check.

5. Get a well know Antivirus software package to protect your computer

There are free versions available but it is best to get advice. There are many special offers available. A great way to give yourself an overall umbrella of protection is to use Kaspersky or Norton Security products. Their Internet security and anti-virus software protects you from malware, spyware, and viruses, and it comes with parental controls as well. Doing some of the legwork on your own certainly helps keep you safe, but use Kaspersky or Norton if you want to make sure all your bases are covered.

6. Managing Passwords

This is such a frustration. They say don't write them down and then you can't remember them. So you choose one that's easy to remember and use it for everything.

Big Problem. You can use a password manager like LastPass or similar but it takes a little time to trust them. All your passwords are stored on their web site. They can suggest passwords to you. You then have just one password to access it when you first switch on your computer. Another suggestion is to use the first three letters of the web site you are accessing – either first or last with your usual password in the middle and a number at the end. Not perfect but better than using the same one everywhere. There is a risk allowing your browser (Chrome or Explorer or Edge) to store your passwords as these can be accessed by a hacker.

7. Check Your Firewall

This stops hackers accessing your computer through some of the "holes". Checking your firewall sounds complicated, but it really isn't. If you own a Windows-based system, just go to your control panel and type "firewall" in the search box. If your firewall is "on" or "connected," then you're good to go. If you own a Mac, click the Apple icon on your toolbar, go to "system preferences," then "security," then "firewall." Making sure you have a firewall in place can go a long way toward keeping criminals out.

8. Avoid Opening Unknown Emails

Never open an email from an unknown or suspicious source, and definitely never open any attachments contained in them. You have to be careful of emails coming from people on your contact list as well because the sender's account may have been hacked.

If an email from someone you regularly communicate with has a suspicious link and unusual content, delete it and immediately alert this person that his or her account may have been compromised. But don't use the reply option. Do a new email. This will help you prevent scams and hacking where you may be a target.

What happens is the link will cause a virus to download to your computer. Often this can be missed from anti-virus software.

There is a huge rise in scams that claim to offer tech support but actually set out to steal your money or install malware on your computer. Often appearing as "pop-up" adverts, these messages contain fake warnings that your device is riddled with malware, mimicking the style and language of genuine antivirus alerts making them seem credible. Do not click on any links or call the phone numbers displayed. Doing either could lead to you being scammed or hacked.

9. Scan for spyware (often part of your Antivirus software)

Spyware is a class of malware that, as its name implies, is typically designed to spy on you or your computer, silently collecting information that is subsequently sent on to others for typically nefarious purposes.

Various forms of advertising, including additional toolbars, homepage hacks, and data insertion (while technically not a form of spying) are often also included in the term spyware.

While very similar to viruses, spyware detection differs from virus detection in that it's more behavioural; it watches what your computer is doing to determine the presence of spyware. Virus detection is more typically data-based, looking for specific patters of data that indicate the presence of a virus.

Spyware is similar to viruses in that they arrive unexpected and unannounced and proceed to do something undesired. Spyware can be relatively benign from a pure safety perspective, as it might "only" spy on you. But that's enough. It can violate your privacy by tracking the websites that you visit, add "features" to your system that you didn't ask for, or record your keystrokes and steal your account login information for any online services that you might use.

Some of the worst offenders are spyware that hijack normal functions for themselves. For example, some like to redirect your web searches to other sites to try and sell you something. Of course, some spyware is so poorly written that it might as well be a virus, given how unstable it can make your system. The good news is that, like virus scanners, there are spyware scanners that will locate and remove the offending software.

10. Stay Away from Rogue Websites

Spotting a rogue website can be difficult, but there are a few things you can do to watch out. With your browser open, look for a green lock in the address bar and the code prefix "https://" at the beginning of the URL. This is essential when visiting banking sites, entering your credit card data or accessing your web mail. Be careful when shopping at a website that ships items from overseas.

11. Avoid Deals That Are Too Good to Be True

Special Deals for well-known products DVDs and music can be links to Trojans and viruses. The Rule is: If it looks too good to be true then it probably is.

12. Never Divulge Sensitive Information

No matter what website you're on be careful of the sensitive information you reveal. Although it's pretty much common knowledge not to give out your social security number or credit card information unless you trust a website completely, you should be just as careful with your social media profiles as well. Revealing information as innocent as your pet's name or mother's maiden name could lead to identity theft, because you probably use the same data as the security question on some other website.

Keeping your computer safe

13. Make sure the Wi-Fi you are using is secure.

Open Wi-Fi is any Wi-Fi connection that has not been configured with a password. Anyone with a Wi-Fi-capable device can connect to an open Wi-Fi hotspot.

If a password is used on a Wi-Fi connection, then the data being transmitted over the air is encrypted. Open Wi-Fi uses no password, and as a result, the data in transit is not encrypted. It can be easily viewed by anyone in range with an appropriate Wi-Fi capable device, such as a laptop, and packet-sniffing software.

If you’re traveling and using internet hot spots, free Wi-Fi, hotel-provided internet, or internet cafes, you *must* take extra precautions.

Make sure that your web email access – or for that matter *any sensitive website access* – is only via secure (https) connections or that your regular mail program is configured to use encrypted connections as well. Don’t let people “shoulder surf” and steal your password by watching you type it in a public place.

Make sure that your home Wi-Fi has WPA-security enabled if anyone can walk within range **and that you’ve changed your router’s administrative password.** Not sure about this? Get help.

14. Educate yourself

To be blunt, all of the protection in the world won’t save you from yourself.

- Don’t open attachments that you aren’t *positive* are OK; attachments are one of the most common ways that malware spreads.
- Don’t fall for phishing scams. *Be sceptical.* Phishing is a common way that online accounts are hacked into and can lead to more serious issues like identity theft.
- Don’t click on links in email that you aren’t *positive* are safe.
- Don’t install “free” software without checking it out first. Many “free” packages are so because they come loaded with spyware, adware, and worse.

When visiting a website, did you get a pop-up asking if it’s OK to install some software that you’re *not sure of* because you’ve never heard of it? *Don’t* say OK.

One way of protecting your computer is to set up an “Admin User” for managing changes to programmes and a second User, without the Administration permission option, for everyday use of the Internet. This should prevent any downloads that might change to your computer.

Not *sure* about some security warning that you’ve been given? *Don’t* ignore it. *Research it* before doing anything

Assembled from articles by askleo.com and David Bowen https://blog.kaspersky.co.uk/6-tips-to-keep-your-home-computer-safe-and-secure/ Computer Active magazine who write about technology, online security, and computer maintenance tips.

Andrew Collinge

August 2019