Latest updates on virus protection and location sharing

Time to uninstall your virus killer?

Installing security software and keeping it up-to-date has long been considered good advice, certainly when talking about Windows PCs. A recent article in Ars Technica (https://goo.gl/4v4jde) highlighted increasing problems with this approach. The conclusion from the article was that people should consider uninstalling all antivirus software, apart from Windows Defender (the one that is built into Windows).

This is not new advice, but it is the first time it has reached the mainstream. The issue here is that third party antivirus software must break some of the Windows integrated security features to scan internet activity and file downloads. This behaviour potentially makes PCs more vulnerable than they would be without such software. Windows Defender is the built-in Windows antivirus software. As such it can do its job without interfering with the security model. The article also cites the well-known problem of computers significantly slowing down as a consequence of running antivirus software.

To illustrate the concerns further, the article highlighted work by Google security researchers in June 2016 who discovered 25 very serious vulnerabilities in Symantec / Norton security products. This type of flaw has been found in all the common security products. It is becoming clear that such software, although purporting to improve security, is exposing users to problems greater than those they were designed to protect against.

Here is the best advice for now. On PCs, ensure Microsoft Windows updates are regularly installed and ensure Windows Defender is enabled. Users should also ensure they are using a supported version of Windows (7, 8.1 or Windows 10). On a Mac, the advice is similar. Ensure MacOS updates are kept up-to-date, but do not install any antivirus or antimalware software. On both platforms, good security habits have long been considered the best solution to avoiding viruses and malware. Many of these techniques have been described in the *Tech Review* previously, but to recap, here are some of the important ones:

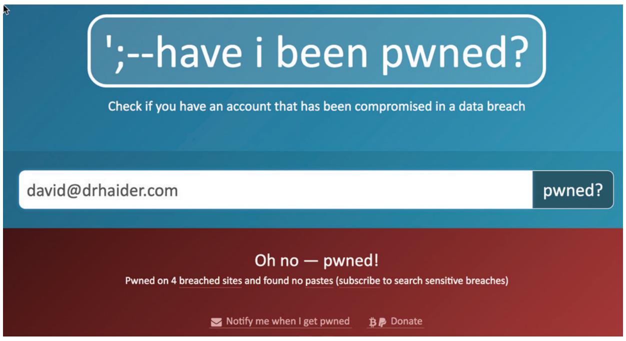
- Do not open email attachments that you were not expecting, ever. If in doubt, check with the sender.
- Avoid 'dubious' websites. They are far more likely to try to trick you into clicking malicious links.
- Use strong passwords (ideally random and not memorable).
- Use a password manager to secure all your passwords (e.g. LastPass).
- Avoid reusing passwords on multiple sites.

The last point of not reusing passwords is very important. If your usual password is published on the net, it won't be long before a hacker tries that password, along with your email address, on countless other sites. This type of attack is very easy to automate, meaning many usernames and passwords can be tried on vast numbers of websites very quickly.

If you want to check if your details have been released onto the internet, type your email address into this website: https://haveibeenpwned.com/

This site will check if any of the websites you have used have been hacked (or breached). If your details have been involved in a breach, your email and password (among other data) will likely have been published online.

Figure 1 shows the outcome of my own email address. You can see that my details have been involved in four breaches. Scrolling down will show the sites concerned. If your details have been involved in breaches, you should consider your passwords for the breached sites. If you have used those passwords on other sites, those sites are at risk. You should change your password on any sites that you have used those same passwords on. Remember to replace the passwords with unique, strong passwords next time.



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

david@drhaider.com

pwned?

Oh no — pwned!

Pwned on 4 breached sites and found no pastes (subscribe to search sensitive breaches)

Notify me when I get pwned

Donate

Figure 1

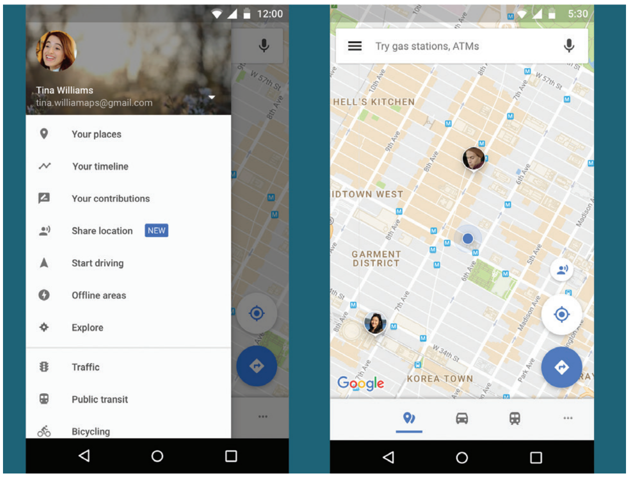


Figure 2

Location sharing in Google Maps

Regular readers may have come to expect new features of the Google Maps app to be covered here. This issue is no exception. A very nice location sharing feature has recently been added to the software. Similar functionality was previously available in the Google+ app, but this has now been removed in favour of Google Maps.

The feature works whether you are using the Android or iOS version of Google Maps. It allows ongoing, or time limited, sharing of your location with other people. This could be used to find friends or family at a conference, festival or maybe ski resort. In everyday life, it can help locate other members of your family. It is not a tool for covert spying, as the app shows exactly who can see your location. Anyone who is sharing their location with you appears as a coloured circle (or photo) at their location on the map. Figure 2 is a screenshot of the option that enables the feature and how it looks when it is in use.

To start sharing, simply press on the 'Share location' option. Next choose how long to share for (several hours, or permanently). Finally, choose a person to share your location with. They will then be sent a share notification by a method of your choice. The accuracy of the location clearly relies on your smartphone being carried on your person and having both charge and network connectivity.

SECTION EDITOR

David Haider,

Consultant Ophthalmologist and
Chief Clinical Information Officer,
Bolton Foundation Trust, UK.

E: david@drhaider.co.uk
Twitter: @drdavidhaider

The author has no proprietary or financial interests in the products discussed.