Internet security Q&A

BY DAVID HAIDER

Internet security advice is constantly changing in response to new and evolving threats. For this reason, it is timely to provide an update on recommended practices and new technologies. For ease of perusal the information is presented as a series of questions and answers. The advice below is general, with more complete answers being nuanced. Increased security typically comes with reduced convenience, whereas the easiest practices generally result in the least security.

Should I use a password manager?

Yes. The only way to maintain a vast number of unique passwords is to record them, typically in a password manager. Broadly speaking, two types exist. There are password managers built into operating systems and browsers (e.g. Apple Keychain or Google Chrome's Password Manager) and then there are third party password managers (e.g. 1Password). These are all reasonable and safe choices. The main reason to choose one over another depends on what device types you use. For example, if you frequently use both a Mac and a PC, you won't want to rely on the Apple Keychain, as it's not accessible outside of the Apple ecosystem. I use a range of devices, so I use 1Password, allowing me to access my stored credentials on all the devices I use.

Is it really that bad to reuse the same password on multiple sites?

Yes. Ideally all accounts should have different and strong passwords. Some accounts are more important than others, and those absolutely should have unique passwords. The most important accounts are those that control access to your emails. These are so important because email check loops are often used to confirm password resets to other sites. If you lose access to your email account, it is quite possible you could lose access to most of your other sites. So, as an absolute minimum, all email accounts should be protected with strong and unique passwords.

How important is two-factor authentication?

Two-factor authentication (2FA) forces users to enter an additional code to confirm login. The additional code often comes via text message or from a mobile app. Some websites always use 2FA, whereas others leave it up to the user to switch it on. Two-factor authentication offers excellent security and is worth using when available. As a minimum, much like passwords, they should always be enabled on any accounts that protect your emails.

What are PassKeys? Do they prevent me from needing to store or remember passwords?

PassKeys are a recent addition to internet security and not yet in widespread use. For websites or apps that support PassKeys, they allow an existing form of security to protect that service, rather than a password. The most common form of security for PassKeys are fingerprints or face ID from smartphones. If you have a modern and up-to-date smartphone (that you mostly keep with you), starting to adopt PassKeys (when offered) is a good choice. At present, most apps and websites do not support them, but adoption is increasing. They do not yet replace the need for strong passwords.

Are ad-blockers safe and easy to use?

Yes, but they are very platform dependent. On a PC or Mac, a good place for an ad-blocker is as a browser extension. For Chrome or Edge, several are available and there is no clear winner. Examples of safe and effective ones are 'uBlock Origin' and 'Ghostery', but others exist. If using Safari on a Mac there are fewer choices, but 'AdGuard' is a good choice, and it works well. It is also a good choice for iPhones and iPads. For Android, neither the Chrome nor Edge browsers support ad-blockers. The easiest option is to use the 'Samsung Internet Browser' instead (even if not using a Samsung phone). It is then possible to turn on one of the supported ad-blockers (such as 'AdGuard'). Advice in this area is often changing.

Are VPNs needed for security?

No. For most people there is no need to use a VPN for typical internet usage or even online banking. This holds true even when using open internet connections, such as in airports and coffee shops. As individual internet sites are now almost always independently encrypted, there is no longer substantial risk when using public internet sites.

Should I use third-party anti-virus and anti-malware software (e.g. McAfee and similar)?

No. For most people (using a degree of care and sense when using the internet) extra security software is not required. All modern devices (Mac, Windows, Android, iOS) have security software incorporated and they generally advise against installing additional software. In some cases, additional software can make the device more vulnerable. These days third-party security software has become somewhat of a money-making scam. I would advise against renewing any subscriptions.

Can the annoying cookie questions be blocked on websites?

Yes, to some degree. Most of the ad-blockers mentioned earlier also block those cookie messages, but some of them require the user to enable that setting in the ad-blocker (as a one-off). If you are not using an ad-blocker, there is an extension for Chrome or Edge called 'I don't care about cookies'. It hides many of those cookie questions and is safe to use.

Final thoughts

- If you frequently have guests that want your Wi-Fi password, investigate giving them guest network access (rather than your primary Wi-Fi details). Different providers make this available in different ways, so you will have to work out the details yourself for this one.
- Keeping your devices up to date is one of the best ways to ensure they are protected from the latest attacks.
- There is no change from the now well-known piece of advice to not open attachments in emails that are not expected.
- If your banking app lets you create one-off (or disposable) credit card numbers, these are great to use if you ever want to buy from less well-known websites. They often allow you to limit the use of the card number to a single purchase and only up to a specific amount.

SECTION EDITOR

David Haider,
Consultant Ophthalmologist and Chief Clinical Information Officer, Bolton Foundation Trust, UK.
david.haider@nhs.net
@drdavidhaider

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