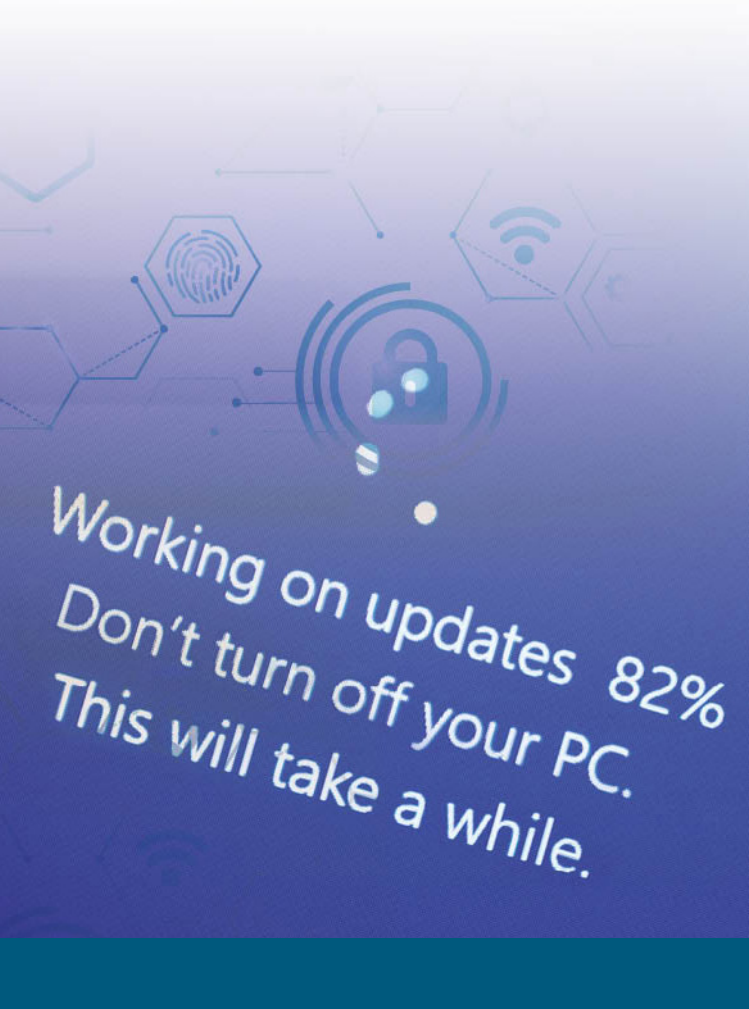
App updates

Are you up to date?

When software companies or mobile app developers add new features to an application or fix problematic issues, it is called an app or software update.

Computers, electronic devices and the software and apps we use are becoming more complex, so they require attention to keep them secure and operational.

Fortunately, software and hardware providers release updates when necessary to help keep systems and devices working well.



Why do they need to do this?

Updates are created for a variety of reasons – to deal with vulnerabilities, fix any software 'bugs', add new features, increase stability, and generally improve aspects of the user experience.

Cyber criminals spend a lot of time trying to find vulnerabilities within apps or operating systems that they can exploit. They will research software, hardware, apps and a variety of other technologies to try and identify weaknesses. Developers must therefore work to identify these problems and fix them to prevent applications being targeted.

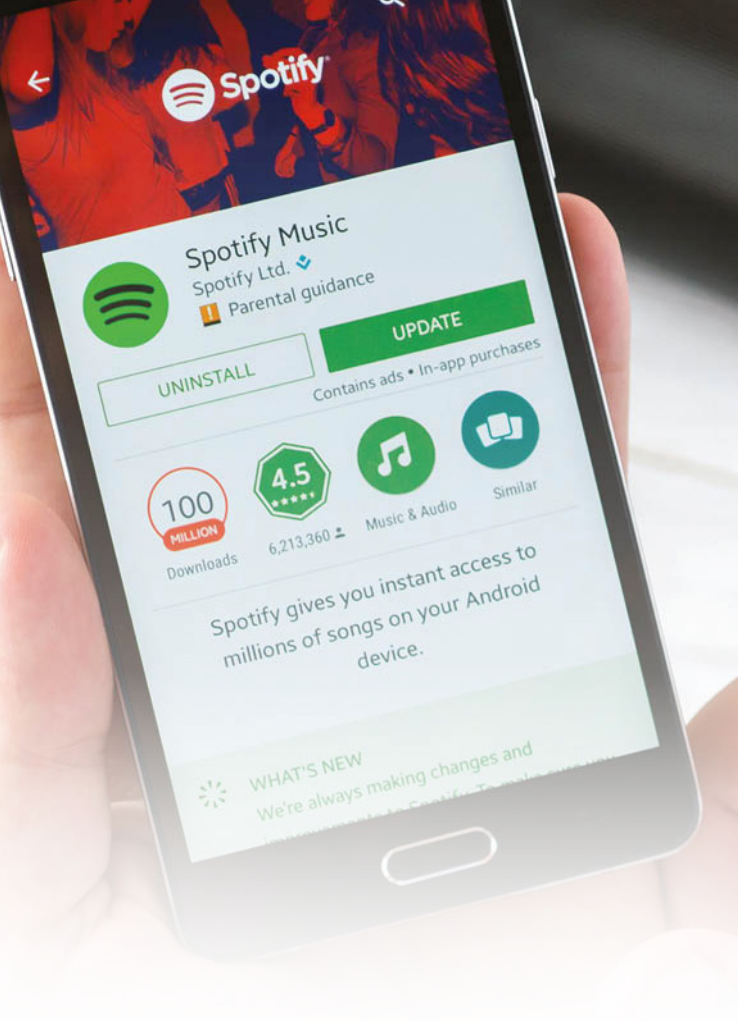
People who lawfully attempt to break into systems and seek out weaknesses are referred to as 'ethical hackers' or 'bounty hunters'. These individuals will identify vulnerabilities, notify the company concerned and receive a financial reward for their 'services'. The company will then look to resolve the issues – often by releasing a 'software patch' or 'update' to fix the vulnerability.

How often does this happen?

Patches are generally released whenever they become available so that fixes can be made as quickly as possible.

Because the detection of vulnerabilities is often made public, it is important to install patches immediately to resolve the problem and prevent any criminals taking advantage of the weakness.

'It's a good idea to install updates. Not updating your devices can lead to unpatched vulnerabilities that could be exploited.'



How do I know a patch is ready?

Modern operating systems all contain automatic update mechanisms – whether it's Windows, MacOS, or Linux running on a home PC, or Android or IOS running on a mobile phone. Most systems will notify you when a patch is ready, and some will automatically install them for you. Check your notifications and update when necessary. Many older operating systems also include update facilities, so check to see if updates are available.

Do I really need to install these updates?

It's a good idea to install updates. Not updating your devices can lead to unpatched vulnerabilities that could be exploited. Usually, it is very easy to install an update, at no charge, with nothing more than a click. This will ensure that devices are kept as secure as possible.

Some businesses need to ensure that bespoke applications will continue to operate properly following the deployment of a patch and will often undertake testing prior to releasing it for general use. Such businesses usually have their own patching systems in place.

What else do I need to know?

Criminals will try to trick you into installing software that they have disguised as a patch. If you are at all concerned about the legitimacy of a patch, you can stop the installation and launch the update process from the software or operating system itself. This will generally identify new updates and you can be sure the patch is genuine.

Remember, some older software and operating systems that have been taken out of service will no longer receive updates and are inevitably more vulnerable than newer systems.

You can access advice and information on a range of cyber security topics at the following sites:

www.ncsc.gov.uk

www.cyberaware.gov.uk

www.takefive-stopfraud.org.uk

www.actionfraud.police.uk

www.serocu.police.uk/individuals

Report online at **www.sussex.police.uk** or **www.surrey.police.uk** or **call 101**.
In an emergency always **call 999**.

Find us on social media

Produced by Sussex Police Corporate Communications 2019