Digital Unite

Inspiring POSITIVE CHANGE through digital skills

10 top tips for smartphone security

Print

It is really important that your smartphone is secure for many reasons. You may keep data on it and if your phone was lost or stolen, this would be lost. Or perhaps your personal information may be hacked from internet pages you have visited or from the smartphone itself. We've put together some tips to help keep your device as secure as possible.

1. Use a screen lock

Many new phones offer a "pattern lock" – a personalised shape or pattern that is drawn on the screen to grant access. However, ensure that the screen is cleaned regularly. If your phone is stolen or lost any finger traces can sometimes be seen and accessed on the screen. Alternatively a PIN code offers an alternative and can also save time. Make your password difficult to crack but memorable for you. The best advice on creating secure passwords is to take the initial letters of a line in a song, play or book, and to make a password from those letters.

You can use remote tracking if you loose your phone. On Android it is called 'Find my Device' and on Apple iPhone it is called 'Find my iPhone'. From here, you can remotely disable your phone if needed.

2. Use a SIM card lock

A screen lock is helpful but won't stop someone removing the SIM card from your phone and using it on another phone. To prevent this from happening, set up a SIM card lock in the form of a PIN number that will need to be entered when a phone is turned on in order to connect to a network.

3. Protect sensitive data

While PIN entry and password locks are helpful, a smartphone is effectively a miniature computer with often easily removable storage. It's far too easy to retrieve data by simply plugging it into a computer or removing a microSD card.

It's important to protect sensitive data saved to internal storage. Software is available that can encrypt files or folders so that a code must be entered before a file can be viewed or copied. A lot of this software is free to download and use and can work effectively with your phone to provide automated protection, so there's little hassle involved once it's up and running. An example of such software is AutoKrypt but do 'shop around' to find the right solution for your set-up.

Always back up your data, for iPhone you will need to back up your data on iCloud. You can also store data on Dropbox or OneDrive.

4. Wireless protection

Any device that's can send data across the airwaves is a concern for security.

Always switch off your wireless connection when it's not in use. It ensures that people can't connect to a device without your knowledge. It's also worth checking your phone's network security settings as it might be configured to automatically connect to a network when in range without you knowing.

Ensure that your home accessed wireless router is protected by a pass code.

If using mobile wireless or a hotspot, be careful of malicious connections that looks very much like a legitimate hotspot from a large company.

5. Protect bluetooth use

Bluetooth isn't generally seen as a risk as it has a relative shot range (10 metres approx). However, hackers have been known to remotely access a phone if they are in range.

Ensure that bluetooth is turned off when not in use. Set the bluetooth configuration to 'non discoverable', so that people searching for nearby devices can't see yours.

Any unknown requests that pop up through a bluetooth connection, such as an offer to 'pair with a device' should be ignored or declined. A hacker in range could make use of your device through bluetooth if it is not secured.

6. Application download security

Unfortunately the increase in malware relating to smartphones has increased the need to be cautious when downloading applications, and to pay attention to the requirements that any software requires when you install. It can be very easy not to read anything in an effort to get the app up and running, but be careful of any demands to access various features of your phone, particularly if the app isn't well known.

7. Internet browsing

Be careful when accessing a web browser on your smartphone as it can be easy to accept messages that pop up. For example agreeing to save user details and passwords might make it easy to remember for later, but unfortunately others can do the same if they gain access to your phone.

If any security warning pop up when looking at a website, take note of it and leave the website if needed. Also, ensure any banking or shopping sites where you put in secure information have a padlock in the address bar to ensure that the site is encrypted. For more on shopping safely online, see our guide.

Make sure you always look at the URL and make sure the 'http' has an 's' at the end. This ensures that the URL you are about to click on is secure. We also recommend that you check for any spelling mistakes in the URL.

8. Turn off geotagging

Many smartphone social networking apps automatically upload photos to the Internet. The problem with this is that many phones embed location tags, also called "geotags," right into the photo files themselves.

Anyone with the right software can look at your Facebook or Flickr pictures and find out where you have been and where you are right at that very moment.

The geotagging feature can be turned off on most phones which gives you privacy and ensures that you can't be found by someone you might not wish to be found by.

9. Install antivirus

The capabilities of smartphones are approaching those of a PC, but most people have no form of protection, although they can face similar threats.

Spam containing malware attachments or links to attack sites or infected apps that exploit weaknesses in the operating system are all starting to appear.

Many antivirus companies now offer free versions of their commercial mobile products and also protection for multiple PCs and a phone, for a yearly subscription.

Unfortunately, fake antivirus software, designed to infect your device or make you think it's protected when it's not, has also now made its way to smartphones so do be vigilant.

10. Remote wipe

If the worst happens and your phone is lost or stolen, you may want to protect your data by wiping data quickly and remotely.

Many operating systems have a range of third-party, dedicated remote wipe applications to choose from. These tend to be subscription services, but prices are usually less than £5 a month.

Alternatively, there are other features offered by antivirus packages. Free versions, like AVG's Mobilation Free, offer local wipe facilities. However, it's not always clear if remote wipe is included or just a local wipe facility, so check with the software vendor before you pay out.

This guide was last updated on 22/02/2019

Next steps

How to shop safely online

Email safety tips

What is malware?

Email safety tips

How to stay safe on Facebook

Internet safety for kids

Staying safe playing online bingo

Search guides

Search

Free how-to guides for your website

Why not add our award-winning and extensive range of digital skills guides to your website?

Find out more

Remote Digital Championing!

Guides covering some tips and techniques for providing remote support to learners, an increasingly important service in times of social isolation.

Find out more

Start a Digital Champion movement!

Could your workplace do with developing its digital skills? With funded membership opportunities currently available, now is the perfect time for organisations to join our Digital Champions Network.

Find out more

Subscribe to our newsletter

Join our mailing list to receive the latest news, offers and expert insights from our team.

First name

Last name

Email address

Submit