Stay healthy ...

But stay safe.

www.getsafeonline.org/westsussex   www.westsussex.gov.uk/stayingsafeonline

Fitness & health apps: the facts

Whether you're a fitness fan or just want to maintain a healthy lifestyle, it's good to keep track of your exercise. Perhaps you use one of the many available health and fitness apps to keep track of your exercise. It may or may not be linked to a fitness watch. Many of these monitor not only your progress, but also vital signs, calorie intake and sleep patterns.

Unfortunately, fitness apps can have drawbacks when it comes to safety and security.

One is location data, which you can use to recall where you did your exercise and also upload to share with others and take part in virtual competitions. Even wearing a device when not exercising means your location is still being recorded. If the website/app, your device or the communication between the two is hacked, it's possible for your and others' locations to be revealed. Worryingly, studies have revealed that a high proportion of both paid-for and free apps contain security vulnerabilities.

Another risk is to your health or medical data. Many apps lack suitable privacy policies, which means that both the details you enter and data gathered by the app could be (and frequently are) sold on to pharmaceutical and insurance companies, even potentially falling into the hands of fraudsters and hostile nation states.

Read our top tips on using fitness and health apps safely and securely.

- Never allow fitness or health apps or computer programs to share your information with third parties. Read terms and conditions carefully before you click to accept them. Even an undertaking that information will not be shared, or shared only with 'carefully selected third parties', is no guarantee that this is the case.

- Never enter competitions or participate in free or cut-price offers in exchange for sharing data.

- Your profile or what you post or communicate on fitness applications should not be associated with anything confidential in your life, for example if you have a job involving sensitive or secret information.

- Don't post pictures or link any of your other accounts to your fitness/health app.

- Don't log in to fitness and health apps through social media applications. Instead, log in to the app itself, using a unique password you don't use for any other app, website or account.

- If you fall victim to fraud or identity theft as a result of using a fitness app – or for any other reason – report it to Action Fraud at **actionfraud.police.uk** You should also report it to the fitness app developer, which is also the case if you discover that your personal data has been compromised via the app.
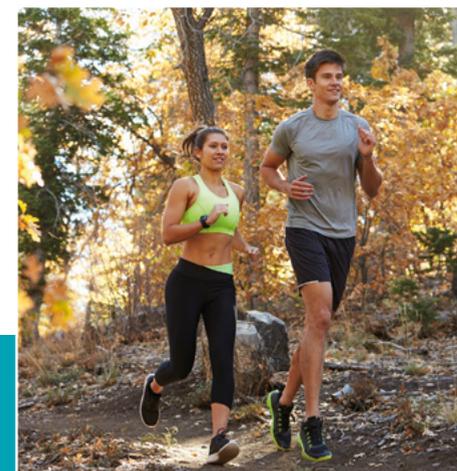
For comprehensive, practical, expert advice visit
www.getsafeonline.org

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

If you think you've been a victim of online fraud, report it to Action Fraud, the UK's national fraud and cybercrime reporting centre on 0300 123 20 40 or at www.actionfraud.police.uk

www.getsafeonline.org/westsussex   **www.westsussex.gov.uk/stayingsafeonline**

OFFICIAL PARTNERS

TESCO · kaspersky · Gumtree · Standard Life · first direct · M&S BANK · HSBC

Royal Bank of Scotland · NatWest · LLOYDS BANK · HALIFAX · BANK OF SCOTLAND · creative virtual · ROYAL AIR FORCE

CITY OF LONDON POLICE · NPCC · NATIONAL TRADING STANDARDS · cifas · VICTIM SUPPORT · EUROPOL EC3 European Cybercrime Centre

ActionFraud · METROPOLITAN POLICE · eCrime Team · Ofcom · neighbourhood WATCH · neighbourhood ALERT