
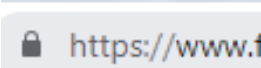



## Privacy: Basic Tips

<p><b>Unlock device:</b> Use a passcode to unlock your device: this means that if it is stolen, it will be harder for someone else to access your data.</p>
<p><b>https://</b>  </p> <p><b>Check the web address – the ‘s’ and the padlock symbol generally indicate greater security</b></p> <p>This information is an assurance that the site encrypts the sensitive data that you send, e.g. your bank and credit card details or address.</p>
<p><b>Passphrase not password:</b> create different passwords for your various accounts based around a meaningless sentence that you will remember, e.g. W33cup0T. Change passwords regularly – use a password manager.</p>
<p><b>Apps permissions:</b> these can access information about you, such as your contacts and emails, and they may even take photos or videos. You can choose which data apps have access to – you can change this in  Settings.</p>
<p><b>Social media:</b> think about how much information you share on social media - you tag friends, reveal your location, your tastes and preferences – even ‘fun’ quizzes that you fill in can be designed to harvest information about you, so that you can be more accurately targeted in marketing campaigns. Take control of your social media privacy settings – for example, choose not to share your actual DOB on Facebook. <i>Don't share anything that you would not be happy sharing publicly! A good rule of thumb is to keep personal information off social networks.</i></p>
<p><b>Search engines:</b> these can allow advertisers to target you personally. You can use private browsing, delete your browsing history, and manage your cookie settings in Internet options. You could also switch to a search engine that does not track your inquiries, for example <a href="#">DuckDuckGo</a>.</p>
<p><b>Bluetooth:</b> Turn Bluetooth off when you're not using it.</p>
<p><b>Wi-Fi:</b> Avoid banking or shopping on public Wi-Fi.</p>
<p><b>Spam:</b> Never reply to messages from people you don't know.</p>
<p><b>Friends?</b> Only ‘friend’ or connect with people online that you know in real life.</p>
<p><b>Location:</b> Turn off GPS on your device's camera and on apps where it's not needed.</p>
<p><b>Security:</b> Protect all your devices with security software. Keep software up to date.</p>
<p><b>Subscriptions:</b> The way in which you consume media can reveal your personal tastes. This in turn can control the suggestions that are made to you (<i>if you like..., you might also like.....</i>)</p>
<p><b>Loyalty cards:</b> These can tell a store or company about your preferences so that they can target marketing directly to you. You may not mind this if this is your favourite company, but you may not like a third party having access to your data. Be very clear about your marketing preferences when you sign up (check the privacy policy to see how they use your data). You can also choose how – and if - you want to be contacted, for example by email only or by text.</p>