Ministry
of Defence

Personal Online Security

blog
upload
update
e-mail
chat
message
text
play
connect
share
tweet
blog
upload
update
e-mail
chat
message
text
play
connect
share
tweet
blog

Introduction

Social networking sites are great for keeping in touch with family and friends, and letting the world know what you're up to. The Online Engagement Guidelines make it clear that we encourage the safe and responsible use of social networking sites. This document contains guidance on how to help you stay safe and to think about what you post online. Remember that there may be those who are using such sites for unsavoury reasons. These can range from criminals looking for ways to con you or steal your identity, to those who may wish us harm. While it is unlikely that you'll fall victim, you should be aware of the risk.

Google yourself – how much information about you exists online? Not just that which you've put there yourself, but what other people or organisations have posted. Be extra careful if you have identified yourself as being a member of the military or an MOD civilian.

It is easy enough to collect information to build up a picture of who you are from various sources. Similarly it might only take one careless comment, or posting a picture without checking what's in the background to put friends and colleagues at risk or major embarrassment.

Alongside being careful about what you choose to share online, you should also look at the privacy and security settings on every social networking site you use. Are you happy with how your information is being used and shared? And if there are sites that you no longer use, and have no intention of using again, it's better for you to close your account rather than just ignore it.

There is a short guide to appropriate social media behaviour for Defence personnel. There is also a guide for commanders - providing guidance on how to deal with the inappropriate use of social media amongst the personnel they command.

Contact Directorate of Media & Communication for more policy, advice and guidance about using social media or speaking officially in the media or in public as a member of the defence community. The guidance in this document does not supersede any other official document.

Security and Privacy Settings

General

Whenever you join a new social network, you should always look at the privacy and security settings so you are aware of how much information the service is sharing about you, and who is going to be able to see it. If you've been a member of a social network for some time, it's worth looking at the privacy and security settings frequently as they are subject to change.

Each social network deals with privacy and security in different ways, and you shouldn't share information on their service until you know where that information will end up.

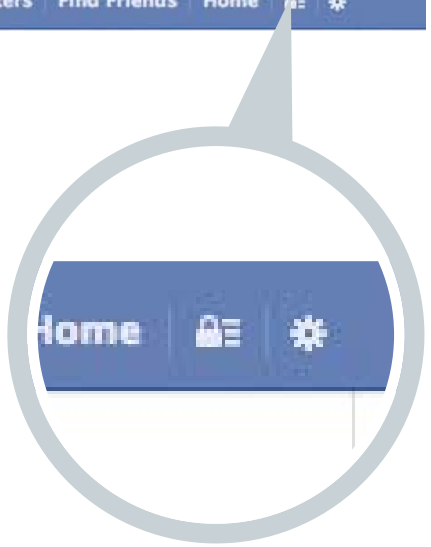
Facebook

You'll find the button for privacy and security in the blue bar on the top of the Facebook page, towards the right side of the page. It has a picture of a lock.

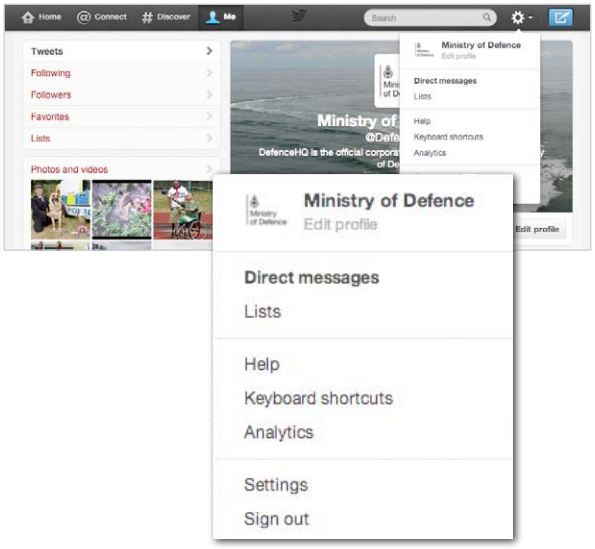
Inside, there are settings where you can decide who can see your 'stuff' - the things you post to Facebook. There's also a handy setting where you can take a look at how your profile will look to someone who is not one of your contacts.

In the same section you choose who will be able to send you messages, and who can send you friend requests.

There are more settings available than the ones mentioned above, and you can reach them from the same tab. It's worth looking through them to get a good idea about what information you're sharing, but at the absolute minimum, you should make a decision about who can see your posts, who can message you, and who can friend you.



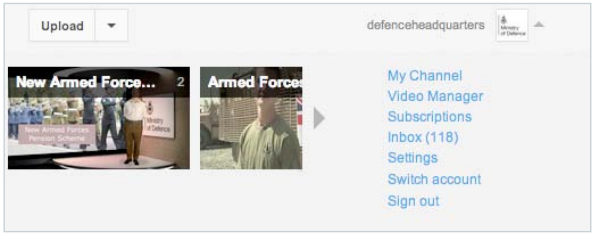
Twitter



Twitter's security features can be reached by clicking on the cog in the top bar, then clicking on settings. On this page you'll be able to choose whether Twitter can add your location to your Tweets (if you have this checked, you can still turn off location on a Tweet by Tweet basis, but if you never want to add your location, you can turn it off using that check box). You can also choose whether Twitter will show you sensitive content, and you can choose whether to 'Protect' your Tweets. If you check this box, all your current followers will still be able to see your Tweets, but any new followers will need to be approved by you before they can follow you. Also, any Tweets you posted before you protected your Tweets will still be searchable.

It is up to you if wish to protect your Tweets, but you should never think that because your Tweets are protected that you can share any sensitive or secure information using your account, because it is still possible that your followers could share your post with others, or the information may get out in other ways.

Google & YouTube



If you're logged in on the Google homepage, and click on your name, you'll find a button marked 'Privacy', where you are able to choose various options about how visible your Google+ account is (if you have one), as well as getting access to your 'Dashboard' where you can view and edit what information Google has across the various services they run and own. This page also gives access to their 'Privacy Centre' which will give you more information about Google's services and privacy policy.

On the same page, if you click on 'Security' on the left, you'll find the place to change your password, and how to set up 'two-step verification' which is a means of making your account more secure from people who may want access it. You'll also be able to find out which apps have access to your account and review these.

If you're logged into your YouTube account and you click on the arrow by your avatar near the top right of the screen, then click on 'settings', then on 'Privacy'

on the left hand of the screen, you'll be able to choose whether your likes and subscriptions are private, you'll also be able to set your account so only your contacts can send you videos and decide whether people can find you on YouTube by using your email address. You can also see what apps have access to your account, similarly to the Google page above.

Pictures and Videos

Pictures are powerful and often revealing assets, and while photos can contain trivial information they can also pose a risk to personal and operational security if placed in the wrong hands.

Whether in a professional or personal capacity, you should always consider what information you are revealing through imagery you publish online or anywhere in a public domain.

Always consider how the images and videos you publish might be interpreted, and what level of information they are really displaying. Remember, unless you have appropriate privacy settings activated, there is a strong chance that your images can be viewed by the wider public, so consider whether you wish to identify yourself, family members or your location, and how you are representing your profession.

In general, you should avoid:

- Operational security breaches; images that disclose location, operational intentions, equipment specifications and capabilities.
- Images that could damage your Service's reputation.
- Aggressive, abusive or inappropriate poses in uniform.
- Identifying yourself or other personnel on operations.
- Using content that you don't own; remember Copyright law exists online too.
- Videos that display specific locations or operational intentions.
- Videos that use inappropriate, foul or abusive language.

View the 'Personal Security Online 4: British Army' video on YouTube

Location Services and Geotagging

Various social media services can use information about your location, either from a mobile device, or from your computer, and attach it to information you share on their site. Some social media is based solely around this (for example, Foursquare, where you 'check in' to places you visit).

Although there is nothing wrong, under the right circumstances, in sharing your location in this way, you need to keep in mind how much information you are giving, and whether you are comfortable with it. Although sharing a single location may seem fine, what information are you giving away when you check into many locations over a long period of time? Is it possible that people could work out your routine, or where you live from this information, even if that is something you have not chosen to specifically share?

View the 'Personal Security Online 1: Royal Navy' video on YouTube

Friends and Family

It's not just you who needs to think about your personal security online. Your friends and family will often know about your deployment, travel arrangements, and other information that should not be publicly available. To make sure they don't share this information, you will need to speak to them about what they can and cannot talk about. You should also ask them to read through this document so that they too can make informed decisions about what they share on social media.

There is nothing wrong with using social media to stay in contact with friends and family, indeed it may well be the best way to stay in touch, but make sure that anything shared online is safe, and that you, your friends and family aren't giving away more than they mean to.

View the 'Personal Security Online 2: RAF, Friends & Family' video on YouTube

Commenting and Debating

Many news websites, blogs and social networking sites allow you to give your views about subjects in comments sections beneath particular stories, and forums provide a place in which many people share their opinions. However, on these sites there are some things you need to bear in mind:

Be careful about giving away too much information as some blogs, news websites and forums are easier to search than sites such as Facebook and keep their information easily accessible for longer than sites such as Twitter.

Never share anything which could breach operational security in a comment section or forum, and be careful not to share personal information such as where you live, names of your family members, or information about anyone else unless you've received their permission in advance.

Please bear in mind that the guidance on communicating with the media applies in comment sections as much as it does if you went to speak to a journalist in person. Don't try and speak on behalf of your service and keep opinions clearly personal. You can read more about the policies relating to communicating with the media here. Act online in a way that reflects well on your Service and if you are a civilian, remember to follow the Civil Service code.

View the 'Personal Security Online 3: Defence Civilians' video on YouTube

Scams, Fraud, Hoaxes, Phishing and Blackmail

Phishing, scams, frauds and hoaxes are a major source of cybercrime affecting many internet users. Most users have a basic awareness of computer viruses and a general notion of what constitutes identity theft, but a number of people don't realise the real threat that phishing, frauds and scams pose.

Given the increasing popularity of social networking sites and the general improvement in email filters, scammers are now using these sites more and more

in an attempt to harvest private information and commit varying levels of identity fraud. On such sites, most users believe they are in a secure network, but this is not the case. The relative ease of creating accounts or setting up profiles provides an easy foundation for scammers to begin a number of fraudulent activities.

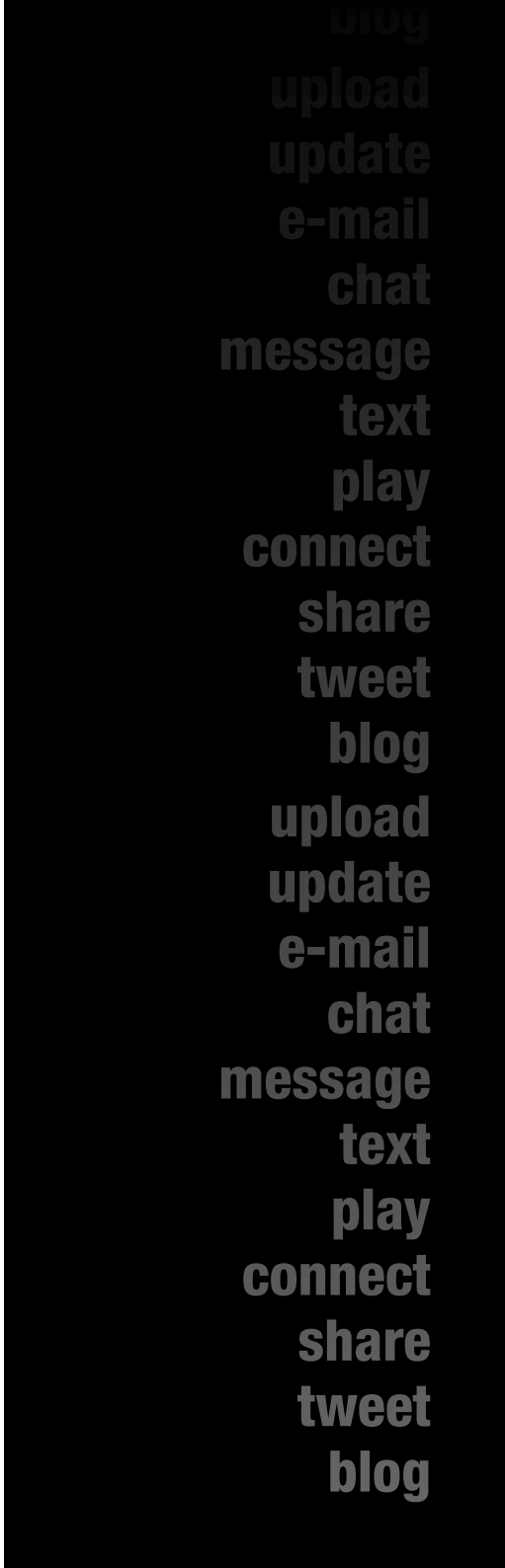
Email and Forums

Most email phishing scams will catch users off guard by appearing to be messages sent from a recognised organisation or source; commonly a bank, paypal, an address book contact, or even one of your social networking sites. The message may prompt you to ‘verify your account’, ‘respond within 48hrs or your account will close’, or take advantage of a ‘free upgrade available on your account’.

Most scams will provide what appears to be a link to the relevant organisation’s main site, but it will actually be a link to a spoof front-end site with a similar (but not the correct) URL. If you enter login information on this site, your account/profile will be vulnerable to attack.

With login information captured, a thief can hack into your account, pass themselves off as you and then either trick your friends into downloading malicious software, make a plea for money, or lead them to a fake website that asks for private login information.

To avoid becoming a victim, make sure you do not give out confidential information readily, especially if you are suspicious of the email/message you receive. Don’t click any links, but go to the organisation’s main site through a new browser window. If there really is a problem with your account/profile, the main site will have the information that you are looking for.



Blackmail

If you share information, or photos or videos of yourself online, especially with people you don't know, could this material be used to blackmail you? Your position in the Armed Forces could be jeopardised if you post material in the public domain that shouldn't. The best way to avoid this is not to share material that could put you in this position, especially with strangers, particularly if they have an avatar that you think is attractive.

General Tips

Scammers are always trying to evolve their techniques and use different methods to con people, so take care on all social networking sites and when using mobile applications. Remember:

- Use strong and unique passwords, with a different one for each site.
- Always check you're in the actual main site before entering any login information.
- Be wary of suspicious links, requests for passwords and unusual comments/ messages/updates from friends/followers. Scrutinise all requests carefully.
- Limit what information you share on your profile/account such as birth dates, phone numbers and use of geo-locating services (such as Facebook Places or Foursquare).
  Use privacy settings to your advantage
- Keep your computer software and browser up-to-date and virus-free.
- Select third-party applications with care.
- If it's too good to be true, it usually isn't. So, don't fall for it!

What to do if something goes wrong

Sometimes, despite our best intentions, things go wrong. It's important, in these circumstances, to stay calm, know what to do and who to turn to for help. This table will tell you what to do if you think you have done something wrong.

Click on a category below to find out what you should do (this will work in Acrobat Reader).

You've slipped up

Unwarranted Attention

Malicious Acts

Resources

- Facebook's Privacy Help Centre
- Facebook's Security Help Centre
- Twitter's privacy policy
- Security at Twitter
- Google security and privacy tools
- The Google Security and Privacy Channel on YouTube
- Amazon Privacy Notice
- Contact with the Media and Communicating in Public