Protecting Social Media Accounts

# Protecting Social Media Accounts

## Summary

Hostile attacks on Social Media accounts pose a serious threat to the Ministry of Justice (MoJ) and its reputation. When attacks happen, they quickly become [headline news](https://www.independent.co.uk/news/uk/politics/boris-johnson-dominic-cummings-tweet-civil-service-arrogant-offensive-a9530706.html), and can [happen to any account, anywhere in the world](https://www.nytimes.com/2019/08/30/technology/jack-dorsey-twitter-account-hacked.html).

Two types of attacks are common:

* Attempts to render the account useless by 'bombarding' it with messages.
* Attempts to 'take over' the account.

## Steps we can all take to protect ourselves

### Ensure our passwords are secure

Passwords are the main protection on our accounts, hence ensuring they are secure is vital. The NCSC has produced [guidance](https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0) on making secure passwords - the summary of which is that picking three random words to make a password (for example RainingWalrusTeacup) is a good policy for securing Social Media accounts.

### Check your email details are up-to-date

Most of the time, the first indication you'll have that something is wrong is when an email is sent to you. This could be to let you know that someone is attempting to log into your account, or that someone is trying to reset your password, or more worringly, that a new device has logged into your account. Hence it is important that you ensure that your email details are up-to-date, and that your email is secure.

### Enable Two Factor Authentication

Two Factor Authentication (2FA) involves requiring a random code to be entered before being logged in. These codes are either sent to the user via SMS or email, or generated every 30 seconds by an app or device the user has which relies on a seed key provided by the service. That seed can then be shared amongst a team, allowing for multiple owners or contributors.

If at all possible, SMS generation should be avoided, as it is theoretically possible for phone numbers to be taken over through various attacks, as well as meaning that only one person can receive the code, which isn't ideal if a team is working on a single account.

If you're using email, then it can be sent to a group account, which also allows for multiple owners or contributors - but it's important to ensure that the email is also protected by 2FA.

If you have a spare 10 minutes, watch [this video](https://www.youtube.com/watch?v=hGRii5f_uSc) for an excellent explanation of how 2FA works and why it's important to have it enabled.

Click the links for details on how to activate 2FA for [Facebook](https://www.facebook.com/help/148233965247823), [Twitter](https://help.twitter.com/en/managing-your-account/two-factor-authentication) and [Instagram](https://help.instagram.com/566810106808145).

### Only use trusted third-party applications

In addition to the official applications, there are many tools and third-party applications that might be used to work with social media accounts.

Some of these tools provide useful extra facilities, such as 'scheduled' posts, or helping you post one message to several different social media channels.

The problem is that you have to give your account details to these tools so that they can post to your account.

This is potentially very dangerous:

* An application might post messages on your behalf, that you do not agree with or are unacceptable.
* An application might store or share your account details.

Only use applications that are trusted and approved for use with your social media accounts. For help with this, [contact Cyber Security](#cyber-security-advice).

### Remove 'unused' applications

People tend not to be very good at removing old or rarely used applications. Older applications should be checked regularly to see if there are any updates.

A good habit is to check your applications once a month or so, and consider:

* Do you still use the application? If not, remove it.
* Whether there is an update available for the application? If so, install it.

As well as increasing safety, removing unused applications frees up storage space on your system.

### Check your privacy settings

The whole point of a social media account is to share information. But that doesn't mean you want to share *everything*.

When you first create a social media account, you are normally asked to decide on the privacy settings. These control how much information you share, and who you share it with.

But it's very easy to forget to check the settings, from time-to-time, to make sure they are still correct.

A good habit is to check your account privacy settings once a month or so. Information on privacy settings is available for the main social media environments:

* [Facebook](https://www.facebook.com/help/1297502253597210)
* [Twitter](https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public)
* [Instagram](https://help.instagram.com/196883487377501/?hel-)

### Limit access to your accounts

You might be tempted to share access to your social media account, for example if you want to have postings regularly, even while you are away.

Avoid sharing access to your social media account. It's easy to forget who the details are shared with. It's also possible that postings might be made on your behalf that you don't agree with, or are not acceptable.

Any MoJ social media accounts that do need to be shared will have proper access controls in place. You should never need to share your account details for work purposes.

If you need more help on this, contact your Line Manager or [Cyber Security](#cyber-security-advice).

### Don't click on suspicious links

Unfortunately, social media postings are a common way of sending you links to malware or other problem material. Postings might also be used to send you 'phishing' attacks.

In the same way that you should be careful with any links or attachments sent to you using email, you should also be suspicious of links or attachments sent to you though social media. This applies to both general postings and messages sent directly to you ('Direct Messages').

For more information, read [this article](https://intranet.justice.gov.uk/news/dont-be-caught-out-by-fraudsters/) on the MoJ Intranet.

## What to do if your account is bombarded

### Remember that these attacks are short lived

Due to the amount of organisation and effort required to coordinate such an attack, they do not last long, and like an intense inferno, will soon burn themselves out.

### Do not respond to the attack

These attacks are designed to attack the person controlling the account as well as the agency itself. By only responding to messages not involved in the attack - especially those trying to share positive messages, the attackers will run out of interest far sooner than if you engage them. If they are posting harmful or threatening messages, report the accounts.

In a single sentence - "don't feed the trolls".

### Feel free to walk away

Dealing with these attacks can be emotionally draining; even just reading the messages can have a far greater impact on you than you realise. Take breaks in the event of an attack, even if it's hard to - consider going for a walk to force yourself away.

## Cyber Security Advice

**Cyber Consultants & Risk Advisors**

* Email: [security@digital.justice.gov.uk](mailto:security@digital.justice.gov.uk)
* Slack: #security