## Recover from a hacked social media account

Social media accounts such as Facebook and Twitter are a common target for cyber criminals. These accounts contain lots of personal and confidential information and can also be used to scam your friends and family. When your social media account is compromised it is critical that you act fast.

We want to better understand the impact of you experiencing this issue, can you share your experience by filling in this online form? This will help us better protect future victims.

## Hacked social media account - Do this first!

1. **Change your password** - if you can still log into your account, follow the usual process to reset your password. Make this a strong password that you have never used before. If the password has been changed, try to reset your password using the 'forgot my password' link.
2. **Turn on two-factor authentication** - almost all good email accounts now give you the option to turn on two-factor authentication. Turn this on now. This site will help you understand what it is and tell you how to turn it on.
3. **Change your log in details for other sites that use the same - or similar - username and password** - any other online accounts with the same or similar log in details need to be changed immediately. It is highly likely that a cyber criminal will check other popular sites as soon as they get into your social media account.
4. **Report the unauthorised access to the social media provider** - Let the provider know your account was hacked and they will follow an evidence preservation procedure at their end. Useful if you need it in a legal case later. Some useful links below to help you do this.

## Approaches to dealing with a hacked social media account

Follow these steps now you have changed your password and turned on two-factor authentication:

1. **Remove any suspicious apps** - it may be a malicious application that has taken over your account. Review the apps connected to your account and remove any that you don't recognise or don't need.
2. **Check your security & privacy settings** - go into your accounts settings and find the security settings area. Check what devices are connected and disconnect any you don't recognise. Check recent log

ins and screenshot the information of unauthorised log ins - most provide time, date, IP address, browser type and device type. Ensure nothing has been changed to enable the hacker to regain access.

3. **Scan your devices for malware** - there are a number of ways the perpetrator may have got your log in details - from a past breach (you can check known breaches here), guessed it, seen you type it in or you may have told them in the past. However, they could also have placed malicious software on one of your devices, giving them access to what you type into websites. Scan all of the devices you use to access your account with an anti-virus solution and remove any malware.
4. **Check your recent activity** - review your recent posts, direct messages and general activity. See if you can find anything suspicious or may be used to scam others.
5. **Set up a recovery email** - if you haven't already, set up a recovery email or phone number. Go to your account settings and do this now. If you get hacked in future and get locked out of your account this will give you a way back in.
6. **Think about the repercussions of someone having access to the data in your social media account** - review what information is in your account and use it to make changes to limit what the criminal can do with it. For example if you have other passwords listed or bank details then take precautions to secure these accounts and change the exposed information.
7. **Warn others that your account was compromised** - if your connections were communicated with by the hacker then let them know it wasn't you and tell them they should look at their own security.
8. **If you are completely locked out** - if you have been completely locked out of your account then follow the providers account recovery process. If you have not set up the recovery process before you may need to raise a case with the provider and work to prove that you own the account.

## Link to social media provider guidance

The following takes you to information and guides from popular social media providers: Facebook, Twitter, Instagram, LinkedIn, YouTube, Pinterest, Snapchat, Reddit, Tumblr, Vimeo, Flickr, Periscope, Myspace.

## Report the crime

If you are in England, Wales or Northern Ireland you should report all cyber crime to Action Fraud. In Scotland, you can see details of reporting to Police Scotland here.

## How do I stop my social media accounts being hacked again?

1. **Get good at passwords** - use strong passwords, use different passwords on each site, never share them and change them regularly. Use a password manager app to help you do this. See some good guidance here.
2. **Commit to two-factor authentication** - two-factor authentication is a way to improve your security drastically in one easy step. Use it on every site that offers it. You can get more information here.
3. **Review account security settings** - all social media accounts offer a range of security features such as log in notification, secure browsing and two-factor authentication. Review these settings and turn all security options on.
4. **Be careful clicking or downloading** - tricking you to share your password by sending you spoof emails or texts is a really common way to have your passwords stolen. As is downloading attachments from emails that contain malicious software. Be extremely careful when clicking online links or opening/downloading online attachments.
5. **Get secure** - take time to improve your general online security. Use sites like Get Safe Online and Cyber Aware to understand what good security looks like and make changes.