A GUIDE TO SECURING YOUR ACCOUNTS, KEEPING SAFE, AND CAPTURING ONLINE EVIDENCE

TOP TIPS

Delete...
any images you are concerned about falling in to the wrong hands. Remember to empty your recycle bin/deleted photos and delete from the cloud.

Update...
your password to three random words.

Lock your phone homescreen...
either by thumbprint, password or pattern. Change your passphrase if you think someone might know it.

Setup 2 factor/phase authentication...
on your social media and email to prevent hacking.

Turn off...
location data in apps.

Set social media accounts to private...
delete friends you do not know or you no longer have a relationship with.

Review...
recovery email addresses and phone numbers linked to your social media accounts to ensure that these are all details your recognise.

Remember...
should anything happen, screenshot the evidence.

HOW DO I PROTECT MY ACCOUNT FROM BEING ACCESSED BY OTHERS?

01 USE STRONG PASSWORDS

Make your passwords stronger with three random words.

To create a strong password simply choose three random words. Numbers and symbols can still be used if needed, however, using three random words is the key to creating a strong password.

Your most important accounts are your email, social media and online banking. It's important to have strong and separate passwords for each account. With access to your email, individuals can take control of all of your online accounts.

Never use any word which is related to you and may be easy to guess. Examples of these are:

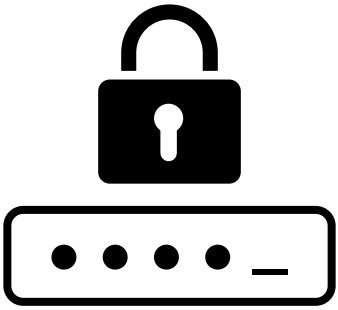
- Current partner's name
- Child's name
- Other family members name
- Pet's name
- Place of birth
- Favourite holiday
- Something related to your favourite sports team, artist or show.

And **NEVER SHARE YOUR PASSWORD** with anyone.

HOW DO I PROTECT MY ACCOUNT FROM BEING ACCESSED BY OTHERS?

Password management

You may also wish to consider getting a password management app that remembers your difficult passwords for you.



Have a look online for reviews of the best ones, and ensure you purchase a product safely through the Apple, Google or Play Stores.

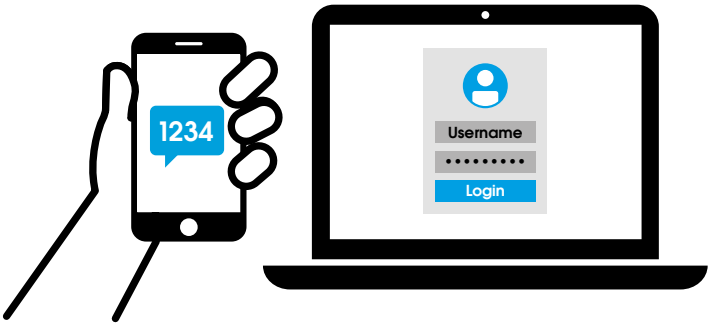
For further advice you may also wish to visit the following websites:

https://www.cyberaware.gov.uk/passwords

https://www.getsafeonline.org/protecting-yourself/passwords/

HOW DO I PROTECT MY ACCOUNT FROM BEING ACCESSED BY OTHERS?

02 SET UP 2 FACTOR AUTHENTICATION



Two factor authentication (2FA) is an extra layer of security on your accounts that not only requires your username and password but also something that you have on your person, such as a mobile phone or fingerprint. If someone were to try and gain access to your account, even if they had your usernames and password they would not be able to get further without having access to your phone and the text code.

HOW DO I PROTECT MY ACCOUNT FROM BEING ACCESSED BY OTHERS?

Setting up 2FA on Facebook

1. Select the three horizontal lines at the bottom right (iPhone) or top right (Android) of your homescreen
2. Scroll down to **Settings and Privacy > Settings**
3. Choose **Security > Security and login**
4. Select use **two factor authentication**
5. Follow the instructions on screen to set up

You can also choose up to 3 friends to contact if you are locked out, select this feature and add your trusted contacts.

There are several authentication methods you can use with your Facebook account when logging in from an unrecognised computer or mobile device:

- Text message (SMS) codes from your mobile phone
- Security codes from Code Generator
- Tapping your security key on a compatible device
- Security codes from a third party app

To view the full article on Facebook, visit:
https://www.facebook.com/help/148233965247823

HOW DO I PROTECT MY ACCOUNT FROM BEING ACCESSED BY OTHERS?

Setting up 2FA on Snapchat

1. On your Camera screen, **tap the profile icon** at the top left
2. **Tap the ⚙️ button** to go to your Settings
3. **Tap 'Two-factor authentication'**
4. Snapchat should guide you through the rest!

There are 2 different styles of two-step authentication:

- **Authentication app**: generate a security code using a trusted app such as Google Authenticator (iOS/Android) or Duo (iOS/Android). These are great if you use Snapchat on a tablet or on your phone while travelling abroad ✈️
- **Text verification**: Snapchat will send a security code in a text message to the phone number linked to your account. Standard messaging and data rates will apply. Bear in mind that if you don't have mobile service, you might not be able to receive a security code by text!

Recovery codes 🔄 If you lose your phone, change your phone number or lose access to your authentication app, then you'll need to use a recovery code to log back in.

To view the full article on Snapchat, visit
https://support.snapchat.com/en-GB/article/enable-login-verification

HOW DO I PROTECT MY ACCOUNT FROM BEING ACCESSED BY OTHERS?

Setting up 2FA on Apple devices

You can follow these steps on your iPhone, iPad, or iPod touch to turn on two-factor authentication.

1. Turn on two-factor authentication in Settings

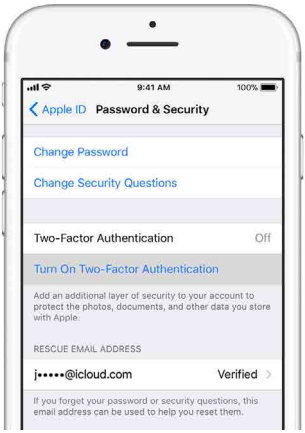
If you're using iOS 10.3 or later:

1. Go to Settings > (your name) > Password & Security.
2. Tap Turn On Two-Factor Authentication.
3. Tap Continue.

If you're using iOS 10.2 or earlier:

1. Go to Settings > iCloud.
2. Tap your Apple ID > Password & Security.
3. Tap Turn On Two-Factor Authentication.
4. Tap Continue.

You might be asked to answer your Apple ID security questions.



2. Enter and verify your trusted phone number

Enter the phone number where you want to receive verification codes when you sign in. You can choose to receive the codes by text message or automated phone call.

When you tap Next, Apple sends a verification code to the phone number you provided.

Enter the verification code to verify your phone number and turn on two-factor authentication.

HOW DO I PROTECT MY ACCOUNT FROM BEING ACCESSED BY OTHERS?

Setting up 2FA on Android devices

On your Android device go to Settings > User and backup section > Google > Sign in and Security > 2-step verification > Get started > sign in to your Google account and follow the step-by-step setup process.

Once you're finished, you'll be taken to the 2-Step Verification Settings page. Review your settings and add multiple verification methods. The next time you sign in, you'll receive a text message with a verification code. You also have the option of using a Security Key for 2-Step Verification.

Note: You may wish to also explore the `recovery phone' and `recovery email' options as well.

Further information can be found here:
https://support.google.com/accounts/answer/185839?hl=en

HOW DO I PROTECT MY ACCOUNT FROM BEING ACCESSED BY OTHERS?

Setting up 2FA on Outlook

Turn two-step verification on or off.

Go to the Security basics page, and sign in with your Microsoft account.

Select more security options.

Under Two-step verification, choose Set up two-step verification to turn it on, or choose Turn off two-step verification to turn it off.

Follow the instructions.

If you turn on two-step verification, you will always need two forms of identification. This means that if you forget your password, you need two contact methods. If you lose your contact method, just your password won't get you back into your account. For that reason, we strongly recommend you keep three pieces of security info on your account, just in case.

Setting up 2FA on Gmail

Visit the following website and login in to complete your security review
https://myaccount.google.com/intro/security

HOW DO I PROTECT MY ACCOUNT FROM BEING ACCESSED BY OTHERS?

03 TURN OFF YOUR LOCATION SETTINGS

iPhone:

Settings -> (select app eg: Facebook) -> Location -> **change option to Never**

Android:

Drag the toolbar down from the top of your screen and deselect location

Or:
Settings -> Location services -> **change access to my location to 'off'**

Or for individual applications:
Settings -> general apps/ app settings -> app permissions -> **de-select as appropriate**

SnapMaps

Ensure ghost mode is switched on

Settings -> See my location -> Ghost Mode -> **toggle to the right**

WHAT DO I DO IF MY ACCOUNT GETS HACKED?

04 GAIN CONTROL OF YOUR ACCOUNTS AGAIN

Report to the website:

Facebook:
https://en-gb.facebook.com/hacked

Snapchat:
https://support.snapchat.com/a/hacked-howto/

Instagram:
https://help.instagram.com/368191326593075

Gmail:
https://accounts.google.com/signin/recovery

Outlook:
https://www.microsoft.com/en-us/safety/online-privacy/hacked-account.aspx

05 GET PHOTOS TAKEN DOWN (REVENGE PORN)

Flag photograph to social media site indicating it violates their T&Cs. If you can no longer access the account, ask a friend to do this for you.

Google your name to see if the image is posted elsewhere, you may also wish to set up Google Alerts who will email you when new information about your name appears online www.google.com/alerts

Contact the Revenge Porn Helpline for further support:
Call 0345 6000 459 or visit https://revengepornhelpline.org.uk

WHAT IF SOMETHING HAPPENS?

06 CAPTURE THE FULL DIGITAL EVIDENCE

- Capture screenshots
- Don't delete messages until they have been viewed by an officer
- If you are concerned about losing the evidence or concerned about your account being hacked, email messages/ screenshots/ call-logs to yourself or a trusted friend, or back up on a USB stick
- It is always best to capture evidence from the desktop version of the site (screenshots of apps don't always give the full picture)
- When identifying a user on a social media site as being a suspect, ensure you capture the URL (eg www.facebook.com/Joe.Bloggs07782) as well as the profile details.
- If you have an iPhone you may also consider setting up screen recording on your phone. Enabling this feature will for example allow you to capture disappearing messages. However, please note that on Snapchat the sender will be notified that you are recording. For further information visit https://support.apple.com/en-gb/HT207935

WHERE CAN I GO FOR FURTHER HELP?

https://www.cyberaware.gov.uk

www.getsafeonline.org

https://revengepornhelpline.org.uk

https://www.internetmatters.org/advice/apps-guide

NOTES

WRITTEN BY
JOANNE BOCKO, CYBER PROTECT OFFICER, AVON AND SOMERSET POLICE