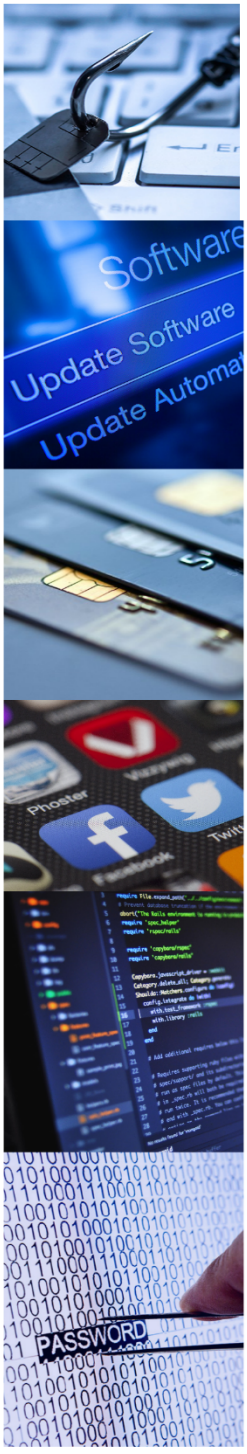
Crime prevention advice for

Two-Factor Authentication



Turn on two-factor authentication on your email

Two-factor authentication (2FA) is recommended for email accounts to make sure your data is secure.

Why do we want this? Because 2FA is the single best thing you can do to improve the security of your important accounts.

However good your passwords are, they can only provide so much protection. They could be stolen from your service provider or from your phone, tablet or laptop. Or you could get tricked into revealing them. Therefore, it's suggested that more people use 2FA, both at work and at home.

Accounts that have been set up to use 2FA will require an extra check, so even if a criminal knows your password, they won't be able to access your accounts. This is reassuring if you suspect some of your passwords aren't as strong as they could be, or you've re-used them across different accounts, or you worry that (like anyone) you may one day fall for a scam email that reveals your password to a criminal.

When setting up 2FA, the service will ask you to provide a 'second factor', which is something that you (and only you) can access. This could be a code that's sent to you by text message, or that's created by an app. Some types of 2FA provide more protection than others (because the second factor is more difficult to steal), but since any 2FA is better than none, you should use 2FA wherever you can. It only takes a few minutes to set up for each account, and it's well worth it for the additional protection it gives you.

How setting up 2FA can help protect your online accounts, even if your password is stolen.

How do I set up 2FA?

Some online services will already have 2FA switched on. However, most don't, so you will need to switch it on yourself to give extra protection to your other online accounts, such as email, social media and cloud storage. If available, the option to switch on 2FA is usually found in the **security** settings of your account (where it may also be called 'two-step verification').

Warwickshire County Council

Warwickshire POLICE

Philip Seccombe Police and Crime Commissioner for Warwickshire

Two-Factor Authentication

What are the different 'types' of 2FA?

When 2FA is switched on, you'll be asked to provide a second factor in order to access your account. There are several types of second factor available:

- **Text messages**. Most services tend to offer 2FA over text message by default. During setup, you provide your phone number, and the service will send you a message containing the code to use. Some services can also send a code using voice message if you find this easier. Text messages are not the most secure type of 2FA, but still offer a huge advantage over not using any 2FA. **Any two-factor authentication is better than not having it at all.**
- **Authenticator Apps** on your smart phone (or tablet) are the main alternative to text messages. Google Authenticator and Microsoft Authenticator are examples of this type of app. Once you've installed one, you can use the same app when setting up 2FA on any accounts that have this as an option. These apps offer lots of advantages over text messages, such as not needing a mobile signal, or having to wait for a text message to arrive.
- Some accounts also give you a list of **backup codes** when you switch on 2FA. When asked for a code you can use one of these, but each code will only work once, so you'll need to create more when you've used them all. Backup codes are really useful if you need to log on without a phone to hand. You will need to store the codes somewhere safe.

Do I have to use 2FA every time I access a service?

No. Once set up, you should only be asked for it when you're doing something where it would really matter if it was a cyber-criminal, rather than you. These are usually things like setting up a new payee for your bank account, logging into an account from a new device, or changing your password. This stops cyber-criminals from doing things that could harm you but means that you don't have to be checked every time. If you are asked for your second factor every time you log in on your own device, you can look for an option such as 'remember my device' or 'remember this browser'.