GUIDANCE

Setting up two-factor authentication (2FA)

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

Introduction

This guidance explains how you can set up two-factor authentication (2FA) on your important online accounts. Doing this makes it harder for criminals to access your online accounts, even if they know your password.

IT professionals who need advice on implementing 2FA across larger organisations should refer to the NCSC's separate guidance on multi-factor authentication for online services.

What is two-factor authentication (2FA)?

Two-factor authentication (often shortened to 2FA) provides a way of 'double checking' that you really **are** the person you are claiming to be when you're using online services, such as banking, email or social media. It is available on most of the major online services.

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.

Why should I use 2FA?

Passwords can be stolen by cyber criminals, potentially giving them access to your online accounts. However, 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.

The NCSC recommends that you set up 2FA on your 'important' accounts; these will typically be the 'high value' accounts that protect things that you really care about, and would cause the most harm to you if the passwords to access these accounts were stolen. **You should also use it for your email, as criminals with access to your inbox can use it to reset passwords on your other accounts**.

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').

The website **www.telesign.com/turnon2fa/tutorials** contains up-to-date instructions on how to set up 2FA across popular online services such as Gmail, Facebook, Twitter, LinkedIn, Outlook and iTunes.

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.

There are other second factors, that are offered by a few services. For example, some have apps that just ask you for permission once you've logged in. Others let you use 'security keys', which are small devices you can buy. You may also be able to use email as the second factor, provided it's a different email account from the one used to reset your password. If your account offers one of these, and you think it would work for you, then they are all good second factors.

It's also a good idea to have a backup plan, in case you haven't got access to your usual second factor (for example, if the battery on your mobile phone has run out). Many services let you set up more than one option for this reason. **Backup codes** are ideal for this, since they can be used even if you lose your phone.

Note that some services use memorable information or a security question (such as '*What was the name of your first pet?*') as an alternative to 2FA. These do **not** offer the same protection so you should still turn on 2FA if it is available.

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'.

What if 2FA isn't available?

The NCSC would like to see 2FA offered on all services which might hold your personal data, spend your money, or play another important role in your life. While many major services do offer it, there are still some that do not. If 2FA is not available on one of your important accounts, like email, **you should ensure that it has a strong unique password**. You may even want to consider changing services to one that does offer two-factor authentication.

PUBLISHED

7 August 2018

REVIEWED

7 August 2018

VERSION

1.0

WRITTEN FOR ⓘ

Individuals & families

Self employed & sole traders

Small & medium sized organisations