A BLUF Guide for LGBTQ+ people and activists

Securing your online accounts

Security matters

We're all in this together

If you've spent much time at all online, you've probably seen it – the Facebook post in which you're tagged along with dozens of other people, which appears to be from a friend, yet links to a website that seems completely random; the message that says "Hey, is this you in the video?" and includes a link for you to click. Or perhaps an email that says there's been suspicious activity on your account, and you need to follow a link verify your details.

All of these can be preludes to an account takeover, and are also often a sign that one of your online contacts has already had their account taken over. And that's a problem for all of us.

The first thought many of us will have if our account is hijacked is what a nuisance it will be, resetting passwords and getting control back – if we can. But as activists or LGBTQ+ people, there's another big problem. What it means for other people.

If your privacy on a site is compromised by hackers gaining access to it, it's not just you that is at risk. Someone who can access your account will be able to see your inbox, and sent messages. They can see the people you've been having conversations with, and they may be able to see personal profile information that wouldn't normally be accessible.

That means that when your account is compromised, the problem isn't just yours alone. It potentially compromises the privacy of other people on the site in question. That could be in the form of private messages revealing someone's sexuality or other personal information, or an otherwise invisible profile that reveals their kinks, or frank discussions about politics. And it goes without saying that, in some parts of the world, this information could literally be a matter of life and death.

So keeping your account secure isn't just a matter of looking after yourself. It's a vital part of keeping the whole community safe.

That's why we've produced this guide, to help show some simple steps that can protect both you and the people you share things with online.

What's the password?

Just about every site you use on the internet requires a password. It's the normal way of protecting your account, and you should choose something that's fairly easy to remember, but not to guess.

There are various ways you can come up with a good password, like using a line of a poem, and taking the first letter from each word, or including something you remember but others will find hard to guess – perhaps a childhood phone number, or part of a relative's postal code.

Some sites will impose rules which can make this trickier. If there simply has to be a punctuation symbol or a number, try changing a letter for a symbol that looks a bit like it, for instance changing a capital I for an ! or the letter A for 4.

There is a better way

Making up passwords like this can work, and you can probably remember a fair number of them. But these days, you are also likely to need to use a lot of sites. It can be tempting to use the same password on many of them, but you really should avoid that. It means that if someone gets access to one site, they can get access to all the others with the same credentials.

If you do try to make life easier for yourself this way, have at least a few different types of passwords. That way, even if someone can take over all your social media accounts with the same details, they can't use them to get into your bank account too.

However for the best password security, we recommend that you use a password manager. This is a program that can be installed on your computer or mobile phone, and can remember lots of different passwords for you, automatically filling them in when you visit a website.

Most password managers can also create random passwords for you too, with options to include numbers, special letters, and a mix of upper and lower case letters. That can help make your passwords very secure – and you don't even have to remember them.

For instance, at BLUF we use the LastPass password manager. There's a very long password needed to sign into LastPass once a day, but after that, it remembers all the passwords we need, and offers to fill them in on each site we visit. On mobile phones, it asks for our fingerprint to keep things even more secure, too.

LastPass can create really long passwords, up to 100 characters long, and is smart enough to realise when you're changing passwords on a site, and save the new one. Thanks to LastPass, we don't even know what our passwords are for most sites, and it doesn't matter.

All the information is securely stored in LastPass, and as long as we remember the master password, we're safe.

There's a cost

Unfortunately, the most popular password managers aren't free. LastPass still has a free version, which you can get from LastPass.com, but it can only be used on one type of device – you can't use it on both a mobile phone and your desktop computer without paying for the Premium version, which is £2.60 per month (£31.20 per year).

The chief competitor is called 1Password, and costs $2.99 per month ($35.88 or just over £25). You can download it from 1password.com. Both 1Password and LastPass have a free trial period, so you can see how you get on with them.

It's also worth noting that if you use a Mac or iPhone, then the built in Keychain can remember passwords for you, and Android phones also have similar functions. Both are free to use, but not in our opinion as flexible as the alternatives, especially if you use a mixture of different devices.

If you can't afford a subscription, the Dashlane password manager has a free plan. It's limited to one device, and only fifty passwords, but may be sufficient if you, for instance, you only use your phone to get online. Find out more at dashlane.com.

In short, if you want to keep secure online, we think it really is worth paying for a password manager. It's a relatively small price to pay for extra security – for you and those you're in contact with.

Don’t play games

One thing to be wary of when you create a password, whether you do it manually or with a password manager, is that there will probably be a way to reset it, and very often that’s in the form of security questions, like “What is your mother’s maiden name.”

If you forget your password, a site may present you with these questions, and allow you to create a new password.

And you may very well have seen ‘fun’ posts on sites like Facebook saying things like “Your drag queen name is the last thing you ate and your mother’s name before she married.”

Post the answer, and anyone reading now knows your mother’s maiden name, and might be able to reset your password, stealing your account. So, tempting though these memes and games may seem, always be careful before joining in, and try not to give away important personal information. You could be unwittingly helping someone gain access to your accounts.

The next level

Passwords are great, but they don’t solve everything. Many of the common types of security breach happen because people receive a link – like the sorts of message mentioned earlier – and when they click it, they’re asked to confirm some details, for example to sign in to Facebook, or some other service.

Often the screens presented can look incredibly like the real thing, but instead of connecting you to the site you think you’re visiting, your details are being harvested. Before you know it, posts might appear under your name, or contacts might receive fake messages, perhaps even asking for money.

Using a password manager can help with this: if you visit a genuine Facebook page, for example, your password will be filled in for you, but if you visit a site that’s just made to look like Facebook, the password manager won’t fill in your password, because it doesn’t recognise the address of the page.

However, you can usually still search for the right password, and have it filled in, thereby blowing a massive hole in your security.

So, how can you protect yourself from this sort of security nightmare?

Introducing two factor authentication

It's time to talk about two factor authentication, sometimes called 2FA. As the name hints, this adds a second bit of information that's necessary before access is granted to a web site. The idea is that to prove you are who you say you are, you need "Something you know, and something you have."

The "something you know" part is the password. The idea behind "something you have" is that there's some other detail that you – and only you – can provide.

So, when you visit a site, instead of just asking for your name and password, once you've entered those you'll be asked for the second bit of information, the "something you have."

You might have see this already, for example when you buy things online using a credit card, and your bank sends a code number in a text message, which you enter to confirm it's really you spending the money.

There are different sorts of two factor authentication – we'll explain them in more detail later – but the general idea is the same. By asking for the extra information, a site can be sure it's really you, and even if someone has managed to get your name and password, they still can't sign in and impersonate you.

Almost all the common account takeovers that you see on sites like Facebook or Twitter can be stopped by using two factor authentication.

Doesn’t this make everything more complicated?

Not really, because in many cases sites that allow you to use two factor authentication are quite clever about it, and you don’t have to use it every time. For example, on Facebook you’ll only be asked for the extra information when you try to log in from a browser that hasn’t been used before.

So, if you use the same computer every day, you won’t really notice any change, but if you go to an internet café on holiday and use their computer, you’ll be asked for the extra information.

However, if someone gets your login details by tricking you with a message, perhaps one of those “Is this you in the video?” tricks, they’ll be asked for the extra information, as Facebook won’t recognise their device as having been approved to use your account. That means they won’t be able to get into your account, and their takeover attempt has been foiled.

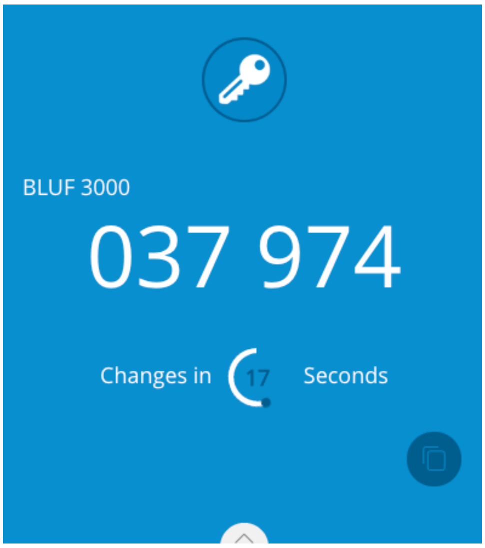
Some sites work the same way as Facebook, checking if you’ve used a particular device, while others will allow you to tick a box to say ‘remember this computer’. Some will ask at regular intervals, like once a week or once every fourteen days. Depending on the site, you may be able to customise how often it asks, and pick a level that you feel gives a good compromise between convenience and security.

Remember, if there’s a tick box when you log in to say “Remember me,” never use it on a computer you share.

Numbers and things

There are two main types of two factor authentication – numbers and things. What does we mean? Well, the most common type is where you are asked for a number, usually six digits long, to confirm your identity to a website.

In some cases, you can choose to have the number sent to your phone as a text message, while in others you open an app on your mobile phone or computer called an Authenticator, which will display a number for you to enter into the website.



If you're given the choice, we recommend an Authenticator app rather than a text message. That's partly because it's generally more secure (there are way to fake text messages that determined crooks can use), but also because an Authenticator app will still show you a number even if you don't have a mobile signal[1]. Who wants to be stuck in an internet café unable to check their messages because you can't get any bars on your phone? Later on, we'll explain how to set up an app called Authy, which is free.

So, in the case of an Authenticator or text message, the "something you have" is your phone. Unless someone has that, they can't access your accounts.

[1] The numbers in an authenticator app are created based on the time, and a secret bit of information from the website when you set it up

What about 'things'? Instead of using a code number, many web sites also support something called a Security Key. This is something that looks a little like a USB flash drive, but instead of storage, it has a unique identity built into it, and understands a set of rules to share that identity with the computer it's linked to.

With a security key you'll typically enter your user name and password as usual and then when the site asks for your second factor, you plug the security key into a USB port and touch the button. It's quick and really easy to use.

Codes or keys?

Which is best to use? Well, we can't give you a straightforward answer, but many of the most popular websites will let you use both an Authenticator and a security key, and offer you the choice of which you want to use when they need you to prove your identity.

Most Authenticator apps are free – Google has one, so does Microsoft, LastPass, and others. But a security key costs money; depending on the features you want – we'll explain in more detail later – they can cost from about £10–£75.

There are some situations where one obviously makes more sense than the other. For instance, if you have to go into an area where mobile phones are not allowed, then a security key is likely to be the better choice. If you're worried about theft too, people are probably more likely to steal your phone than something that looks like a USB drive on your keyring.

On the other hand, many of us always carry our phones with us anyway, so simply adding an additional app is a free and easy way to add extra security. And the cheaper security keys tend not to work with mobile phones – if you want one that plugs into your iPhone, or can communicate via Bluetooth, it will cost more.

Personally, we use a combination of the two – the Authy app on our phones, and a security key on the keyring. Both are almost always at hand, and we can use whichever is the most convenient.

When you set up two factor on many sites, you'll often also be given a set of 'emergency codes.' Typically, each of these codes can only be used once.

You should write them down or print them out, and store them somewhere secure – like a safe. If you lose your phone, for example, you can use one of the emergency codes to access the website. So too could anyone else who finds the list, so it's important to keep it somewhere secure.

We've included more information about choosing a security key later on in this guide.

Where to use two factor authentication

Broadly speaking, if you want to keep yourself and your community secure, you should use two factor authentication everywhere you possibly can. Most major websites support at least one type of it (though, sadly, many hook–up or dating sites don't).

In additional to Authenticator, text message or security keys, some sites will use their own app, sending a notification that you have to open and respond to. You'll usually be given a choice of which authentication method you'd like to use.

We'd recommend setting up Authenticator for most sites, and having security keys as an alternative, if you use sites that support them.

Authenticator can be used with (among others) Facebook, Twitter, Instagram, Amazon, Dropbox, PayPal, LinkedIn, Twitch, SnapChat, Yahoo, Github and Google.

Facebook, Twitter, Dropbox, Github and Google are among the sites that support security keys.

We strongly recommend all LGBTQ+ people, and especially activists and community leaders, enable two factor authentication on all their social media accounts, as a bare minimum.

Getting started with Authy

Now, we're going to look at using an app called Authy to set up two factor authentication. Authy is one of several apps that creates what you may see referred to as TOTP codes. That stands for Time-based One Time Password. Anywhere you see a reference to the Google Authenticator app (or other Authenticator apps) you can use Authy instead. All the apps use the same way of creating codes, so they're compatible.

To start using a site with an Authenticator app, the site will generate a secret code which is passed to the app. That code is then used to create a number which changes every 30 seconds or so. When a site asks you to verify your identity, you open your Authenticator app, select the site, and type in the current number. As long as the website and the app both have the correct time, the site can verify the number is right, and you're let in.

Usually, adding the secret code to the app is easy. The website will display a QR code – that's a square barcode – and you just take a photo of it with the app. The details of the site then appear on your phone screen. In some cases, the site may display a string of letters and numbers you can type in instead, but the QR code is much more common and simpler to use.

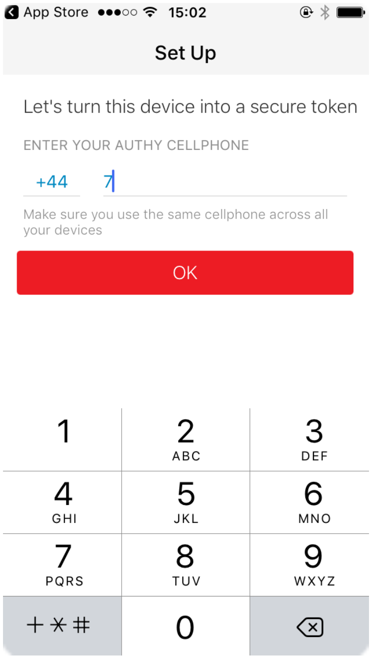
Why Authy?

If all the authenticator apps work much the same, why pick one? The main reason we prefer Authy is that it has built in synchronisation. That means that if you use more than one phone, you only have to add all the details of your sites once, and they'll be automatically copied between devices. You can install Authy on iPhones and Android, and there's also a version for Mac and Windows. They'll synchronise, so adding a site on one device will make it appear on all the others.

Some other Authenticator apps aren't as straightforward and while you may only use one device now, it can be very frustrating having to set everything up all over again if you upgrade your phone.

You can find Authy in the app store for your phone, or by visiting Authy.com, where you'll also find a load of useful guides for setting up two factor authentication on many different sites.

To start with, install Authy on the mobile phone you use most. The number of that phone can then be used to link other copies of Authy to the same account.



Set Up

Let's turn this device into a secure token

ENTER YOUR AUTHY CELLPHONE

+44 7

Make sure you use the same cellphone across all your devices

Visit the app store on your phone and search for Authy. The full name may appear as "Twilio Authy 2-Factor Authentication" – Twilio is the name of the company that makes the app. Tap to install it on your device.

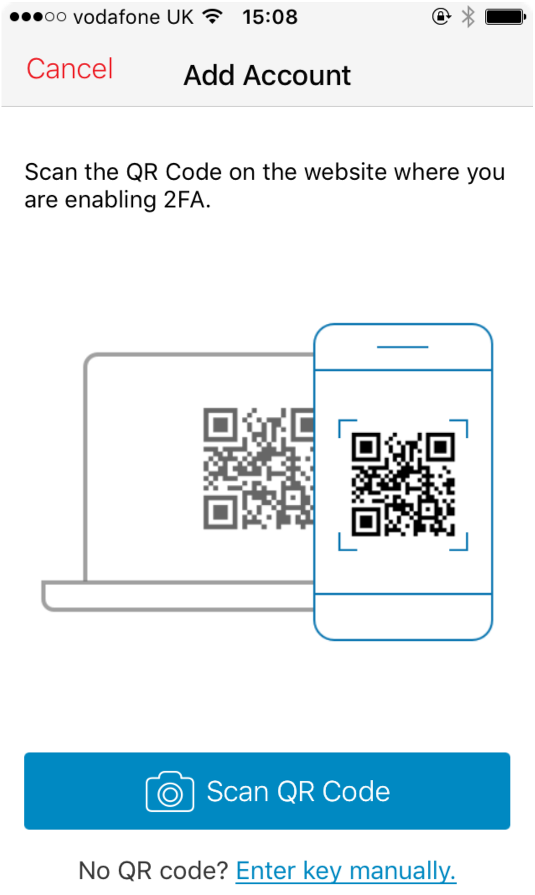
The first thing you'll be asked to do when you run Authy is enter your mobile number, then a verification code will be sent, which you need to enter into the app, to confirm the mobile number is correct.

Remember, if you install Authy on another device later and want to synchronise details, you should enter the number of the first phone on which you installed it.

Depending on your phone, you may be asked to grant Authy some permissions, including to use the camera. On older phones, this may happen when you first install or run the app, or it may happen when you try to add a site.

Adding Authy to your Facebook account

Now Authy is set up, let's see how it can be used to secure your Facebook account.



Scan the QR Code on the website where you are enabling 2FA.

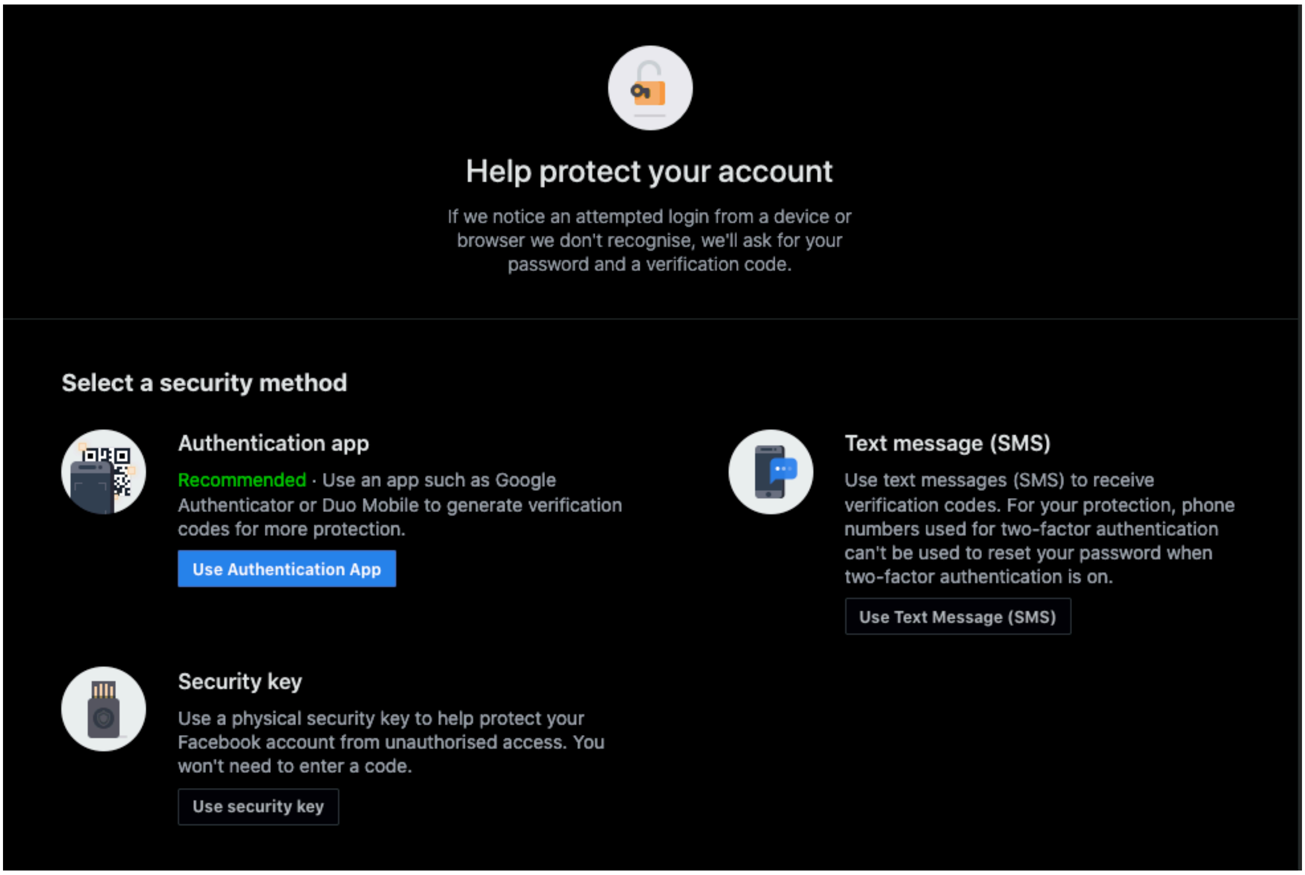
In the iPhone app, tap the cog wheel at the top right of the main Authy screen, then tap the *Accounts* icon at the bottom and finally click the + button top right again to reach the *Add account* screen.

If you're using an Android phone, click the three dots at the top right of the screen and select Add account.

You'll see a screen similar to the one shown here, with options to scan a QR code, or enter a key manually.

Now, head to your Facebook account. Click the downward pointing arrow at the top right of the screen, and select *Settings and privacy* then select *Settings* and finally click *Security and login*.

In the main part of the screen, click the *Edit* button next to *Use two factor authentication*.



Help protect your account

If we notice an attempted login from a device or browser we don't recognise, we'll ask for your password and a verification code.

Select a security method

Authentication app

Recommended · Use an app such as Google Authenticator or Duo Mobile to generate verification codes for more protection.

Text message (SMS)

Use text messages (SMS) to receive verification codes. For your protection, phone numbers used for two-factor authentication can't be used to reset your password when two-factor authentication is on.

Security key

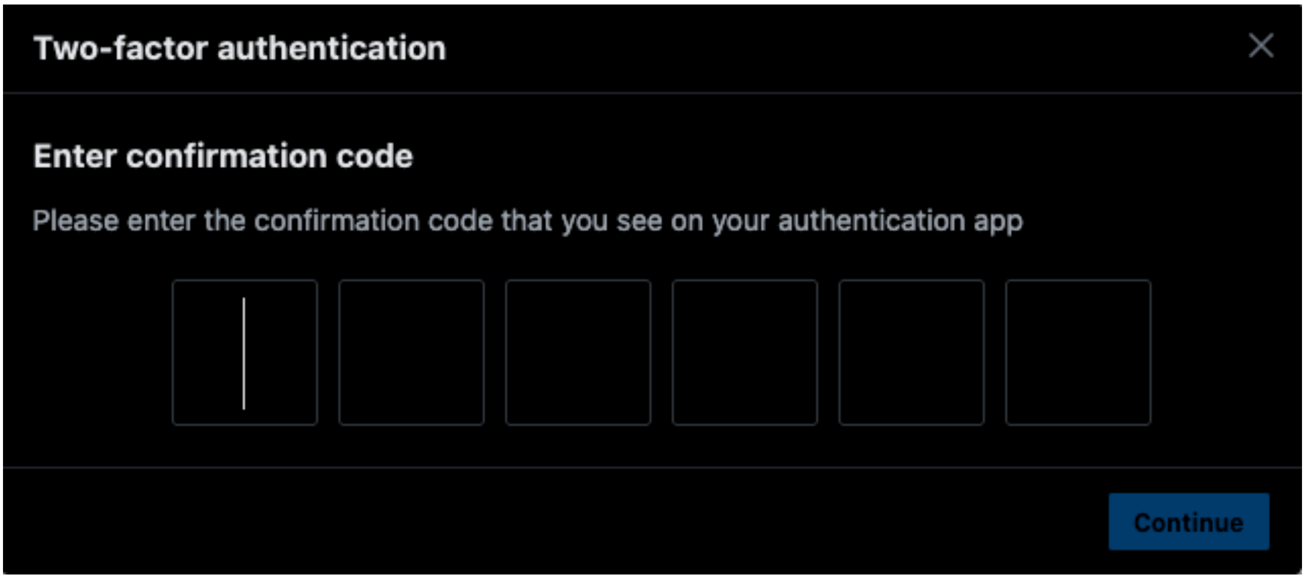
Use a physical security key to help protect your Facebook account from unauthorised access. You won't need to enter a code.

When you see this appear, click Use Authentication app. A new window will appear, showing a QR code, and a text version of the code. Pick up your phone and in the Authy app tap the *Scan QR code* button, and point the phone's camera at your computer screen.

Authy will work out your Facebook account name, but you can change that to something else if you like – that’s just used to help you find accounts in the app - then click Save.

On iPhone, tap Exit at the top left of the screen. On Android, you don’t need this extra step.

Now you’ll see your Facebook account shown in Authy, together with a code number and a count down. Go back to your web browser and click Continue, then you’ll be asked to enter the number from the app.


Two-factor authentication

Enter confirmation code

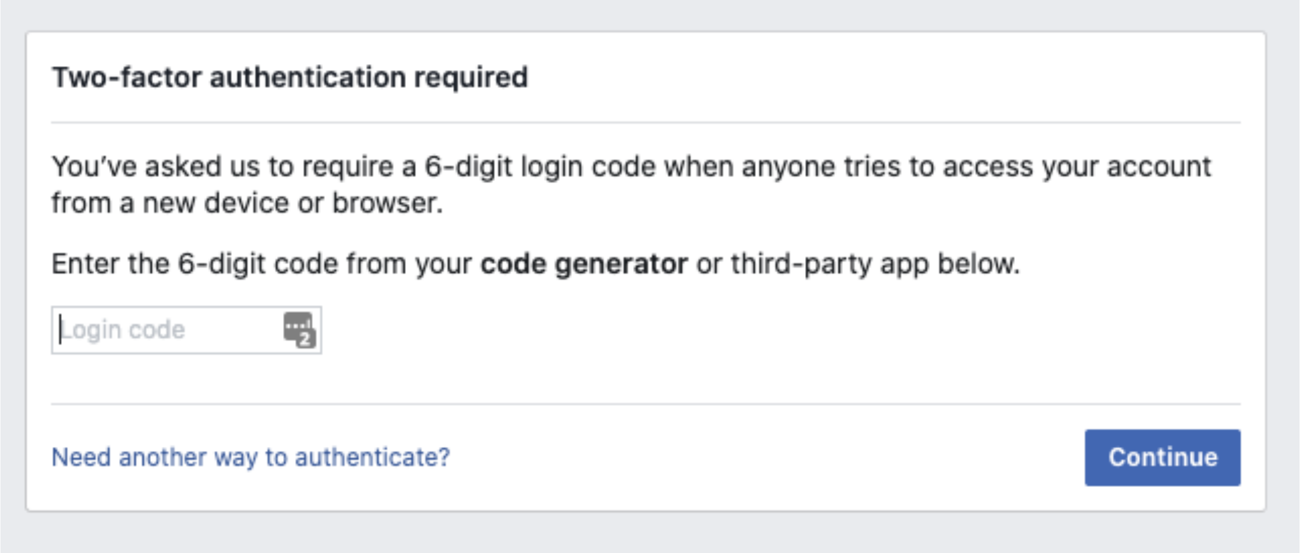
Please enter the confirmation code that you see on your authentication app

Type in the six digits from Authy and click Continue. If the countdown’s almost at zero, wait a few seconds until the number changes, to give yourself more time.

If the code is verified, you’ll see a confirmation message. Click Done and your account is now protected by two factor authentication.

Logging in to Facebook with Authy

Now, if you sign in to Facebook from a computer you haven't verified before, you'll enter your email address and password in the usual way, then you'll see this message

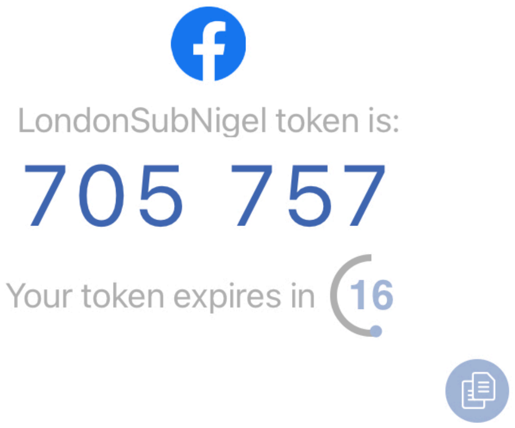


Two-factor authentication required

You've asked us to require a 6-digit login code when anyone tries to access your account from a new device or browser.

Enter the 6-digit code from your **code generator** or third-party app below.

At this point, grab your phone, open the Authy app, and select your Facebook account. Just like when you set the code up, you'll see your Facebook id, a six digit code number and a countdown.



LondonSubNigel token is:

705 757

Your token expires in 16

Just type the number into your browser and click on Continue, and you'll be logged into Facebook.

Incidentally, see that symbol bottom right in Authy? If you tap that, the current code is copied to your phone's clipboard, which is really useful if another app on the phone is asking for the code.

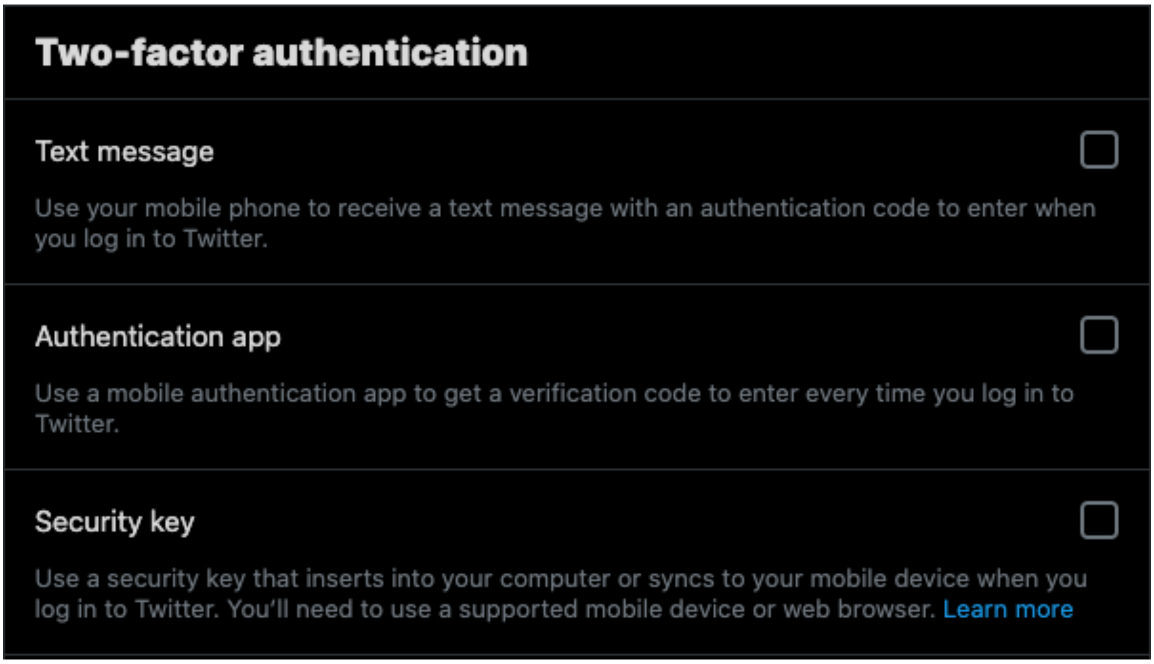
Setting up Authy with Twitter

We're going to assume you've set up Authy on your phone. To protect your Twitter account, start Authy, and tap to add a new account, as we described above.

Note that you need to have an email address associated with your Twitter account before you can enable two factor authentication.

On the Twitter website, click *More* then *Settings and privacy* and then *Security and account access.* Next click *Security* and finally *Two factor authentication.*

You'll see a list of methods that can be used, like this.



Two-factor authentication

Text message ☐

Use your mobile phone to receive a text message with an authentication code to enter when you log in to Twitter.

Authentication app ☐

Use a mobile authentication app to get a verification code to enter every time you log in to Twitter.

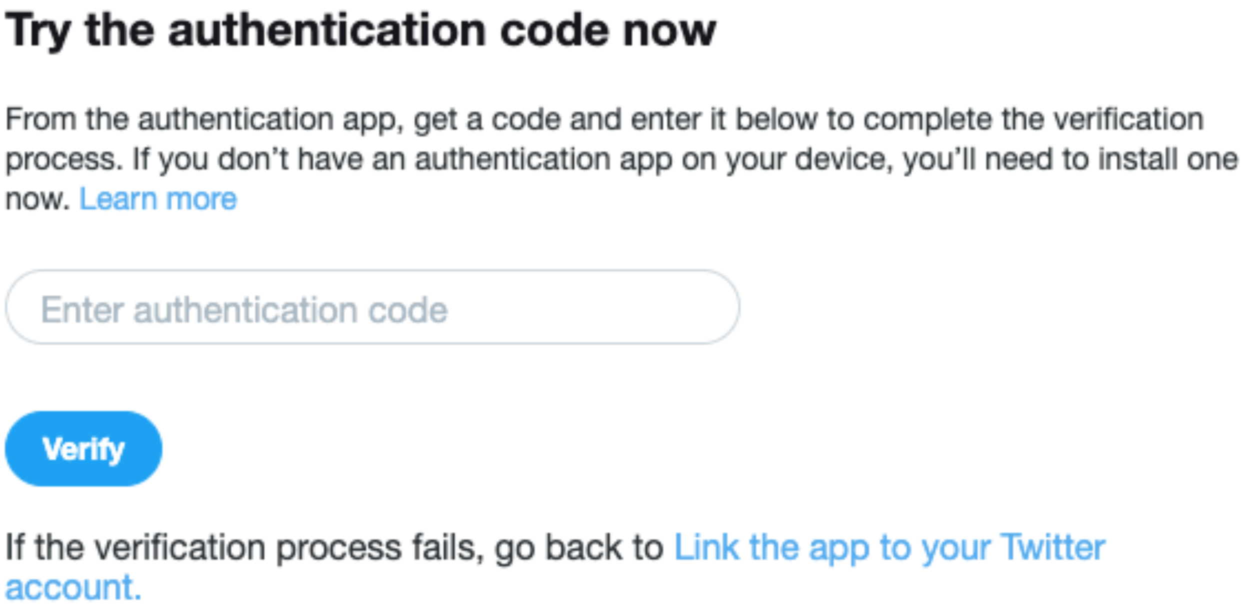
Security key ☐

Use a security key that inserts into your computer or syncs to your mobile device when you log in to Twitter. You'll need to use a supported mobile device or web browser. Learn more

Click the tick box for Authentication app and Twitter will begin to guide you through the process. Click Start on the Twitter screen, and you'll be shown a QR code.

Go back to your phone and in Authy, scan the code. Click to save then account and if you're using an iPhone, click Exit at the top left.

Back on your computer click Next. Now enter the code shown in Authy and click the Verify button.

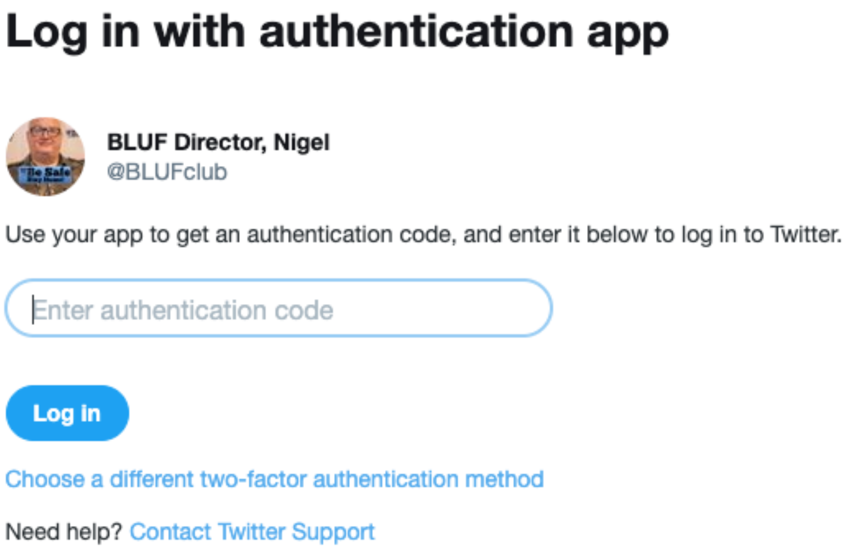


Try the authentication code now

From the authentication app, get a code and enter it below to complete the verification process. If you don't have an authentication app on your device, you'll need to install one now. Learn more

If the verification process fails, go back to Link the app to your Twitter account.

If all is well, Twitter will then show you a single use code you can also use. Write it down or save it in a safe place. Your Twitter account is now protected. When you sign in future, you'll see an extra screen like this one.



Log in with authentication app

BLUF Director, Nigel
@BLUFclub

Use your app to get an authentication code, and enter it below to log in to Twitter.

Choose a different two-factor authentication method

Need help? Contact Twitter Support

Other sites

Now you've seen how easy it is to set up Authy to work with Facebook and Twitter, and it's a simple extra step to log in with an Authenticator code.

The process works in a very similar way on most other websites. Just look for 'Two factor authentication' or 'Authenticator' or 'Google authenticator' in the login, account or security settings of a site or app, and follow the instructions on-screen.

Remember you can install Authy on other devices, and link them to your main one, using the phone number. You can also set a password for backing up information - and there are lots of step by step guides on the Authy website, including detailed information for many popular sites like Amazon, Google, LinkedIn, Microsoft, PayPal and more.

Choosing a security key

If you've decided you want to use a security key, you need to think about what you'll be wanting it for. You might even decide to buy more than one; many sites will let you have multiple keys linked to your account, so you can keep a backup somewhere safe, or on your spare keyring.

Standards

To make sure keys will work with different sites, there's a standard called U2F, for Universal 2nd Factor. It's from an organisation called FIDO, and when you're looking for security keys to buy, you should search for 'FIDO U2F.'

The latest version, FIDO2, includes the U2F standard and has new features that some sites will use in future to allow login without a password. If you have a choice, you should make sure you get a key that supports FIDO2, so it will last as long as possible.

Another term you'll see often is Yubico or Yubikey. The first is a company, and the second is their product. Most Yubikey products support U2F and also their own standard. They're considered some of the best around, but they are more expensive on the whole.

A major consideration when buying a key is what you will be using it with. For example, the cheapest keys are designed to fit in a standard USB socket; at BLUF that means they plug into a socket on the back of our keyboard, with is really convenient.

If you use a modern laptop, it might only have USB–C connectors, so you'd need a key compatible with that. For the iPhone, there are Yubikey models with a Lightning connector. You can also find some keys that have NFC – the same technology as contactless payment cards – built in. These can be used with Android phones, so when a website asks you to verify yourself, you tap the key against your phone; another alternative is a Bluetooth key.

Think about the places you might need to verify your identity, and the devices you'll be using, so you know what connectors your key will need. Remember you can have more than one.

On many keys, there's a small metal contact that you touch to activate them; generally this is not a fingerprint reader. There are a few security keys that do include one, but they're more expensive, and probably not necessary for most people.

That said, you shouldn't leave security keys lying around. Think of them as like your front door keys – if you leave your security key plugged into your computer all the time, it's like leaving your house keys in the lock. Anyone can come along and use them.

Using security keys – a quick overview

Before we look in detail at how you use security keys in practice, here's a quick overview – they work in much the same way on most websites that support them. Remember that you'll need to be using a fairly modern computer and web browser – if you're still on Windows XP, for instance, you're not going to be able to do this.

But if you have a PC or Mac from the last few years, or a recent mobile phone, you'll be fine.

Each security key has a unique identity coded into it, so no two are the same. You'll usually find security key options in the account or security section of a website's settings. Look for Two factor authentication and then Security keys, or U2F keys.

You may need to turn on two factor authentication first, and then specify that you want to use security keys. Then, typically, you'll click to add a key. The website will start the registration process and ask you to insert they key into a USB slot. As well as the message from the website, you might also see a pop–up message in your web browser, or from your computer's operating system.

Slide the key into a USB port, and when the light on it flashes, touch the button or contact. The key will exchange its details with the computer, and they'll be saved by the website. If you're using a Bluetooth key, you'll probably need to press a button on it, and if you're using one with NFC, tap it against your phone.

And that's all there is to getting set up. Now, when the web site wants you to confirm your identity, it will ask you to insert your key again, and you do exactly the same thing, proving your identity with a single tap.

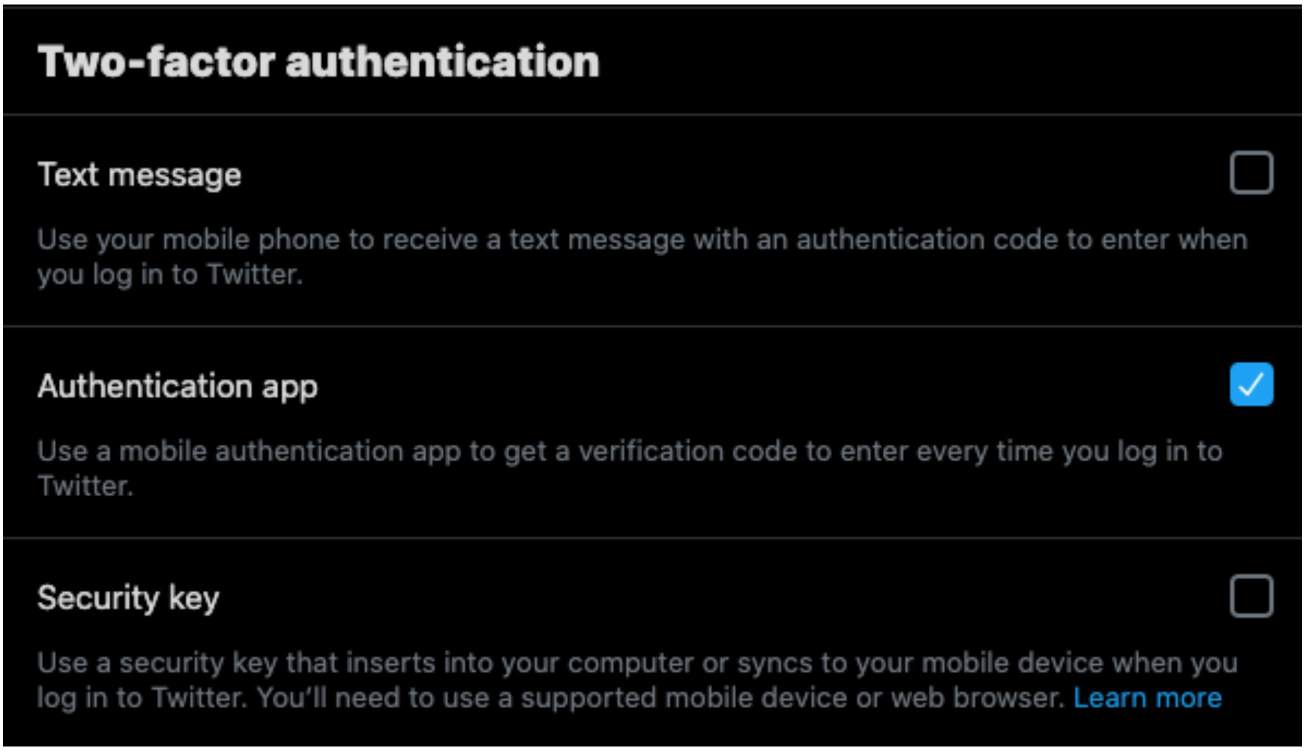
There will also usually be options to add extra keys and of course to delete them, if they've been lost. Most sites also allow you to add a descriptive name for each security key.

Adding a security key to your Twitter account

Now, let's see how it works in practice, looking at Twitter in this example. The process is very similar for other sites that support security keys, and you'll usually find the settings alongside those for other two factor options, so look under 'security', 'login' or 'account' settings to find them.

Sign in to Twitter then in the options on the left click *More*, followed by *Settings and privacy* then select *Security and account access* followed by *Security* then *Two factor authentication*.

You'll see a list of the types of authentication that can be used.



Two-factor authentication

Text message □

Use your mobile phone to receive a text message with an authentication code to enter when you log in to Twitter.

Authentication app ☑

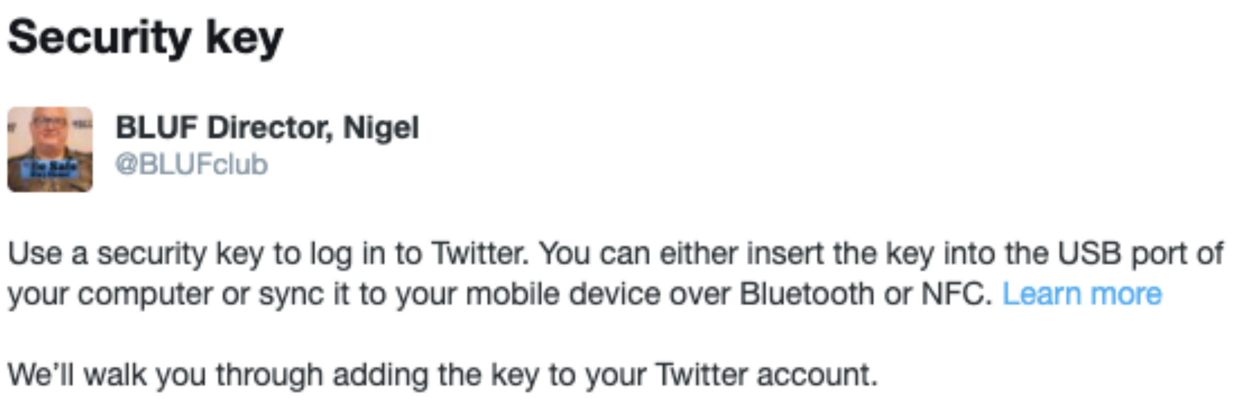
Use a mobile authentication app to get a verification code to enter every time you log in to Twitter.

Security key □

Use a security key that inserts into your computer or syncs to your mobile device when you log in to Twitter. You'll need to use a supported mobile device or web browser. Learn more

Click the checkbox next to Security key, and then enter your Twitter password when prompted (or let your password manager fill it in for you).

Now, Twitter wants to register your security key. You'll see a message like this on screen.



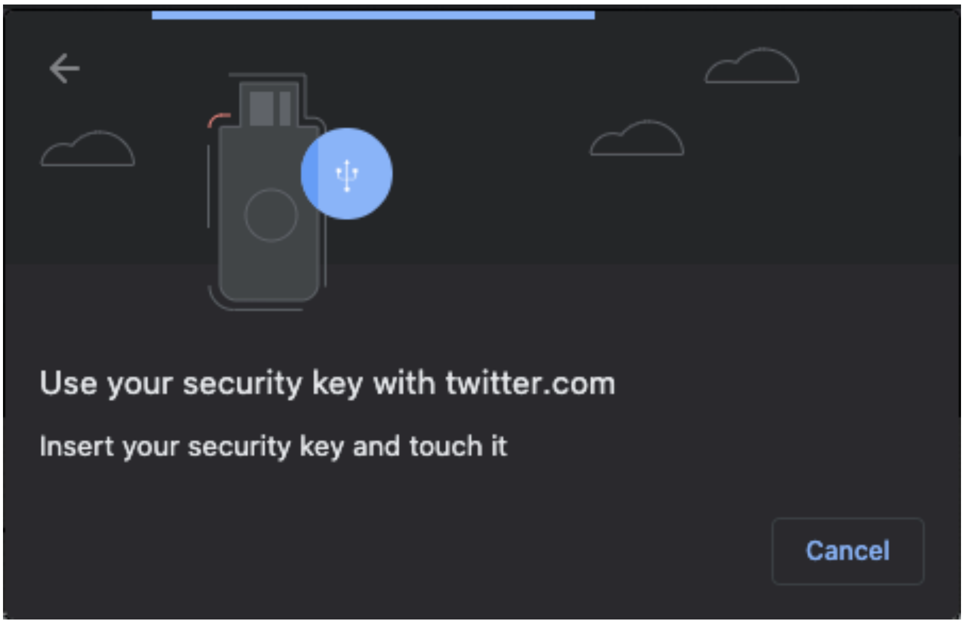
Security key

BLUF Director, Nigel
@BLUFclub

Use a security key to log in to Twitter. You can either insert the key into the USB port of your computer or sync it to your mobile device over Bluetooth or NFC. Learn more

We'll walk you through adding the key to your Twitter account.

Click the Start button just below it and a pop-up will appear - it may not look exactly like this, as the pop-ups are sometimes created by your web browser, or your computer's operating system, depending on what device you're using.

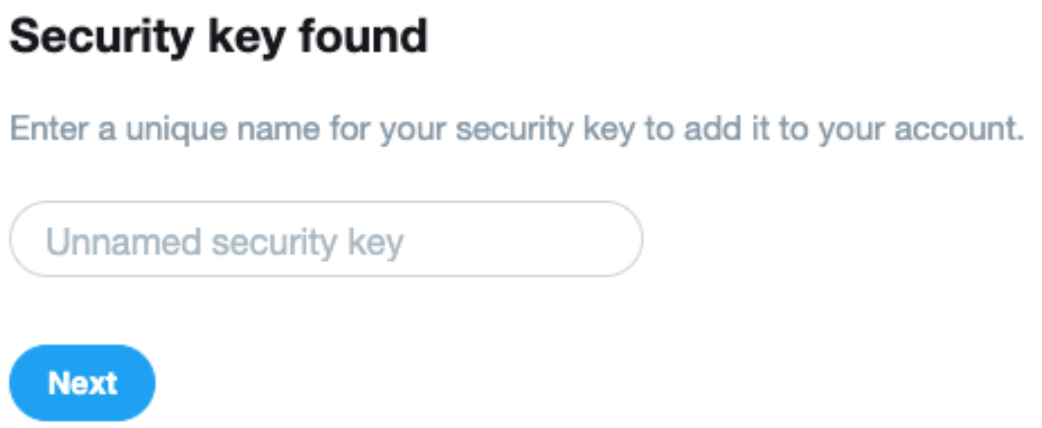


Use your security key with twitter.com

Insert your security key and touch it

Plug in your security key, if it uses USB. Then press or touch the button. If it's an NFC security key, you may need to hold it against the back of your phone, and if it uses Bluetooth, it will probably also have a button to press.

When the key has been detected, you'll see a message like this



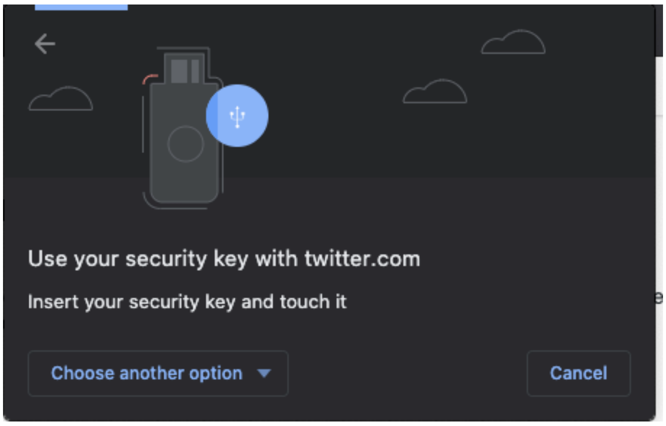
Security key found

Enter a unique name for your security key to add it to your account.

Unnamed security key

Fill in a name for the key, like *Nigel's main security key* and click Next. Twitter will display an emergency code, which you should write down or save in a secure location. You can use this code if you lose your key. Click 'Got it' to finish, and your account is now protected by a security key.

Now, when you log in, you'll see a pop-up message like this. When it appears, plug in your security key and touch the button. You can also click to select another authentication type, so it's quite easy to choose between Authy and security keys.



Use your security key with twitter.com

Insert your security key and touch it

As with using Authy, this process will be similar on all sites that use security keys. Once you've protected one account, it's easy to protect many more.

So, what are you waiting for? Securing your accounts is quick and easy to do - and it protects not just you, but the whole community.

Help! I've been hacked!

If you've downloaded this guide because you've already been hacked, here are some quick tips to help you get things back under control again.

Two of the most common sites, Twitter and Facebook, are also often used to provide authentication services for other sites – that's the 'Login with Facebook' option you see on some other sites.

It's convenient because you don't have to remember as many details, but it can also be a problem – it means that if one password is guessed, someone can have access to a lot of other information using the same details. (And let's not even think about the tracking that it enables Facebook to do).

Because of the way that these login systems work, they store information called "authentication tokens." You don't need the technical information – what it means in practice is that sometimes, changing your password after a hacker has obtained it isn't enough.

They may no longer be able to get into the account you just changed the password for, but if they used your password to access any linked sites in the meantime, they could still be able to access those.

So, as part of the clearing up after your password has been compromised, you should make sure you revoke permissions you gave from one website to another, and terminate any logins that might still be ongoing.

Ideally, this is what you should do if you get hacked:

1. Change your password. Pick a strong one or – better – use a password manager, and have it create a long password for you.

2. Disconnect any linked websites from your account, and terminate any sessions other than the one you're logged into. This means you'll have to log in again on your phone, for example.

3. Set up two factor authentication to protect your account in future.

4. Re-establish any links or authorisations that you still want to use. This is a good time to think whether you really do want information shared between sites.

Facebook

On Facebook, click the small arrow at the top right and then *Settings & Privacy*, then *Settings* and select the *Security and Logon* section.

Under the heading 'Where you're logged in' click to show all the devices currently logged in to your account. Then either click the dotted menu for each one you want to log out individually, or click

Log out of all sessions at the bottom of the list. If you do that, you'll then have to log back in again.

You should also click the Two factor authentication section, and review the list of *Authorised logins*. This shows devices where, even if it's turned on, Facebook won't ask for a security code. Tick the box and click Remove for any devices you don't recognise.

Then, from the left hand menu of the site, select *Apps and Websites*. You'll see a list of sites that you have used Facebook to log in to. You can view the details of each, or just tick the box to remove them. If you don't remember what a site is, that's a pretty good sign you should remove its link to your Facebook account.

It may be simplest to simply remove permission from everything, and then log back in to sites as and when you need them.

Twitter

On Twitter, from your home page click *More*, then *Settings & Privacy*. From the list of settings, click *Security and account access* then *Apps and sessions*.

Under *Sessions*, you can disconnect any other devices presently linked to your account. Click *Log out of all other sessions*, or select devices individually. Under *Connected Apps* you'll see a list – which can be surprisingly long – of all the apps that you have given permission to access your Twitter account.

This can look a bit scary, especially if you see things you don't remember. You can click on an app to see what it's allowed to do with your Twitter account. In many cases, it may be read only, which means the app can't do anything like pretend to be you, or send messages pretending to be you. In this category you might find things like WiFi hotspots that you signed in to using your Twitter details.

Apps that have 'write' permission can send tweets; you should think very carefully about whether you want these to stay. And you won't usually break anything permanently by removing an app. At worst, you'll just have to sign in to a website or app again.

Other sites

Although less common, you should check other sites where you might have used their login service too, if you think you might have been hacked. For example, Google, Amazon and eBay also allow you to link other services to your account.

It's a good idea to get into the habit of reviewing what's linked to different accounts from time to time, and remove anything you no longer use.

This guide © Nigel Whitfield

BLUF is the Breeches & Leather Uniform Fanclub, a social network for gay men of which I am Director. We aim to keep our site as secure as we can for members, and share useful information to help the broader LGBTQ+ community too.

All information correct at time of publication, May 2021.

Version 1.

E&OE.