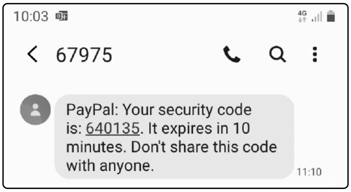
When a Password Isn't Enough, Use Your Mobile Phone to Boost Security

This article shows you:

✓ What two-factor authentication is and why it's useful

✓ How to set it up at the most popular websites

✓ How to find out whether you can use it at other websites


10:03

67975

PayPal: Your security code is: 640135. It expires in 10 minutes. Don't share this code with anyone.

11:10

Having read the name 'two-factor authentication', your first thought might be that you don't want anything to do with it! In fact, though, it's a very simple idea hiding behind a complicated name.

More importantly, it's something that's well worth knowing about, because it gives you a way to prevent criminals from hacking into your online accounts and stealing your money or your identity. Read on to discover what two-factor authentication is all about, why and when you need to use it, and how to set it up.

Two-Factor Authentication: What's It All About?

Don't be put off by the name!

Someone somewhere chose the name 'two-factor authentication'. With a whole dictionary full of words to choose from, they decided to put those three together. The result is something that (to most of us) doesn't seem to mean anything, but sounds truly intimidating!

Also known as 'two-step verification'

That's unfortunate because 2FA (as it's known for short) is a simple, valuable idea hiding behind a complicated name. Some people refer to it by names that make it sound rather less daunting: 'two-step authentication' or 'two-step verification'. The last of those might give you some clues what it's all about.

Two ways of proving your identify

It's about using two methods of proving who you are when you sign into a website, and as a result, forcing anyone with criminal intent to try to do the same if they want to break into your account.

Crucially, though, that doesn't mean using two passwords; that would make things too easy for the criminal. In general terms it means using any two of the following:

- **Something you know**: a password, a PIN number, your date of birth...
- **Something you have**: a phone, a credit card, a flash drive containing a particular file...
- **Something you are**: your fingerprint, your voice pattern, your face...

We already use this for card transactions

A good example of somewhere we use two-factor authentication already is when we pay for goods in a shop. We put our bank card ('something we have') into the machine and tap in our PIN number ('something we know'). Neither of those by itself is enough to make a payment successfully, so a criminal would need to steal or clone our card and discover our PIN before he could do any damage.

How two-factor authentication works online

All websites we use have been ‘one-factor’

Until very recently, all the accounts we’ve set up online have used ‘one-factor authentication’. Basically, that’s a password. It’s always combined with a username, but in most cases the username is our email address rather than some additional word or phrase we choose for ourselves.

You might think of this username+password pairing as two factors, but it’s really just one: both items fall into the ‘something you know’ camp, and your email address isn’t even particularly private.

Worse, a website has to store this username+password combination somewhere in order to compare it with what you type when you visit, and if a hacker is able to steal these details from the website, that’s all he needs.

The unavoidable problem with the ‘something you know’ items is that someone else might also know them, or be able to work them out, or guess them, or steal them.

Many now offer this extra security

Now, websites are increasingly offering us the option to add a second ‘factor’. You register your phone number with the website and, whenever you sign into your account at that website, it sends a numeric code to that phone number, usually as a text message.

A one-time code is sent to you by phone

Thus, as well as having to demonstrate you know the username and password for the account you’re signing into, you also have to demonstrate you’re in possession of the phone with that telephone number by typing the numeric code that’s just been sent to it. If you can’t supply both these proofs of identity, you won’t be allowed into the account.

A criminal may know your password, but doesn't have your phone!

More importantly, of course, the same applies to a criminal who's trying to get into your account. He may even have hacked into the website and found your username, password and telephone number in the list of customer details he stole. He can't get his hands on your phone, so he won't be getting into your account.

The exact form of this 'second factor' can vary. If you don't have a mobile phone and can't receive a text message, you can often give your home phone number and opt to receive a call from a recorded voice reciting the numeric code.

You might also be able to install a special 'authenticator app' which generates a code for you. In addition, we're just starting to have the option of using a fingerprint reader or some similar biometric gadget to prove who we are.

Where to use two-factor authentication

You wouldn't want to use it at every website

At the moment, few websites insist we use two-factor authentication, and many of those only require it in particular, unusual situations such as when you've forgotten your password. That's partly because it's annoying: anything that takes two steps when it could take one is going to slow us down. At the moment, you can arrive at a website, bash out your password and be in within seconds. Having to check your phone for a text message and then type the code adds extra time and trouble, and most of us would regard it as an irritation rather than a help.

Security vs convenience

Clearly, then, there's a balance to be struck between security and convenience! You've probably had to set up username+password accounts at a fair number of websites, and you don't want to start using two-factor authentication at all of them – you'd be forever waiting for text messages!

Use it where security really matters

Fortunately, you don't have to. It's only worth using for accounts containing something of value, or accounts where an intruder could wreak havoc. For example:

- Shopping websites such as Amazon that have your credit card details for one-click purchases.
- Cloud storage sites such as Dropbox where copies of your (possibly private) documents are stored.
- Payment services such as PayPal which have your bank or card details.
- Sites where you manage your banking, mortgage, investments, pensions and other financial dealings.
- 'Under-one-roof' services such as a Microsoft account, Google account or Apple account which may store your personal details, payment information, documents, photos and more.
- Sites where you didn't choose as strong a password as you should have, and which you know should be better protected. Rather than changing the password to make it more complicated (and more difficult to remember!), add two-factor authentication if the site offers it.

Get Set Up at Popular Websites and Services

Three popular sites you probably use

Although it's up to you where you use two-factor authentication, the catch is that not all websites offer it as an option. I'll show you how to find out which ones do on page 14, but in the meantime, to get you started, I'll explain how to set up two-factor authentication on a handful of the most popular sites – Amazon, PayPal, and Microsoft. You quite likely have an account at one or more of these sites, and they're all good candidates for that extra layer of security.

Amazon – www.amazon.co.uk

Your Amazon account has your personal and financial details

As well as storing your name and address, your order history and your recently-browsed products (which could all be useful to an identity thief or scammer), your Amazon account probably holds your payment details. If a criminal hacked into this account, he could potentially go on a spending spree at your expense.

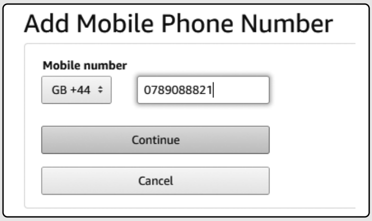
Protect it with two-factor authentication

This is why so many email scams are designed to look like messages from Amazon. Criminals would love to fool us into divulging our Amazon username and password at their fake website. By setting up two-factor authentication at Amazon, you can keep the criminals out. Here's what to do:

1. Start your favourite web browser, visit: **www.amazon.co.uk** and sign into your Amazon account. (To do that, click on **Hello, Sign in|Accounts & Lists** near the top-right of the page.)
2. After signing in you'll be back at the home page. Move the mouse to **Hello, [name]|Accounts & Lists**, and on the menu that appears click on **Your Account**.
3. On the 'Your Account' page, click on **Login & security**.

Add your mobile phone number to Amazon

4. On the page that opens next, click the **Add** button beside **Mobile Phone Number**. This takes you to the simple page pictured to the right: type your mobile phone number in the box (making sure there are no mistakes!) and click **Continue**.



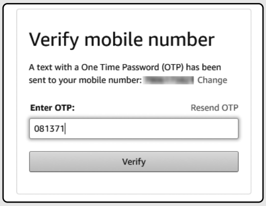
Add Mobile Phone Number

Mobile number: GB +44 0789088821

5. Now you'll see a 'Verification Required' notice which says it's going to send you a text message to verify your phone number: click **OK**.

Type the 'OTP' code you've just received

6. Within a few seconds, you'll receive a text message saying **081371 is your Amazon OTP. Do not share it with anyone.** ('OTP' stands for One Time Password. Of course, the code you receive will be different from mine.) Type that code into the **Enter OTP** box and click the **Verify** button.



Verify mobile number

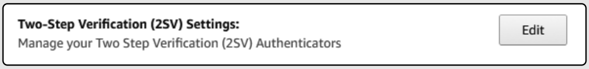
A text with a One Time Password (OTP) has been sent to your mobile number: [redacted] Change

Enter OTP: Resend OTP

081371

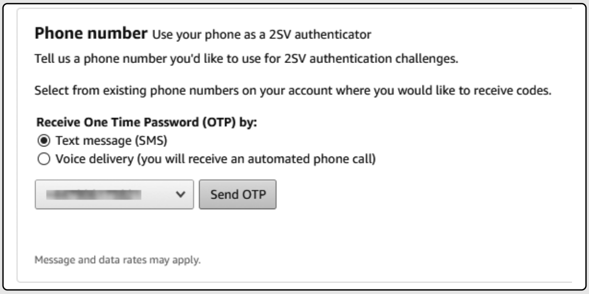
Now set up two-step verification

7. Now you'll be returned to the Login & security page you reached after step 3. This time, beside the words **Two-Step Verification (2SV) Settings**, click the **Edit** button and then click **Get Started**.



Two-Step Verification (2SV) Settings:
Manage your Two Step Verification (2SV) Authenticators

8. On the next page, make sure that the option **Text message (SMS)** is selected, and that your mobile phone number is selected in the drop-down list below, and then click the **Send OTP** button.



Phone number Use your phone as a 2SV authenticator

Tell us a phone number you'd like to use for 2SV authentication challenges.

Select from existing phone numbers on your account where you would like to receive codes.

Receive One Time Password (OTP) by:
● Text message (SMS)
○ Voice delivery (you will receive an automated phone call)

[redacted]

Message and data rates may apply.

9. Once again, Amazon will send a code to your phone, and a box for the code will appear on the web page. Type the OTP code into that box and click **Continue**.

Enter a security code every time

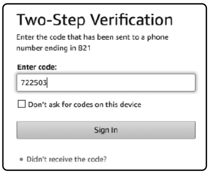
10. Finally you arrive at an ‘Almost finished’ page which explains a couple of extra things. In particular, you’ll see an option that lets you avoid entering codes when you sign in using the web browser you’re currently using. In other words, when you use this browser on this PC you’ll continue to sign into Amazon using just your username and password, but on any other devices you use (and – crucially – any device a criminal may be using!) a code must be used. If you want to do this, you can tick the box beside **Don’t require OTP on this browser**. Finally, whatever you decided for this, click on **Got it. Turn on Two-Step Verification**.

Done

11. This will take you back to the ‘Two-Step Verification (2SV) Settings’ page which now looks different, showing your mobile phone number and letting you make changes (including, if you ever decide to, switching off two-step verification). Now you can carry on browsing Amazon or, if you choose to, sign out and close your browser.

How to sign into Amazon in future

In future, assuming you haven’t told Amazon to skip security codes in the current web browser, you’ll visit **www.amazon.co.uk** and sign into your account by typing your username and password and clicking the **Sign In** button, just as you always have done. At that point, you’ll see this extra step prompting for a code that has been sent to your mobile phone. Type that code and click **Sign In** and you can carry on using Amazon just as you always have done from this point.



Two-Step Verification

Enter the code that has been sent to a phone number ending in 821

Enter code:

722503

□ Don’t ask for codes on this device

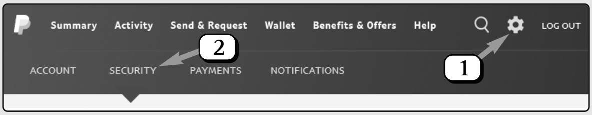
PayPal – www.paypal.co.uk

PayPal has your bank and/or credit card details

A PayPal account allows you to buy for goods and services at an enormous number of websites without the palaver (and risk) of entering all your contact details and payment information at those sites. You simply choose the option to pay using PayPal, then sign into your PayPal account with your username and password to confirm the payment.

Of course, as PayPal obviously does have your contact details and payment information, that makes your PayPal account a popular target for criminals and a prime candidate for two-factor authentication. Here's how to add that extra security to your PayPal account:

1. Start your favourite web browser, visit: **www.paypal.co.uk** and sign into your account (by clicking **Log In** at the top of the page).
2. After signing in, click the cog-shaped icon 1 on the blue bar at the top-right of the page followed by **SECURITY** 2.



Set up 2-step verification

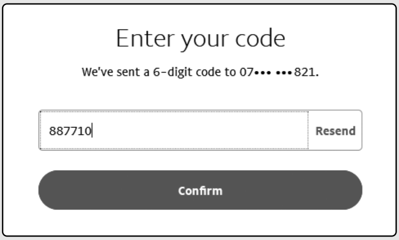
3. Now you'll see a list of security-related items you can update (your password, security questions, and so on). Alongside the words **2-step verification**, click on **Update**.
4. On the pop-up panel that appears, make sure **Text me a code** is selected and click on **Set up**.

Enter your mobile phone number

5. The panel changes to prompt you to enter your phone number. Type it into the **Mobile number** box and then click **Next**.

Type the security code you've received

6. Within a few seconds you'll receive a text message saying **PayPal: Your security code is 887710. It expires in 10 minutes. Don't share this code with anyone.** (Of course, your own code will be different from mine.) At the same time, the pop-up panel on the web page has changed to a box that's waiting patiently for this code: type the code into the box and click **Confirm**.



Enter your code

We've sent a 6-digit code to 07••• •••821.

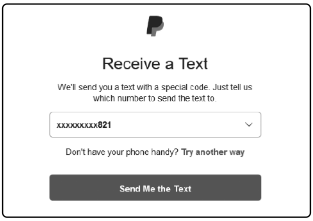
887710 | Resend

Confirm

Signing into PayPal in future

7. Finally, you'll arrive at a page confirming that you've successfully added 2-step verification to your account. Click the **Done** button at the bottom and you've finished.

In future, whenever you sign into your PayPal account – most likely because you're about to pay for something – you'll enter your username and password and click Log in in the usual way, but then you'll arrive at the additional step pictured to the right.



Receive a Text

We'll send you a text with a special code. Just tell us which number to send the text to.

xxxxxxxxx821

Don't have your phone handy? Try another way

Send Me the Text

PayPal sends you a text message

Here, click the **Send Me the Text** button. You'll be taken straight to another page asking for the security code you've just received at that mobile number: type the code and press Enter (or click **Continue**) and you're in.

Microsoft – www.microsoft.com

Access to services – and private details!

If you use Windows 10 or Windows 8.1, you quite likely have a Microsoft account whose username and password you use to sign into your PC. But that account gets you into a range of Microsoft services online as well. Perhaps you use the Outlook.com webmail service, or store files at the OneDrive cloud storage service? Or maybe you have a subscription to Microsoft 365, or buy apps from the Windows Store, in which case your Microsoft account has your payment details.

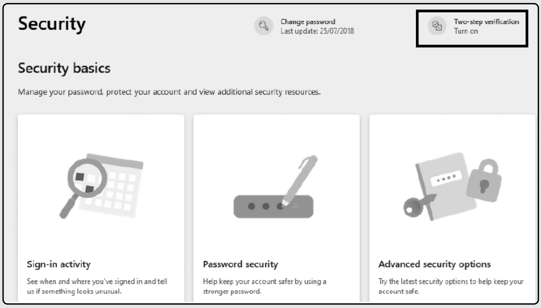
How to protect your Microsoft account

Since that single account can do so much, it's wise to protect it with more than just an email address and a password. Here's how to set up two-factor authentication for your Microsoft account:

1. Start your favourite web browser, visit **account.microsoft.com** and sign into your account (by clicking **Sign in** in the top-right corner of the page).
2. This takes you to your personal account page, which is divided into eight sections, each in its own box, such as 'Subscriptions', 'Family' and 'Devices'. Click somewhere in the **Security** box.

Set up two-step verification

3. At the top of the 'Security' page that opens, click the words **Two-step verification|Turn on**.



Security

Change password
Last update: 25/07/2018

Two-step verification
Turn on

Security basics

Manage your password, protect your account and view additional security resources.

Sign-in activity

See when and where you've signed in and tell us if something looks unusual.

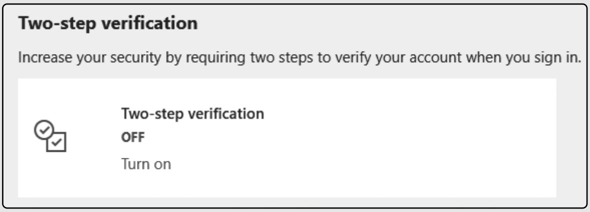
Password security

Help keep your account safer by using a stronger password.

Advanced security options

Try the latest security options to help keep your account safe.

4. On the next page, you'll find the 'Two-step verification' section pictured below. Click the blue words **Turn on**.



Two-step verification

Increase your security by requiring two steps to verify your account when you sign in.

Two-step verification

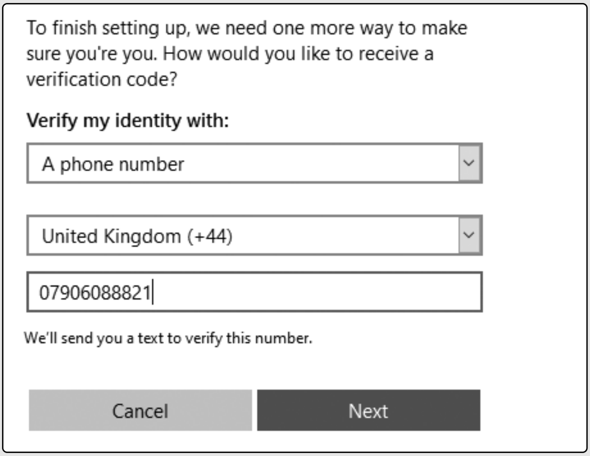
OFF

Turn on

5. This takes you to another page which explains roughly what's going to happen next. There's nothing to change on this page: just click **Next**.

Enter your mobile phone number

6. This takes you to the simple page pictured below. Open the drop-down list headed **Verify my identity with** and choose **A phone number**. Then, in the box below, enter your mobile phone number (making sure there are no mistakes!) and click the **Next** button.



To finish setting up, we need one more way to make sure you're you. How would you like to receive a verification code?

Verify my identity with:

A phone number

United Kingdom (+44)

07906088821

We'll send you a text to verify this number.

7. Within a few seconds you'll receive a text message from Microsoft saying **Use 4924 as Microsoft account security code.** (Of course, your own code will be different from mine, and it may be longer – Microsoft's codes vary in length from 4 to 8 digits.)

Type the code you've received

8. At the same time, you'll find that you've arrived at a new page prompting you to enter the code you've just received. Type that code and click **Next**.

Copy or print your 'recovery code'

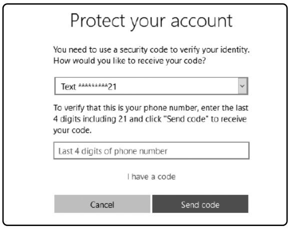
9. Now you'll reach a page confirming that two-step verification is now turned on. This page also gives you a long 'recovery code' that can be used to regain access to your Microsoft account if you should ever lose the other methods of proving your identity. It's a good idea to write this down or print this page. (If you click the **Print code** link it will open a new tab in your browser which will then be printed. Close this tab afterwards.) When you're ready, click **Next**.

These steps may apply (but probably don't!)

10. Now you'll reach a couple more steps that explain what to do if you use your Outlook.com email account on a mobile phone, and after clicking **Next** again, what to do if you use certain other Microsoft programs and devices. You can read this now or skip past it – you'll also receive an email containing the same details and giving you a link to click to do any additional setting-up that's needed. Finally, click the **Finish** button and sign out of your Microsoft account.

How to sign into your Microsoft account in future

In future when you sign into your Microsoft account online, you'll enter your email address, then your password, and then you'll see the extra step pictured to the right. In the upper box, choose how your security code



Protect your account

You need to use a security code to verify your identity. How would you like to receive your code?

Text *********21

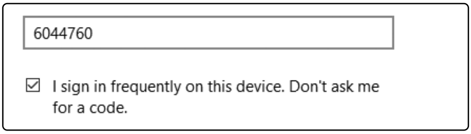
To verify that this is your phone number, enter the last 4 digits including 21 and click "Send code" to receive your code.

Last 4 digits of phone number

should be sent to you (either via one of the phone numbers registered with your Microsoft account or one of its email addresses). If you opted for a phone number you'll be asked to enter the last four digits of that number in the lower box; for an email address you'll be asked to supply the complete email address.

Type the code you've just received

Do that and click the **Send code** button, and the code will be sent to you in a text message, in an email message or via a voice call, according to which method you chose. At the same time, your browser will take you to a page in which the code has to be typed:



6044760

☑ I sign in frequently on this device. Don't ask me for a code.

Enter a security code every time?

You'll notice there's a tick beside the option **I sign in frequently on this device. Don't ask me for a code.** Assuming you're signing in to this account on a device you own and use regularly, you can leave this tick in place to avoid having to receive and type a security code every time. If this isn't your device, be sure to remove this tick. Finally, click the **Submit** button and you're in.

Find Out What to Do for Your Other Accounts

See which websites offer two-factor authentication

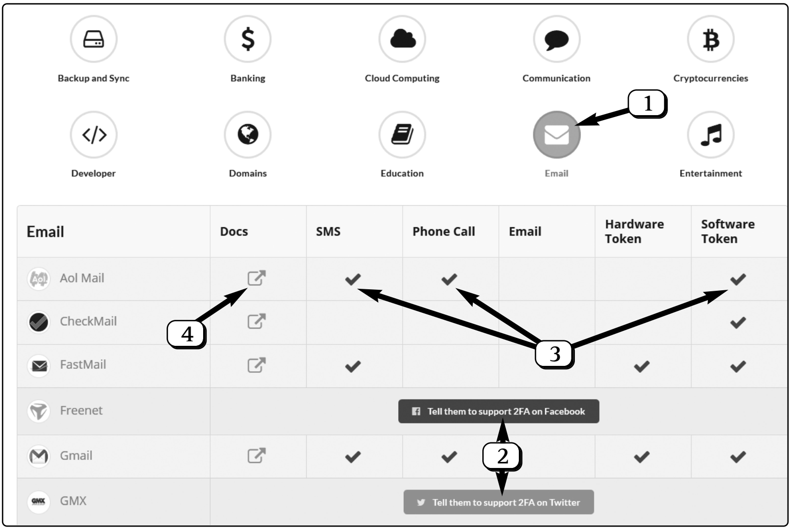
You know which online accounts you have that could do with some extra security, but how can you find out whether they offer two-factor authentication? Normally you'd have to visit each site and look through its security-related options, as in the examples above, but fortunately there's a much better way – a website named Two Factor Auth which maintains a list.

Click a category icon

Visit twofactorauth.org and you'll arrive at the page pictured below. Initially you'll see a collection of circular 'category' icons, and one way to use this site is to click an icon (1).

When you do that, the lower icons slip downwards, out of the way, and a table appears below the category you clicked. This table lists websites that fall into the category you clicked and tells you whether or not they support two-factor authentication.

For sites that don't, you'll see wide buttons (2) beside their names which you can click to post a request to the site's Twitter or Facebook page asking them to do so. Whether you do that is up to you (and also requires that you have a Twitter or Facebook account), but it obviously won't make anything happen immediately.



Email	Docs	SMS	Phone Call	Email	Hardware Token	Software Token
Aol Mail	↗	✓	✓			✓
CheckMail	↗					✓
FastMail	↗	✓			✓	✓
Freenet	Tell them to support 2FA on Facebook					
Gmail	↗	✓	✓		✓	✓
GMX	Tell them to support 2FA on Twitter					

See what options are available

For sites that do support two-factor authentication, you'll see ticks indicating which methods they offer (3). The options are to send you a security code by SMS (text) message, voice phone call or email, or to have a security code generated by a 'hardware token' (a keyfob-sized device with a small screen) or a 'software token' (an app you can install).

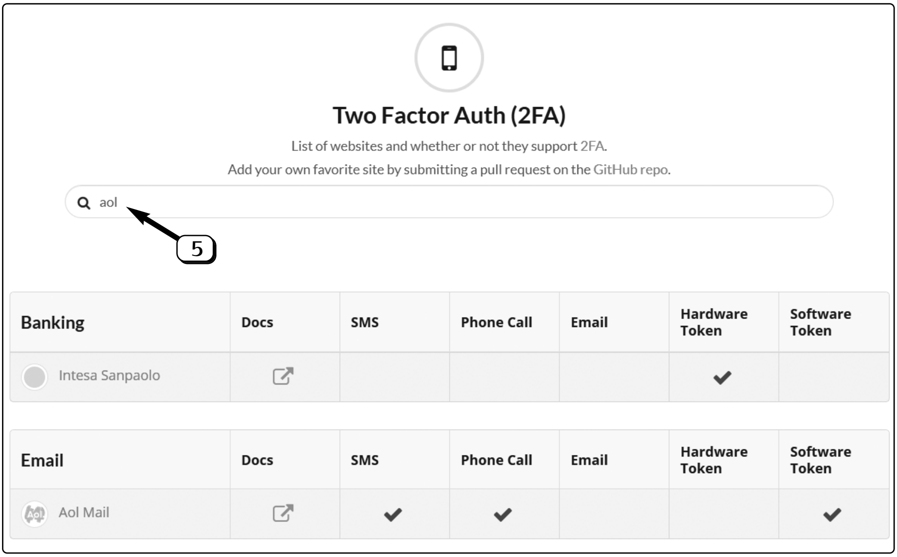
Click the 'Docs' icon to visit the website itself

So, you can quickly determine whether a particular site supports two-factor authentication, and how it does so, but what next? Simple: click the icon in the 'Docs' column (4) and you'll be taken to the appropriate page on the corresponding website where you can read how to set it up on that site.

That's all very well, but if you're looking for a particular website at Two Factor Auth, how can you be sure what category you'll find it in?

Use the search box to quickly find a certain website

A better way is to use the search box near the top of the page. Just start typing the name of the website you're interested in (5), and details of the websites whose names contain the letters you've typed will appear:



Two Factor Auth (2FA)

List of websites and whether or not they support 2FA.

Add your own favorite site by submitting a pull request on the GitHub repo.

Banking	Docs	SMS	Phone Call	Email	Hardware Token	Software Token
Intesa Sanpaolo	↗				✓	

Email	Docs	SMS	Phone Call	Email	Hardware Token	Software Token
Aol Mail	↗	✓	✓			✓