EAST MIDLANDS CYBER SECURE

A Comprehensive Guide To Two Factor Authentication

DERBYSHIRE CONSTABULARY

NOTTINGHAMSHIRE POLICE

LEICESTERSHIRE POLICE

LINCOLNSHIRE POLICE

NORTHAMPTONSHIRE POLICE

If you find yourself the victim of a cybercrime, report it to...

ActionFraud

National Fraud & Cyber Crime Reporting Centre

0300 123 2040

https://www.actionfraud.police.uk

For more information about cybercrime and cybersecurity visit...

EAST MIDLANDS CYBER SECURE

https://www.eastmidlandscybersecure.co.uk

What is 2FA?

Two-factor authentication (or sometimes called 2 step verification) provides a way of verifying 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 major online services.

Most Services allow you to verify your identity in two ways. Firstly you can have a SMS text message sent to your phone with a unique, one time code that you redeem to verify. Or, you can link the service with an approved authenticator app which will generate unique one time codes that you redeem. You can also have security keys which are one time use verification codes, once you have used them all you will need to generate new keys.

SMS text messages are useful as they do not require internet or data however the authenticator app bypasses the need to have mobile service and could be still used if your mobile provider has an outage. It id up to individual preference which service you choose.

Why Use 2FA?

Passwords can be stolen by cyber criminals or obtained via data breaches, 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.

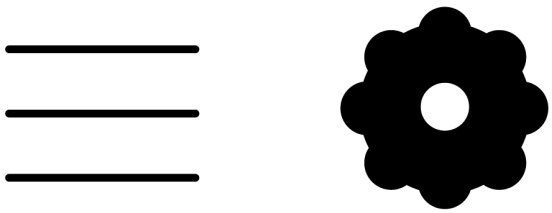
It can also act as a notification as if you recieve a code but did not attempt a login, this means someone has successfully tried to login with your password and you need to change it.

It is reccomended that you enable 2FA on all of your important online accounts, especially email accounts as a hacker could use a compromised email account to reset the passwords of other online accounts.

facebook

emcybersecure

1

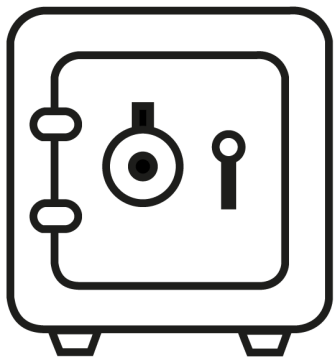


Go to Menu and then click on the settings icon which looks like a cog.

2

Go to Account and then to Password and Security.

3



Select the form of verification and follow the on screen instructions.

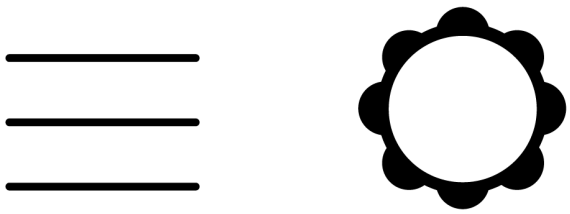
You can choose to use your phone number to verify or authenticator apps.

Like Comment Share

Instagram

EMCyberSecure • Follow

1



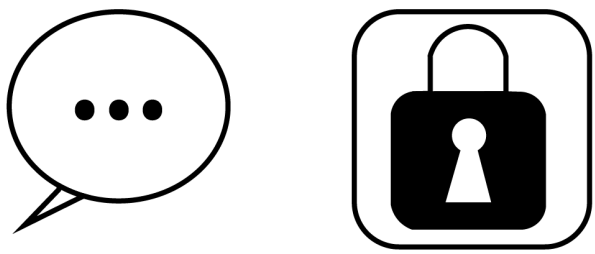
Go to your profile and click on the three lines icon. Then go to settings.

2

Go to Security and then click on the two factor authentication tab.

3

Tap the get started button and follow the on screen instructions.



Instagram allows for verification by SMS text or authenticator apps.

Edit

Chats

Search

Broadcast Lists

New Group

Setting up 2FA on Whatsapp

Step 1: Open Whastapp and go to the in app settings.

Setting up 2FA on Whatsapp

Step 2: Click on 2 step verification and enable it. Then enter a six digit pin.

Setting up 2FA on Whatsapp

Step 3: Enter your email address to verify the change and then click save.

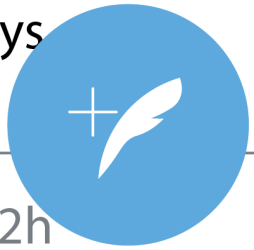


emcybersecure @emcybersecure · 1h
Step 1: got to the side menu, click More, then click Settings and privacy.

emcybersecure @emcybersecure · 1h
Step 2: Click on Security and account access, and then click Security.

emcybersecure @emcybersecure · 1h
Step 3: Click on two factor Authentication and select your prefered method of verification.

emcybersecure @emcybersecure · 1h
Twitter accepts verification via sms, authentication codes and security keys



emcybersecure @emcybersecure · 2h
Check out our new security articles




Turning On 2FA For Snapchat

Step 1: Visit your profile by clickling on the top left icon.

Step2: Click on the  In the top right.

Step 3: Click on “Two Factor Authentication”.

Step 4: Follow the on screen instructions

Step 1: Click on “me”, then click on the three dots to go to your settings.

Step 2: Go to security and click on 2-step verification.

Step 3: Follow the on screen instructions.

999

101

Share

@emcybersecure

How to set up 2FA on TikTok **#police #cybersecurity #cybercrime #2fa**

Original Sound - emcybersecure

Search in mail

PRIMARY

East Midlands Cyber Secure 11:56

How to set up 2fa on google

Google 2FA is universal and will protect all of your google accounts e.g. Gmail, Youtube, Google Drive and others.

East Midlands Cyber Secure 11:56

Step 1:

Click on your account and click "manage your google account". From there, go to the security tab to get to security settings.

East Midlands Cyber Secure 11:56

Step 2:

Scroll down to the "signing into google" section and click on the "2 step verification" button. Then click get started and follow the on screen instructions.

Compose

99+

C

Inbox

Focused Other

Filter

East Midlands Cyber Secure 10:30 AM

Setting up 2FA on Outlook and Hotmail

Step 1: Go to the Microsoft account management website and go to security.

East Midlands Cyber Secure 10:30 AM

Setting up 2FA on Outlook and Hotmail

Step 2: Go to the more security options link and you will be asked to verify your account by entering a code.

East Midlands Cyber Secure 10:30 AM

Setting up 2FA on Outlook and Hotmail

Step 3: From here scroll down to two step verification and follow the on screen instructions.

Contact us!

	Email: cyber.protect@leicestershire.pnn.police.uk
	Email: cyber@derbyshire.police.uk
	Email: cyberprotect@nottinghamshire.pnn.police.uk
	Email: cybercrime@lincs.pnn.police.uk
	Email: cyberprotect@northants.police.uk

Follow us on social media

@emcybersecure

@emcybersecure

While we have you...

Here are some additional steps you can take to protect yourself from cybercriminals:

Use a strong and seperate password for your email accounts.	Your email account is used often to set up online accounts and can be used to reset the passwords of other accounts. As such it's one of your most important accounts that you need to protect and you should use a strong seperate password for it.
Install the latest software and app updates.	Updates help protect your device from viruses and other kinds of malware, and will often include improvements and new features. You can turn on automatic updates to make them less of a burden.
Back up your data.	Keeping your information backed up acts as a good insurance policy in that in the event your computer is infceted with malware, you can easily recover any lost data. Be sure to not keep your back up constantly connected to the PC as it may get infected as well.
Don't allow remote access to your computer.	A lot of scammers are now pretending to be from IT providers and companies to try and gain remote access to your PC to "fix an issue". Don't ever do this as they will have full access to everything on the PC and will steal personal information. No legitimate company will ever ask you for remote access to your computer.
Three random words.	When making passwords, consider using three random words, e.g. bluedolphinchair. Mix in special characters as well like numbers, capital letters and symbols. Don't use personal information which could be found on social media as passwords e.g. date of births, pets names and family names.