Lancashire Cyber Foundry

Why You Should Use 2-Factor Authentication

READ TIME: 2 MINS

AUDIENCE: BUSINESS & TECHNOLOGY

Password protection is quite frequently the last and only layer of defence between criminals and our personal data.

Whilst, passwords can be very secure, there are always issues regarding online password leaks, hacking, email phishing and more. If there is only one layer of protection for our personal data, all it takes is one slip up to have potentially major repercussions. This is why having at least one more level of security is always a good idea. Enter 2-Factor Authentication (2FA).

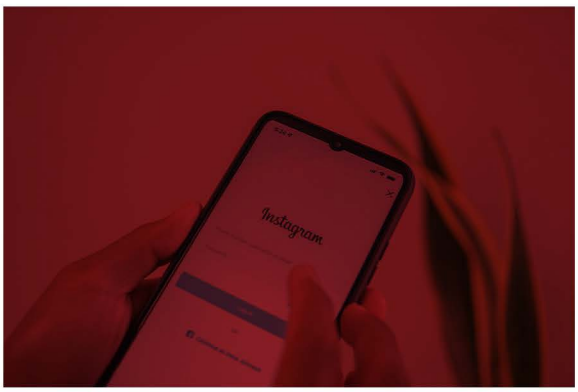
WHAT IS 2FA?

In the simplest terms, 2-Factor Authentication is just requiring two distinct types of information to gain access to something. The first factor is usually a password, just like usual and then the second component can be a variety of things. Some examples are:

- Fingerprint Identification
- Facial Identification
- Retina Identification
- Code Sent Via Email/Text
- Authentication Applications

2FA EXAMPLE

Let's say you're going to log in to your Twitter Account. With 2-Factor Authentication enabled, you would enter your password and then Twitter would generate a random code and send it to your mobile phone or email address. You would then be required to enter in order to gain access to your account.
These randomly generated codes are time-sensitive and so will expire after short periods of time such as 30 seconds or a minute. You can always request a new code be sent to you if the last code expires.



European Union
European Regional Development Fund

NORTHERN POWERHOUSE HM Government

Lancaster University

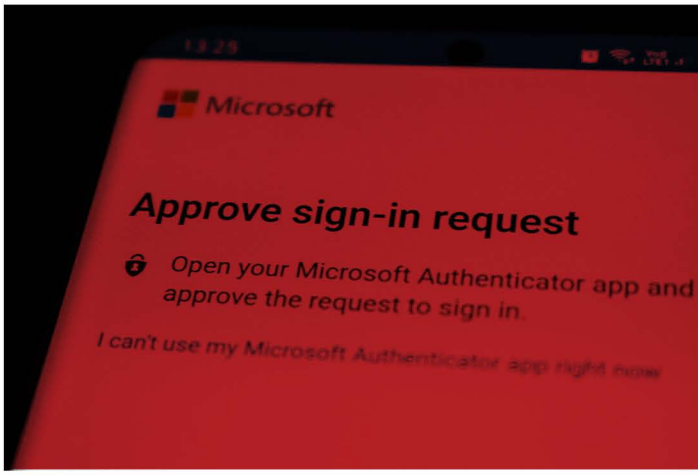
2-Factor Authentication

SECURING MY ACCOUNT

2-Factor Authentication makes your account substantially more secure, because even if someone knows your password, they wouldn't be able to login if they didn't have access to the authentication code. And vice versa, even if someone found out the authentication code, they wouldn't be able to login without the password. This gives some leeway for errors and allows time to change passwords with the knowledge that your personal information remains secure.

Obviously, 2-Factor Authentication will not prevent every hack attempt, as some hackers may intercept the text containing the code or gain access to your texts. This is not, to dispute the effectiveness of 2-Factor Authentication, but more just to state that it is not completely fool-proof and can be bypassed.

Codes sent via Text, whilst still substantially more secure than using just a password, are the least secure form of 2-Factor Authentication. So if you wish to use your mobile device for authentication, it is recommended that you install and use an authenticator app whenever possible.



CONCLUSION

Overall, having an extra layer of protection on your online accounts is always an excellent idea to keep your online presence safe from the multitude of threats that are posed by cyber criminals on a daily basis around the world.

PATRICK DASTEY - LCF INTERN

ABOUT US

Lancashire Cyber Foundry

The Lancashire Cyber Foundry runs a programme designed to s upport businesses facing cyber challenges in Lancashire. Digital Innovation support is part of this programme but there is also business strategy support available which includes specialised workshops to help businesses innovate and grow.

To find out more visit our website, https://www.lancashirecyberfoundry.co.uk/ or email us at;

cyberfoundry@lancaster.ac.uk