SOCURA

FTSE 100 for sale

An analysis of stolen credentials and passwords across the UK's biggest businesses

flare

In partnership

Introduction

The FTSE 100 includes some of the largest and most trusted brands in the UK. Across sectors including retail, energy, financial services, and defence, these companies are among our biggest employers and most significant contributors to GDP.

While they may have bigger cyber security budgets than the average UK business, our analysis shows that FTSE 100 companies struggle with the same core cyber security concerns as the UK's other 5 million businesses. Their employees are using and re-using weak passwords, using corporate email addresses to sign up for personal services, and accessing business networks from devices infected with infostealer malware.

This is not about criticising the FTSE 100. Instead, it's a wake-up call: if the country's biggest companies are vulnerable, then every organisation is too. Businesses must act to reduce their threat exposure, embrace the latest methods of passwordless authentication, and ensure they can identify and respond to threats swiftly.

Andrew Kays
CEO, Socura

Contents

01. Key findings

Based on an analysis of leaked and stolen credentials found on the clear and dark web:

01 **460,000** instances of leaked credentials linked to corporate email addresses from FTSE 100 companies

02 **45,000** instances of leaked credentials associated with one FTSE 100 company alone

03 **28,000** instances of corporate credentials from FTSE 100 businesses leaked via infostealer logs

04 **59%** of FTSE 100 companies have at least one instance of an employee using 'password' as a password

05 **CEOs and CXOs** email addresses and passwords shared on dark web sites like Doxbin

02. Methodology

Using the Flare Threat Exposure Management platform, researchers from Socura and Flare analysed the domains of every FTSE 100 company to find leaked credentials. The Flare platform monitors the clear and dark web, including more than 58,000 cybercrime communities and forums.

The figures stated in the report represent the aggregate number of credential instances discovered, not necessarily the number of unique employee accounts compromised.

In instances where FTSE 100 companies use different email domains (such as for different brands), more than one domain per company was analysed

For the leadership section of the report, the researchers identified twelve well-known CEOs and other leadership figures in the FTSE 100. They checked for leaked credentials linked to these individuals, as well as mentions in illicit networks, including forums, blogs, marketplaces and ransomware leaks. Popular networks include 4Chan, Telegram, LeakForums, Nulled and Doxbin.

03. Leaked credentials

We discovered 460,000 instances of leaked credentials linked to the corporate email addresses of FTSE 100 companies. This figure is roughly equivalent to the entire population of Bristol.

To illustrate the results we found, suppose we searched for leaked credentials at a fictitious FTSE company, 'Fake Company.' The results might look something like this:

Source	Email	Password
MyFitnessPal	homer@fakecompany.com	Springfield!
LinkedIn	marge@fakecompany.com	L1inked1n
Collection #1	bart@fakecompany.com	Snowball2
Neopets	lisa@fakecompany.com	saGR0sakjbA52

Credentials like these appear in 'combo lists' —files containing large collections of stolen data, such as usernames, emails, and passwords. This data is gathered from multiple breaches before being sold or distributed on the dark web.

Notably, many individuals have their credentials stolen multiple times, or the same records appear in numerous leaks (with Collection #1 being one of the largest and best-known databases).

> Cybercriminals are opportunists. Most won't waste precious time hacking for credentials when they can easily find or buy them online.

Anne Heim, Threat intelligence Lead, Socura

460,000

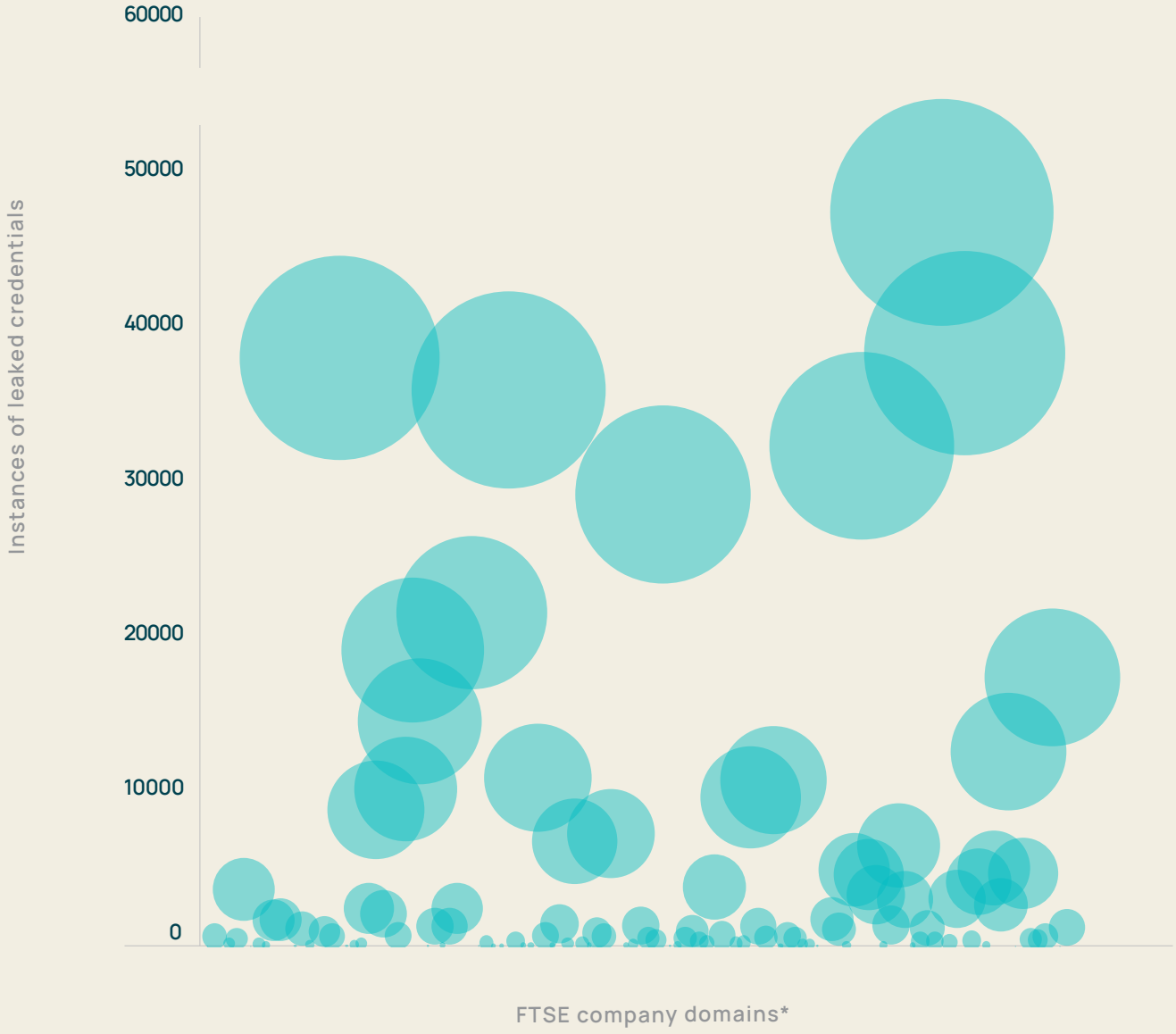
instances of leaked passwords across the FTSE 100

Visualising the problem

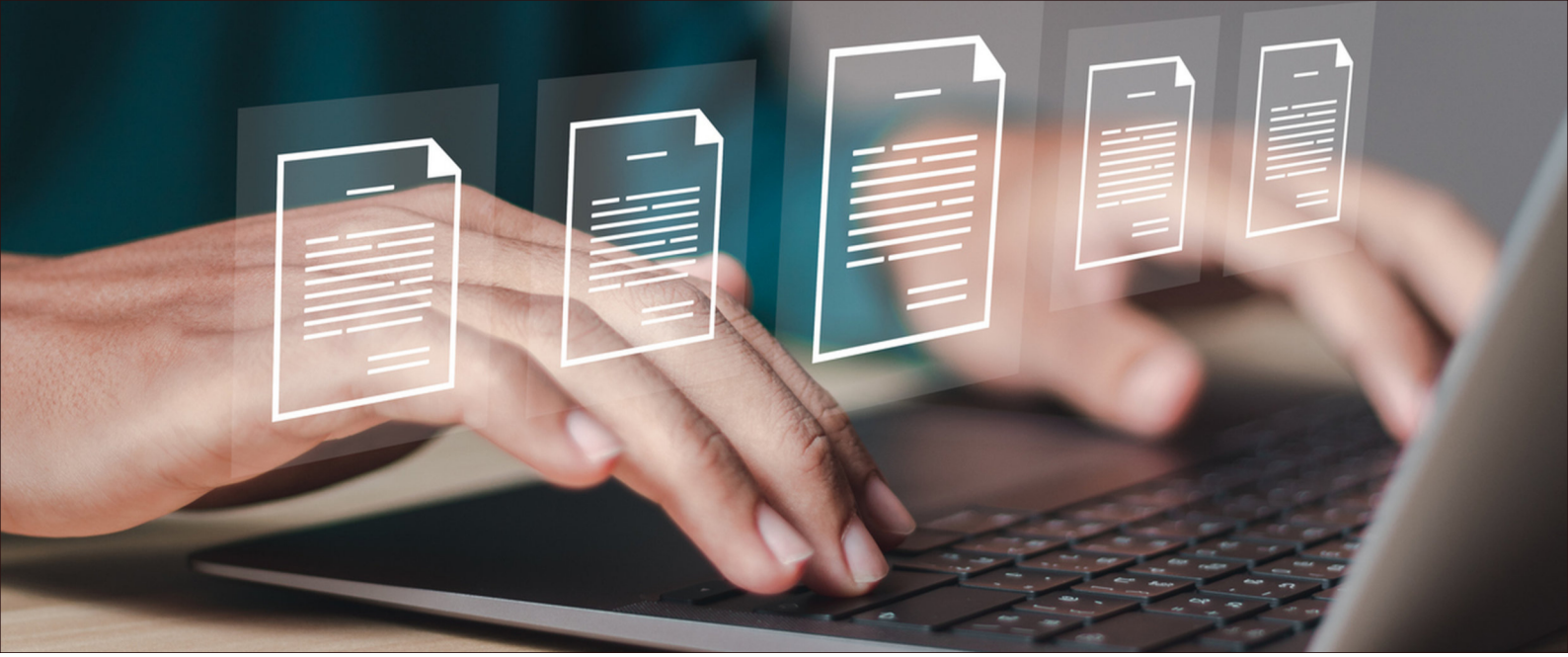
The graph below shows the number of instances of leaked credentials discovered for each FTSE 100 company domain. The x-axis is intentionally left blank to keep the organisations anonymous.

The data reveals that some organisations have as many as 45,000 instances of leaked credentials, with 15 companies having more than 10,000 instances each.

Leaked credentials are a problem across every sector. More than 70,000 instances were found linked to financial services companies in the FTSE 100 alone.



*A total of 117 domains were analysed for this report, as some FTSE 100 companies operate multiple domains.



04. Stealer logs

Credentials appearing in combo lists pose a security challenge, but the volume of stealer logs in the FTSE 100 is arguably a much more serious risk.

infostealer malware is designed to extract information such as documents, usernames, and passwords from users . We found 28,000 instances of corporate credentials from FTSE 100 businesses that were leaked this way.

> In the wrong hands, data from stealer logs is a dangerous asset. Attackers can sell credentials and sensitive details on the dark web, blackmail targets, and even use information to launch secondary attacks against an organisation's customers and partners.
>
> **Anne Heim,** Threat intelligence Lead, Socura

28,000

Instances of credentials found via stealer logs

Infostealer malware

On average, each FTSE 100 business has 280 instances of employee credentials stolen via infostealer malware.

However, this number may be just the tip of the iceberg, as these are only the credentials that we are aware of from public leaks, areas of the dark web, and criminal channels. A company could have many more stolen credentials that are yet to be sold, are in active use, or have been distributed through channels unknown to us.

For a better understanding of how credentials are used, sold, and distributed, see 'The credential economy' section of this report (p10).

A foot in the door

In most cases, infostealer malware is installed on personal machines. While company-owned devices can be infected, it is generally less common due to the stronger security controls in place. Users also tend to be more vigilant on their corporate devices.

A typical scenario could be a CEO logging in to multiple applications from an infected device, giving an attacker access to a wide range of data that may help them escalate privileges, deploy ransomware, and conduct follow-up attacks.

Access to email could enable an attacker to impersonate their target and conduct phishing campaigns.

Sensitive data and intellectual property could be encrypted and exfiltrated to extort money.

Information about customers and partners could be used to facilitate supply chain attacks.

> Once infostealer malware infects a device, attackers can harvest credentials for key systems and use this data to escalate privileges and target an organisation's most valuable assets.
>
> **Anne Heim,** Threat intelligence Lead, Socura

05. The credential economy

The following extracts from darknet forums and Telegram show how cybercriminals discuss, sell, and use FTSE 100 credentials.

To protect privacy, we have redacted all names of companies, individuals, and threat actors. Any additional context provided by our research team is highlighted.

Extract 1

POSTER [In French]:
voici une liste d'emails et mot de passes fresh récupérer par mes soins
Je vous donnerai une liste de plus de 2000 demain.

[TRANSLATED]:
Here is a list of emails and passwords I recovered. [list includes a FTSE 100 corporate email address and password]
 I will give you a list of over 2000 tomorrow.

Extract 2

SELLER 1: Good day all! I pay good money for UK and IE logs with my link! For 1 log I pay from $10 to $900, the price depends on the balance on the account, validity of log. And if comes with personal details like mobile number, name and email. I pay in any crypto currency. You tell me which links you have logs for and I tell you which I require. Payment will come upon checking each log for valid. Links that I buy in UK and IE

[List of domains including a FTSE 100 business]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

If you have any other logs for UK financial institution links, please let me know and there is a possibility I will buy these also. Contact PM on forums or TG @[redacted]

Extract 3

POSTER [In French]:
SELLER:
full database Size : 700 GB+ Type : CSV Country : All countries Contains : first name, last name, gender, phone, email, job title, job designation, industry, company email, company phone, etc Paid content. Purchased: 1. Open content for 15.00 $ Purchase user upgrade "Покупка группы Premium" and view the buy tag without restrictions

POSTER 1:
Sample?

SELLER:
Shares sample data, including credentials of a VP at a FTSE 100 company.

First Name Last Name Title Company Email Email Status Mobile Phone Employees Industry Person Linkedin Url Website Company Linkedin Url City State Country Company Address Company City Company State Company Country Company Phone

POSTER 2:
wow expensive!

POSTER 3 [in Russian]:
На самом деле это потрясающе, спасибо, что поделились!

[Translated]
This is actually amazing, thanks for sharing!

POSTER 4 [in Russian]:
Да, г**нецо общедоступное. И древнее...

[Translated]
Yes, publicly available sh**. And ancient...

Extract 4

POSTER 1:
data from [redacted] [FTSE 100 business] include all the files from their server user details payment details contact details images and all other server files 91gb + archives Buy @ $1000

Extract 5

POSTER 1:
UK Company with Weak Security and Valuable Data

This is an intelligence leak about a small company with poor security and lots of sensitive valuable data about its large blue chip clients that forum members could probly monetise.

[proceeds to name a small supplier and its customers which include large global brands including FTSE 100 businesses]

What we care about is they have no security tests and a long list of big clients and lots of data that would be valuable if it found its way into some enterprising person's hands.

POSTER 2: I've had a little poke around here, and I've decided to post about it on an alternate account because this [redacted] outfit have some security service links.

My initial reconnaissance strongly suggests this is a good lead.

[redacted] is a tiny company with [redacted]. Casual investigation reveals they have a malconfigured set of cloud platforms hosting instances of the same buggy insecure custom application. There is a lot of data here that could be sold and what looks like incorrectly hashed passwords. I'm pretty sure some Russians might pay top dollah for the questions you need to answer to get hired by [redacted] clients. Extracting the passwords using a rainbow table could lead to attacks on other accounts possessed by users and give leverage on staff inside government agencies. I personally don't want the heat but I think some people here should dig into this further and see how deep the rabbit hole goes.

06. Targeting the c-suite

Credential leaks are an issue at every level of an organisation. However, the risk is significantly greater when the credentials of senior leaders are compromised. From a sample of 12 FTSE 100 CEOs, we found:

4 instances

of personal data belonging to CEOs and CFOs being shared on Doxbin, an illicit website used for posting the information of targeted individuals

3 instances

of information leaked from the DemandScience breach in 2024, which exposed information relating to over 122 million people

1 instance

of a CEO caught in the infamous MyFitnessPal breach. Even CEOs are using corporate emails for personal services

1 potential death threat

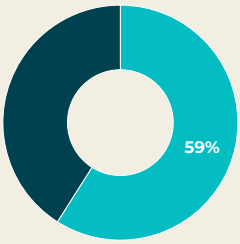
posted to 4chan, an anonymous imageboard website

07. Most common passwords

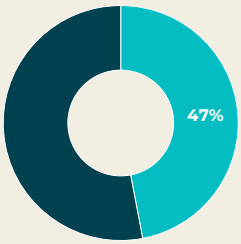
The most common passwords in the FTSE 100 are depressingly familiar. Of the 100 businesses analysed, 59 had at least one stolen corporate account that used 'password' as its password. Almost half (47) had at least one instance of 'Password' being used. The top six, all of which are incredibly weak, are listed below.

The prevalence of passwords like 'Password1' shows why mandating password policies in accordance with the latest best practices is essential. Educating employees on the importance of setting strong passwords and avoiding password reuse is also important.

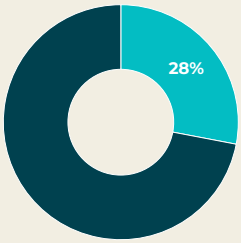
password



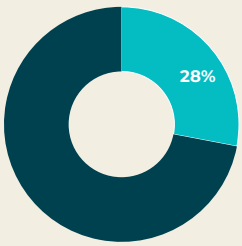
Password



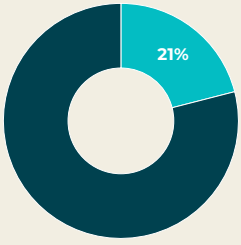
123456



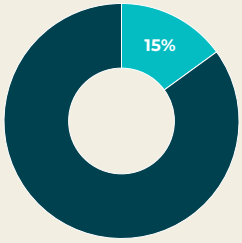
welcome



Password1



default



The Premier League of passwords

Football is the most popular sport in the UK, and Premier League clubs are well-represented in the list of most passwords used by FTSE 100 employees.

Nine FTSE 100 companies have at least one instance of 'Liverpool' among their leaked credentials—not including other variations of the word. Rivals Arsenal and Tottenham were also popular choices, with variations of 'Arsenal' appearing twice in the list.

Position	Club	% of FTSE companies that use password
1	liverpool	9
2	arsenal	6
3	tottenham	6
4	liverpool1	6
5	football	6
6	chelsea	4
7	arsenal1	4

Password re-use

Passwords are frequently reused across different apps and services, and our analysis shows that this also happens across the FTSE 100.

For example, one employee at a major UK retailer used three variations of the same main password, found across six different data leaks. This pattern suggests they adapt the password to meet different complexity requirements (e.g. adding a capital letter) or simply change a character or two when forced to change a password or perform a reset.

The employee is clearly a big fan of British actor, Ross Kemp. Passwords using a variation of his name include:

- RossKemp
- RossKemp.
- RossKemp!

Ross Kemp

Credit: Simon Dwain Kalavazides, CC BY 4.0

> Not only are employees using corporate emails for personal services and websites, but they are also using weak, easily guessable passwords, and multiple variations of the same words.
>
> This is why passwordless authentication based on biometrics is now a stronger option for organisations that want to minimise risks.
>
> **Anne Heim,** Threat intelligence Lead, Socura

8. Conclusion

This report makes one thing clear: even the UK's biggest and wealthiest companies are struggling with stolen passwords. We found credentials for everyone from the shop floor to the CEO's office for sale online, which proves that a big budget doesn't guarantee security. After all, why would criminals bother with complex hacks when they can just buy your password and log straight in.

We're not trying to single out the FTSE 100. This is a wake-up call for every business in the UK. If this is happening to the country's corporate giants, you can bet the problem impacts small and medium-sized businesses too. The core issues are the same everywhere: employees reusing weak passwords, signing up for personal services with their work email, and getting infected with data-stealing malware.

So, the only way forward is to be more proactive. You have to assume your company's credentials are already out there and act accordingly. This means implementing essentials like Multi-Factor Authentication, particularly passwordless options like biometric passkeys. It also means constantly monitoring for new data leaks, and detecting and responding to threats like malware and suspicious logins as early as possible.

These steps are no longer optional—they're part of a baseline for staying safe and protecting organisations against attacks.

Anne Heim
Threat intelligence Lead, Socura

9. Recommendations

To strengthen security posture against the risks of leaked and stolen credentials, Socura recommends that organisations implement the following measures:

01 **Enforce strong password policies** by following the NCSC's best practices and educating employees on creating unique passwords and using a password manager.

02 **Implement multi-factor authentication** as a standard across all devices and services to drastically reduce the impact of leaked credentials. The use of passkeys and other phishing-resistant forms of MFA is strongly advised over other forms of authentication, which can be susceptible to adversary-in-the-middle attacks.

03 **Use conditional access policies** to grant or block user access based on factors like authentication strength, device compliance status, and user risk level.

04 **Monitor your attack surface proactively** by regularly checking for leaked credentials and immediately resetting passwords for any compromised accounts.

05 **Manage the risks of personal devices** by implementing a clear Bring Your Own Device (BYOD) policy that requires MFA for accessing any work-related services.

06 **Implement robust detection controls** to alert on suspicious behaviour, such as unusual logins and activity that could identify infostealer malware.

10. Appendix

Password and % of FTSE 100 using it	
password	59%
Password	47%
123456	28%
welcome	28%
Password1	21%
default	15%
password1	14%
12345678	10%
123456789	10%
liverpool	9%
george	9%
Welcome123	8%
lectures	8%
tigger	8%
charlie1	8%
holiday	7%
wealth	7%
charlotte	7%
daniel	7%
Password123	7%
12345	7%
jonathan	6%
arsenal	6%
tottenham	6%

Password and % of FTSE 100 using it	
liverpool1	6%
football	6%
sunshine	6%
admin	6%
654321	6%
chester	6%
Welcome1	6%
1234	6%
https	6%
charlie	6%
scotland	5%
summer	5%
robie	5%
william	5%
scabal	5%
William1	5%
P@ssw0rd	5%
London01	5%
standard	5%
Welcome	5%
secret	5%
princess	5%
elephant	5%
Liverpool1	4%

Appendix

Password and % of FTSE 100 using it	
bollocks	4%
Richard	4%
matthew	4%
welcome1	4%
peanut	4%
qwerty	4%
alexander	4%
chelsea	4%
ginger	4%
newyork	4%
harley	4%
hockey	4%
chocolate	4%
scorpio	4%
sterling	4%
louise	4%
arsenal1	4%
Happy	4%
joshua	4%

About us

Socura

Socura is a Managed Detection and Response provider bringing the power of calm to organisations across the UK. In an ever-changing landscape, we empower teams with the clarity, control, and confidence to minimise cyber security risk and thrive.

Trusted by businesses and critical infrastructure, we deliver a precise, measured, and personal service that shuts down threats swiftly and effectively. We're proud to be ranked among the top 250 managed security service providers globally.

socura.co.uk

Flare

Flare is the leader in Threat Exposure Management, helping global organisations detect high-risk exposures found on the clear and dark web. Combining the industry's best cybercrime database with a ridiculously intuitive user experience, Flare enables customers to reclaim the information advantage and make cybercrime irrelevant.

flare.io

socura.co.uk