Most hacked passwords revealed as UK cyber survey exposes gaps in online security

ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security

- NCSC's first 'UK Cyber Survey' shows 42% of Brits expect to lose money to online fraud
- Breach analysis finds 23.2 million victim accounts worldwide used 123456 as password
- Global password risk list published to disclose passwords already known to hackers
- NCSC urges using 3 random words as passwords on the eve of CYBERUK 2019 event

Brits have been urged to apply steps to stay safe online after results of the UK Cyber Survey exposed exploitable gaps in their personal security knowledge.

The polling was independently carried out on behalf of the National Cyber Security Centre (NCSC), a part of GCHQ, and Department for Digital, Media and Sport (DCMS).

The findings, released ahead of the NCSC's CYBERUK 2019 conference in Glasgow this week, will inform government policy and the guidance offered to organisations and the public.

The cyber summit will see a range of sessions delivered by industry, academia and government, including a keynote speech by Cabinet Office Minister David Lidington.

Amongst the results – which have been published in full on www.ncsc.gov.uk - were that;

- Only 15% say they know a great deal about how to protect themselves from harmful activity
- The most regular concern is money being stolen – with 42% feeling it likely to happen by 2021
- 89% use the internet to make online purchases – with 39% on a weekly basis
- One in three rely to some extent on friends and family for help on cyber security
- Young people more likely to be privacy conscious and careful of what details they share online
- 61% of internet users check social media daily, but 21% report they never look at social media
- 70% always use PINs and passwords for smart phones and tablets
- Less than half do not always use a strong, separate password for their main email account

The NCSC has also today published separate analysis of the 100,000 most commonly re-occurring passwords that have been accessed by third parties in global cyber breaches.

The results show a huge number of regularly used passwords breached to access sensitive information.

Most used in total	Names	Premier League football teams	Musicians	Fictional characters
123456 (23.2m)	ashley (432,276)	liverpool (280,723)	blink182 (285,706)	superman (333,139)
123456789 (7.7m)	michael (425,291)	chelsea (216,677)	50cent (191,153	naruto (242,749)
qwerty (3.8m)	daniel (368,227)	arsenal (179,095)	eminem (167,983	tigger (237,290_
password (3.6m)	jessica (324,125)	manutd (59,440)	metallica (140,841)	pokemon (226,947)
1111111 (3.1m)	charlie (308,939)	everton (46,619)	slipknot (140,833)	batman (203,116)

Dr Ian Levy, NCSC Technical Director, said:

“We understand that cyber security can feel daunting to a lot of people, but the NCSC has published lots of easily applicable advice to make you much less vulnerable.

“Password re-use is a major risk that can be avoided - nobody should protect sensitive data with something that can be guessed, like their first name, local football team or favourite band.

“Using hard-to-guess passwords is a strong first step and we recommend combining three random but memorable words. Be creative and use words memorable to you, so people can’t guess your password.”

Margot James, DMCS’ Digital and Creative Industries Minister, said:

"Cyber security is a serious issue, but there are some simple actions everyone can take to better protect against hackers.

“We shouldn't make their lives easy so choosing a strong and separate password for your email account is a great practical step.

“Cyber breaches can cause huge financial and emotional heartache through theft or loss of data which we should all endeavour to prevent."

David Lidington, Chancellor of the Duchy of Lancaster and Minister for the Cabinet Office, said:

"Given the growing global threat from cyber attacks, these findings underline the importance of using strong passwords at home and at work.

"This is a message we look forward to building on at CYBERUK 2019, an event that reaffirms our commitment to make Britain both the safest place in the world to be online and the best place to run a digital business."

The NCSC hope to reduce the risk of further breaches by building awareness of how attackers use easy to guess passwords, or those obtained from breaches and help guide developers and System Administrators to protect their users.

The compromised passwords were obtained from global breaches that are already in the public domain having been sold or shared by hackers.

The list was created after breached usernames and passwords were collected and published on Have I Been Pwned by international web security expert Troy Hunt. The website allows people to check if they have an account that has been compromised in a data breach.

Troy Hunt said:

“Making good password choices is the single biggest control consumers have over their own personal security posture.

“We typically haven’t done a very good job of that either as individuals or as the organisations asking us to register with them.

“Recognising the passwords that are most likely to result in a successful account takeover is an important first step in helping people create a more secure online presence.”

Notes to editors

- The NCSC‘s two-day CYBERUK 2019 conference will see 2,500 delegates come to Glasgow’s Scottish Exhibition Centre on 24 and 25 April for a range of speeches, workshops and interactive displays.
- The conference is the flagship event for the tech community in the UK and includes participation from Government, industry and academia sharing knowledge to help make the country the safest place to live and do business online.
- The Government’s Cyber Aware campaign on online safety can be found here.
- The survey was commissioned by the **National Cyber Security Centre** and **Department for Digital, Culture, Media and Sport** as part of the UK Government’s National Cyber Security Programme. **Ipsos MORI** were commissioned to carry out the research.
- The findings will inform Government policy and the guidance which is offered to organisations and the public on a range of cyber security issues, as part of making the UK the safest place to live and do business online.
- Over 2,500+ respondents aged 16+, businesses and charities were surveyed from late November 2018 to January 2019 via telephone.
- The NCSC has also published a blog post alongside the release of the most common passwords that have been accessed by third parties in global cyber breaches

Password breaches

The 20 most commonly occurring names used as passwords in breaches;

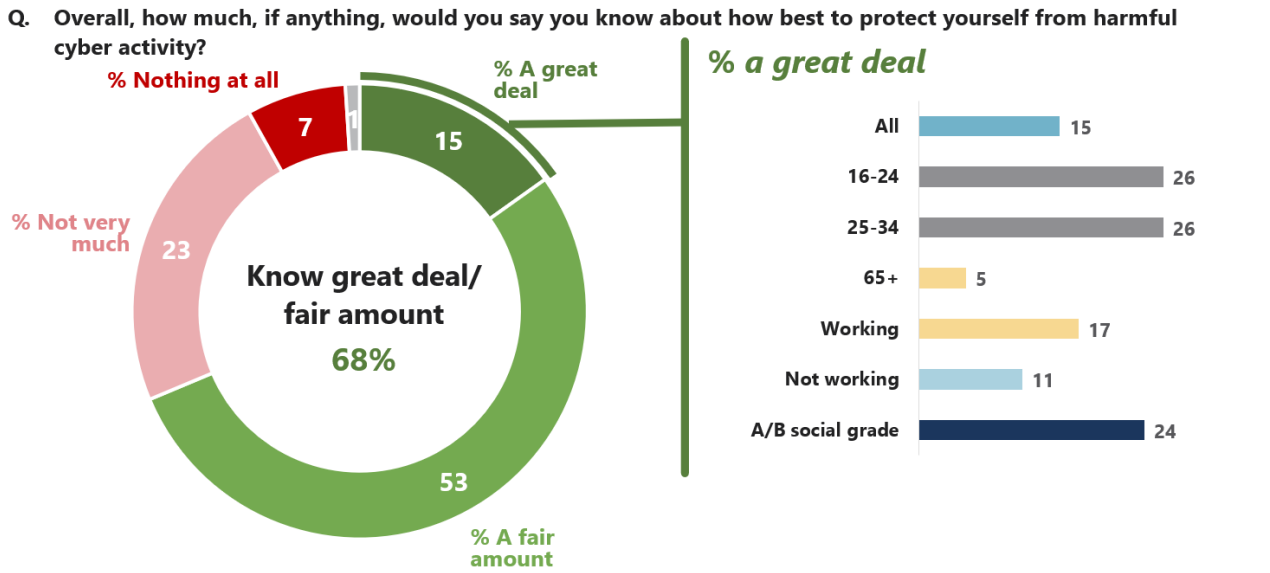
1. ashley	432,276	11. andrew	261,453
2. michael	425,291	12. joshua	259,079
3. daniel	368,227	13. justin	256,388
4. jessica	324,125	14. anthony	256,277
5. charlie	308,939	15. jennifer	245,653
6. jordan	297,882	16. robert	233,773
7. michael1	294,662	17. matthew	221,591
8. thomas	284,148	18. andrea	220,764
9. michelle	278,545	19. hannah	219,400
10. nicole	278,170	20. george	215,350

The full ‘table’ of Premier League football teams whose name was used to breach accounts;

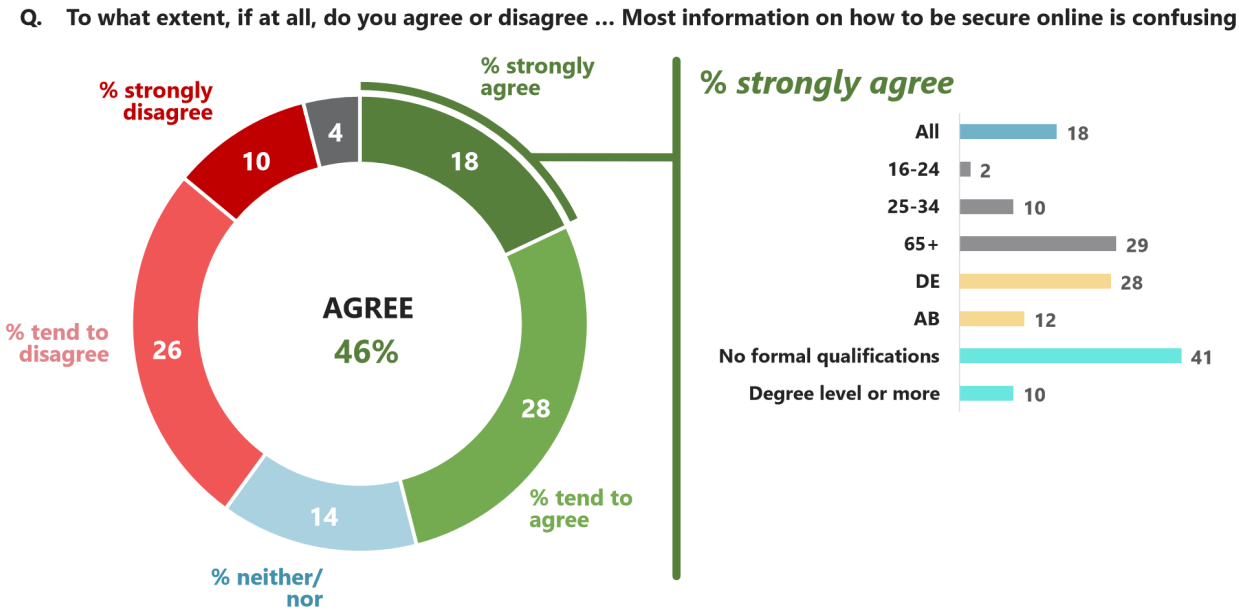
1. liverpool	280,723	11. mancity	13,796
2. chelsea	216,677	12. palace	13,796
3. arsenal	179,095	13. cardiff	12,594
4. man utd	59,440	14. leicester	7,921
5. everton	46,619	15. fulham	5,984
6. wolves	35,256	16. watford	5,563
7. newcastle	32,143	17. southampton	3,691
8. tottenham	19,596	18. burnley	3,494
9. westham	18,801	19. bournemouth	Not in the top 100k
10. brighton	15,523	20. huddersfield	Not in the top 100k

See the full 100k in full here.

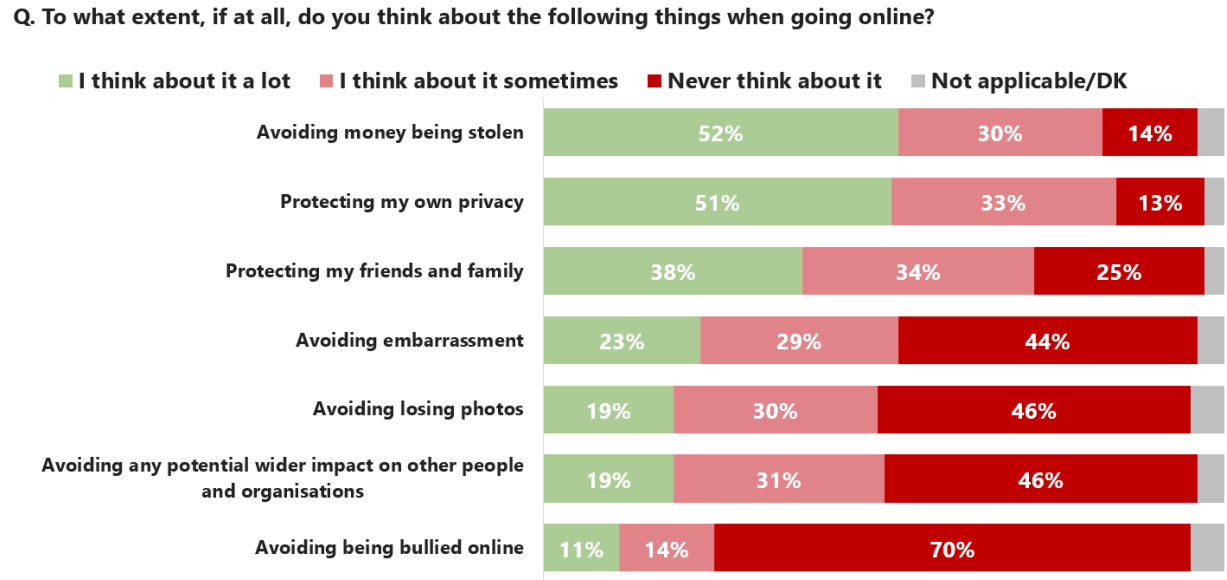
Cyber Survey – some of the findings



Almost half (46%) agree that most information about how to be secure online is confusing, though this falls to 18% who agree strongly.



The most pressing security-related considerations for people online are protecting their privacy and avoiding money being stolen



The proportions who feel they will be a victim of cyber crime in the next two years range from 12% having information stolen and a ransom demanded, through to 42% who feel they will have money stolen which is later reimbursed.

Only 51% feel that apps being accessed without consent will have a big personal impact whilst 91% feel having money stolen without reimbursement would have a big impact.

that have been accessed by third parties in global cyber breaches