5 terrifying password stats

that prove your business is at risk

DRAGON

Why are so many companies still getting caught out by hackers?

The simple answer that it's all a bit too much hassle.

Cyber threats are a daily problem for businesses of all sizes. Everyone knows the risks, but despite all the news reports and constant warnings, trends demonstrate a huge hike in data breaches and hacks over recent years.

The use of mobile devices for work have enabled us to become immensely more productive and flexible with our time.

But without proper management it's also created the perfect opportunity for cyber criminals to make money (and lots of it).

Proper robust passwords can be notoriously onerous to manage. So many companies simply pass it off as a job too time consuming to do anything about.

Even when faced with the ever-increasing risk of data loss, downtime and public naming and shaming, bosses everywhere are still burying their heads in the sand and hoping it all goes away.

When employees leave a company on bad terms, countless organisations fail to put the correct procedures in place to protect their critical data.

Even when password policies are written and shared with staff, they're still not being enforced.

A 2019 report from Yubico revealed that despite an increase in understanding about cybercrime and password best practice, behaviour is still falling short.

Look in any office and you'll still find people:

- Sharing login details
- Scribbling passwords on Post-it notes and sticking them on their computer screens
- And failing to keep schedules for password changes

Huge data breaches continue to happen every single day.

Both Yubico's report, and the first ever UK Cyber Survey, conducted by the National Cyber Security Centre (NCSC) identified scary password statistics that are putting businesses everywhere at risk.

Here are five of them >

69%

Two in three (69%) of users still share passwords with colleagues to access information.

51%

Over half (51%) of users use the same passwords for work and personal accounts.

57%

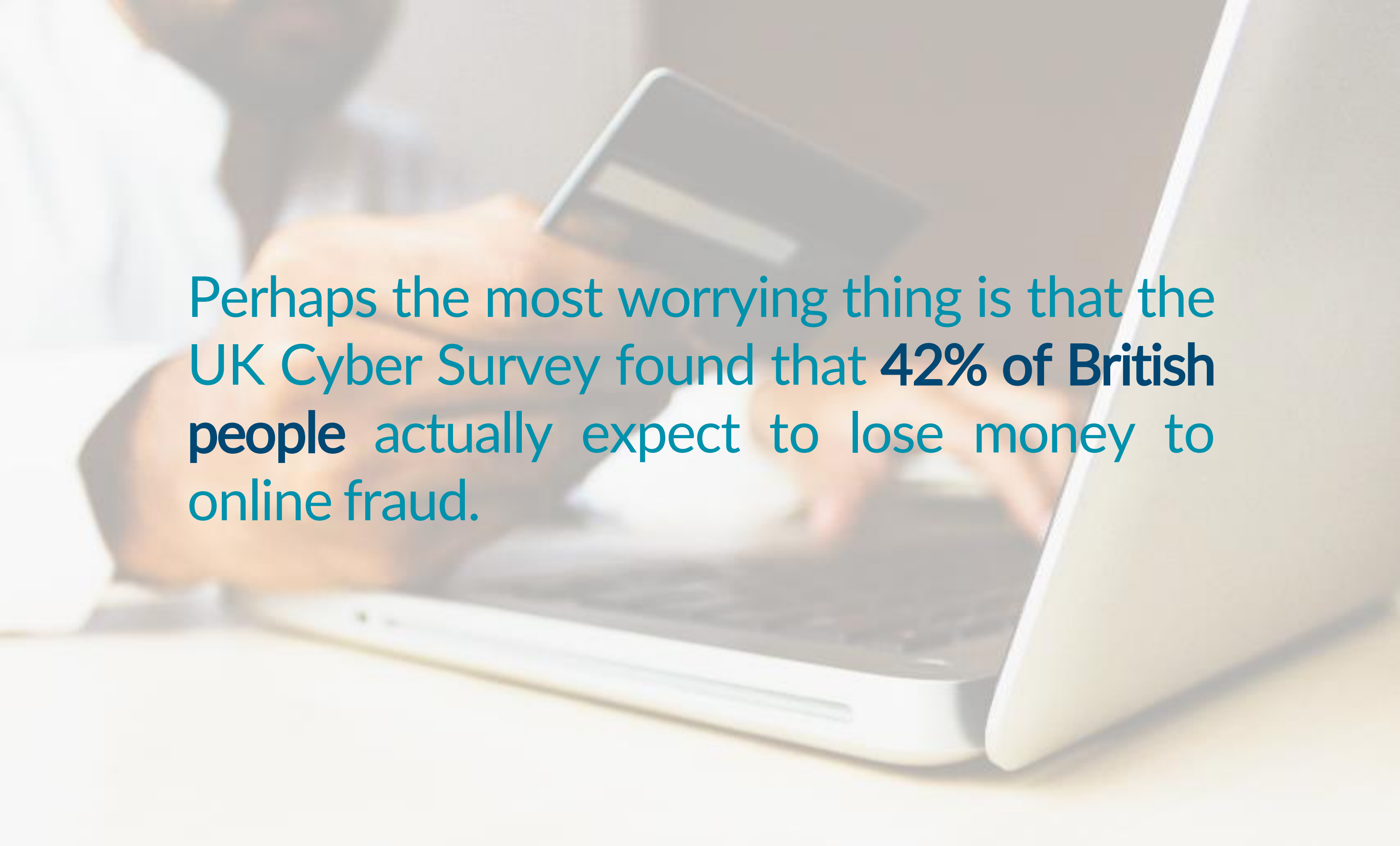
57% of people who have already fallen prey to phishing attacks still haven't changed their passwords.

23 million

23 million account holders are still using 123456 as their password, even though it's been proven to be just about as effective as the proverbial chocolate teapot.

57%

57% of people said they find password management an irritation that stops them doing their jobs, so they don't bother with it.



Perhaps the most worrying thing is that the UK Cyber Survey found that **42% of British people** actually expect to lose money to online fraud.

That means we're totally aware of the risks of poor password management, but we still refuse to do anything to prevent them.

Scary stuff.

The NCSC survey revealed even more worrying facts, including:

- **Only 15% of users** know how to protect themselves from cyber crime
- **89% of people** make online purchases with the same passwords
- **One in three people** rely on friends and family to keep them updated about cyber security
- **30% of people** never lock their mobile devices because re-entering passwords gets on their nerves

You can't run your business like this. It's time to change

This is our call to arms for more robust cyber security in your business.

Getting password management right starts at the top - and not just with writing a shiny new policy. Documents and procedures mean nothing unless they're enforced, so companies that are serious about cyber security need to put robust, actionable measures in place.

The bottom line is that organisations that fail to take action will be caught out sooner or later. And with the Information Commissioner's Office now taking a zero-tolerance approach to GDPR breaches, that's a risk nobody should be taking.

Here are our top 12 rules for good password hygiene:

1. Passwords should be changed on a regular basis - usually once a month

2. Never re-use passwords

3. Never write your password down

4. Never share login details

5. Block access for past employees as soon as they leave the building – even if there's no bad feeling between you

6. Don't use easy to guess passwords like football teams, special dates or children's names. Just a quick social media search can provide plenty of clues about seemingly unguessable passwords

7. Be creative about passwords by combining random but memorable words. Use a random password generator if possible

8. Use a password manager to remove the annoyance of robust passwords that change regularly

9. Consider using multi factor authentication, to provide an extra layer of security

10

Make sure everyone in your organisation is trained in cyber awareness and understands how to identify common threats

11

Keep the password policy on your shared drive and ensure everyone signs to acknowledge they've received and read it

12

Provide a contact person who will act as the main individual responsible for password security

As the head of your company or team, it's up to you to set a good example. Never share your login details with anyone and make it clear to everyone that doing so will be treated as a serious offence.

If people continue to sidestep the rules, you'll have to get tough - this is your company's reputation and money at risk.

Your password policy should become an essential document in your organisation that forms part of its overall culture. Make sure everyone reads it, signs it, and is made aware of what will happen if they continue to wilfully disregard it.

You know it makes sense…

Password security isn't about slowing down productivity. It's about enabling people to do their jobs safely and efficiently.

Data breaches don't just slow things down, they cost money. For every minute your team is unable to access their documents your business could be losing tens, hundreds or thousands of pounds.

And if a data breach does happen, the GDPR police will be delighted to use your poor password practices as an example to others - after they've fined you a hefty sum. Good password management should be an important part of your organisation's cyber security strategy. When combined with the right security software, procedures and attitudes, your organisation stands a fighting chance against the cyber baddies no matter what dirty tricks they try to deploy.

That means they can huff and puff as much as they like, but they still won't be able to hurt you.

Contact us today for a free, no obligation cyber security assessment and to find out more about stress-free password management.

For proven, trusted IT systems
support to keep your business
trading profitably

Dragon Information Systems Ltd
6 Bassett Court, Newport Pagnell, Bucks MK16 0JN
Tel: 01908 613 080 | helpdesk@dragon-is.com | www.dragon-is.com