The ClearScore Darkpaper

THE DANGER OF THE DARK WEB 2020

Shining a light on the data being sold on the dark web and how we can protect ourselves.

SHORT ON TIME? HERE ARE THE KEY OUTTAKES

Key Findings

MOST UK RESIDENTS HAVE A DECENT UNDERSTANDING OF THE DARK WEB.

People in the UK think the #DarkWeb is used for illegal pornography (46%), drug dealing (46%) and buying/selling people's #data (44%). Get @ClearScore Protect to see if your #passwords have been stolen.

GIF Tweet

A quarter of UK residents think some of their data could be for sale on the #DarkWeb, although over 55s are most likely not to know (53%). Find out if your #passwords have been stolen with @ClearScore Protect.

GIF Tweet

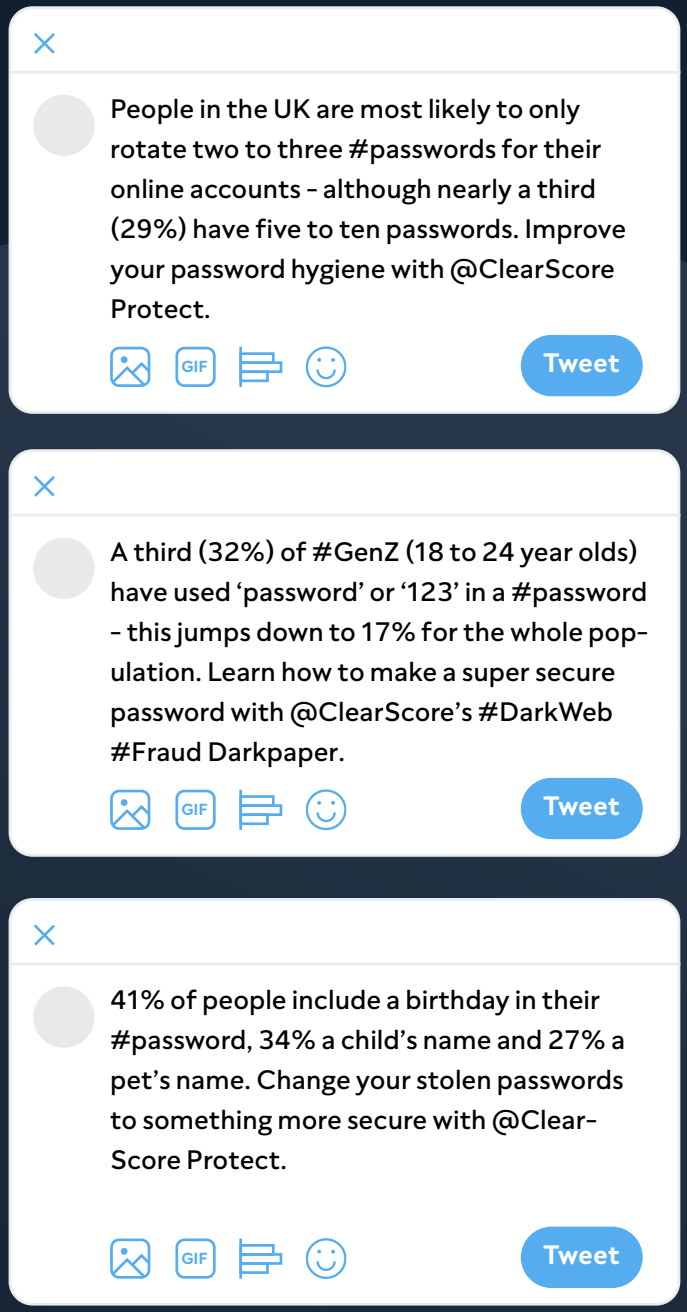
If people found out their #data was for sale on the #DarkWeb they'd either change all their #passwords (43%) or call the police (33%). Check out if your passwords have been stolen with @ClearScore Protect.

GIF Tweet

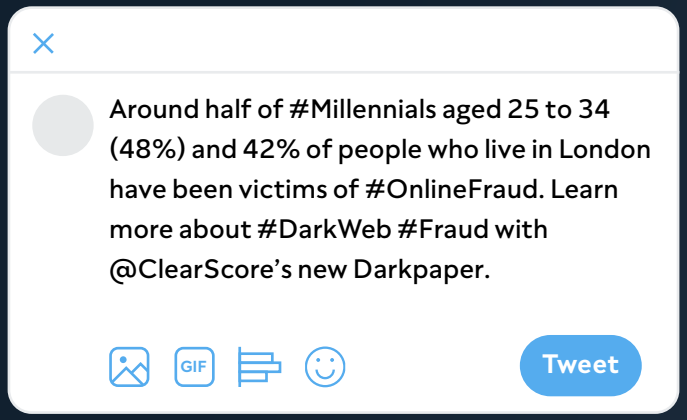
Half of people (52%) think the #DarkWeb is run by cybercriminals, although a quarter don't know who is behind it. Read @ClearScore's Dark Web #Fraud Darkpaper for the truth.

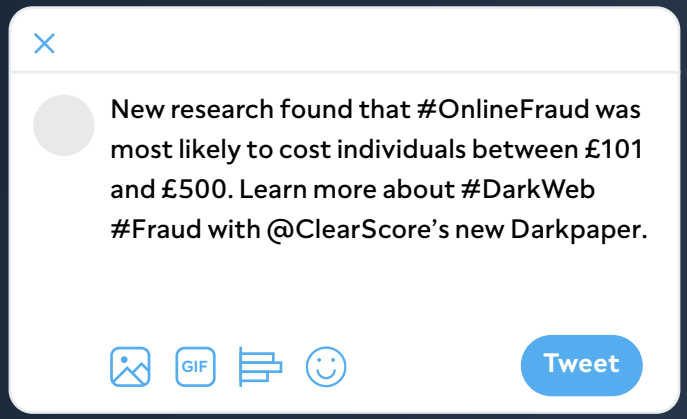
GIF Tweet

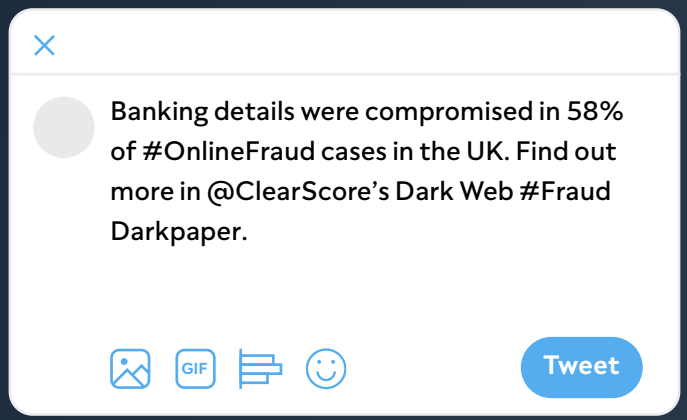
PASSWORD HABITS NEED SIGNIFICANT IMPROVEMENT.

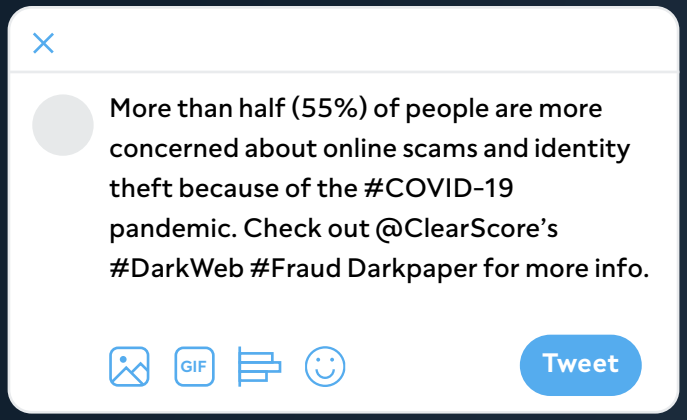


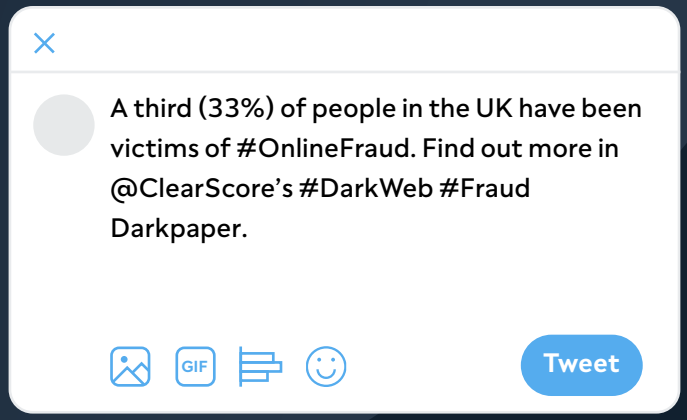
ONLINE FRAUD REMAINS A HUGE PROBLEM IN THE UK.











Overview

ClearScore's Darkpaper: The danger of the dark web 2020 examines UK citizens' understanding of the dark web and online fraud alongside the latest industry insight on these themes. It will also take a look at how COVID-19 has affected online fraud and people's perceptions of it, before concluding with actionable guidance on how individuals can protect themselves from this growing threat.

The purpose of this Darkpaper is to highlight the problem that online fraud poses to the UK's population and help guide them to a better understanding of online security with the launch of ClearScore Protect.

ClearScore Protect is a free dark web monitoring service provided to all ClearScore users, for free. Every three months, ClearScore privately and securely runs a scan of the dark web, monitoring for any stolen passwords associated with your ClearScore-registered email address. You'll be alerted by email if any of your data is found so that you can take action and secure your accounts against fraudsters. You'll also get personalised security tips to help protect your identity.

For enhanced protection, ClearScore also offers Protect Realtime - a subscription service for just £2.99 a month which monitors the dark web daily for up to three email addresses. ClearScore will scan for names, phone numbers, postcodes and other data that has been compromised in addition to passwords.

ClearScore Protect, dark web monitoring, for free, forever.
Activate ClearScore Protect here.

What you'll find in this Darkpaper

Forewords

"We launched ClearScore in 2015 to help people achieve greater financial well-being by providing credit scores and reports for free, forever. We now serve 9 million people in the UK.

A big part of financial well-being is understanding how and where your data is being used, and so we designed ClearScore Protect 18 months ago to help consumers take control of their online presence. I myself have fallen victim to identity theft and have had first-hand experience of how it can an impact a person's financial and mental well-being.

On behalf of the team at ClearScore, I hope that ClearScore Protect and the guidance in this Darkpaper will help you steer clear from becoming a victim of online fraud."

— JUSTIN BASINI, CEO & CO-FOUNDER CLEARSCORE

"There's a fundamental lack of cyber security awareness amongst consumers and it's leading to a great deal of personal distress, both emotional and financial.

ClearScore Protect is a great consumer resource, especially given it provides tailored support from a human by way of Protect Realtime. This can make a huge difference to those who've just lost money to cybercriminals.

Online fraud has been plaguing consumers for years, I hope the launch of Protect helps drive consumer awareness around online safety."

— TROY HUNT, WEB SECURITY EXPERT & CREATOR OF 'HAVE I BEEN PWNED?'

SECTION 1:

What's so dark about the dark web?

EXAMINING PEOPLE'S CONCEPTIONS & MISCONCEPTIONS ABOUT THE DARK WEB

WHAT IS THE "DARK WEB"?

The Cambridge Dictionary defines the dark web as:

> **Dark web**
>
> ***noun*** (also **dark net**)
>
> "parts of the internet that are encrypted (= use a secret code), and that cannot be found using ordinary search engines, and that are sometimes used for criminal activity." [1]

This matches relatively well with the UK population's general understanding of the dark web. They may not know how to access it necessarily, but popular culture (alongside stock images of people in hoodies in front of computers) means 83% of Brits have heard of the dark web and most (69%) see it as *"a hotbed of all sorts of criminal activity"*.

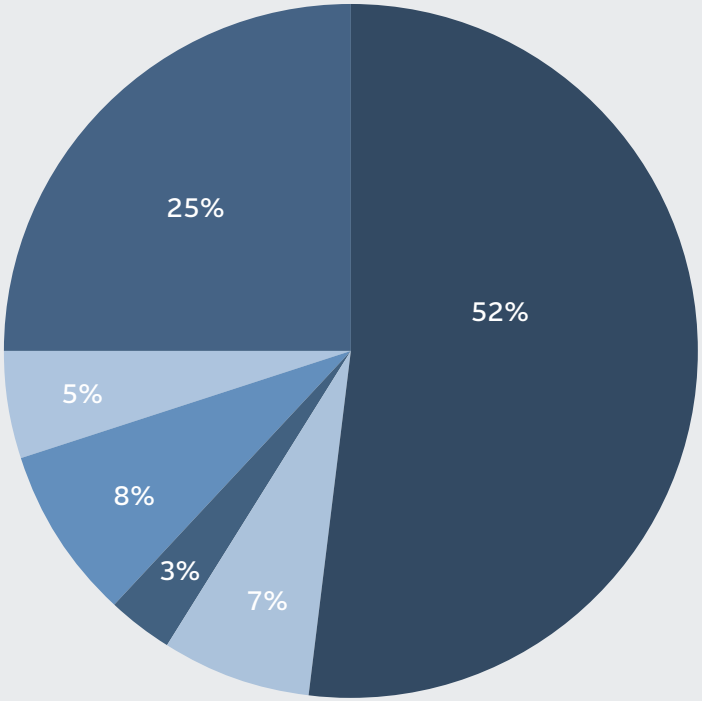
SO...WHAT ACTUALLY IS IT?

- The dark web refers to all websites that are only accessible through a **TOR network**.
- TOR stands for "**The Onion Router**", so-called because it sends encrypted traffic through layers of relays around the world so as to hide the website, the searcher and their location.[2]
- In a nutshell, everything on the dark web is there because it wants to be **anonymous**.
- To access the dark web, you have to download the **TOR browser** and you can then surf it either by knowing the web address you want to visit or using a search engine like DuckDuckGo.[3]

Dark fact: You may have heard the term "deep web" as well as dark web and assumed they are the same thing, but they're not. The dark web is actually a small, encrypted (locked up) part of the much larger deep web, which is the 95% of the internet not indexed by web search engines like Google. Content on the deep web includes academic journals, company intranets and even your email account.[4]

WHO RUNS THE DARK WEB?

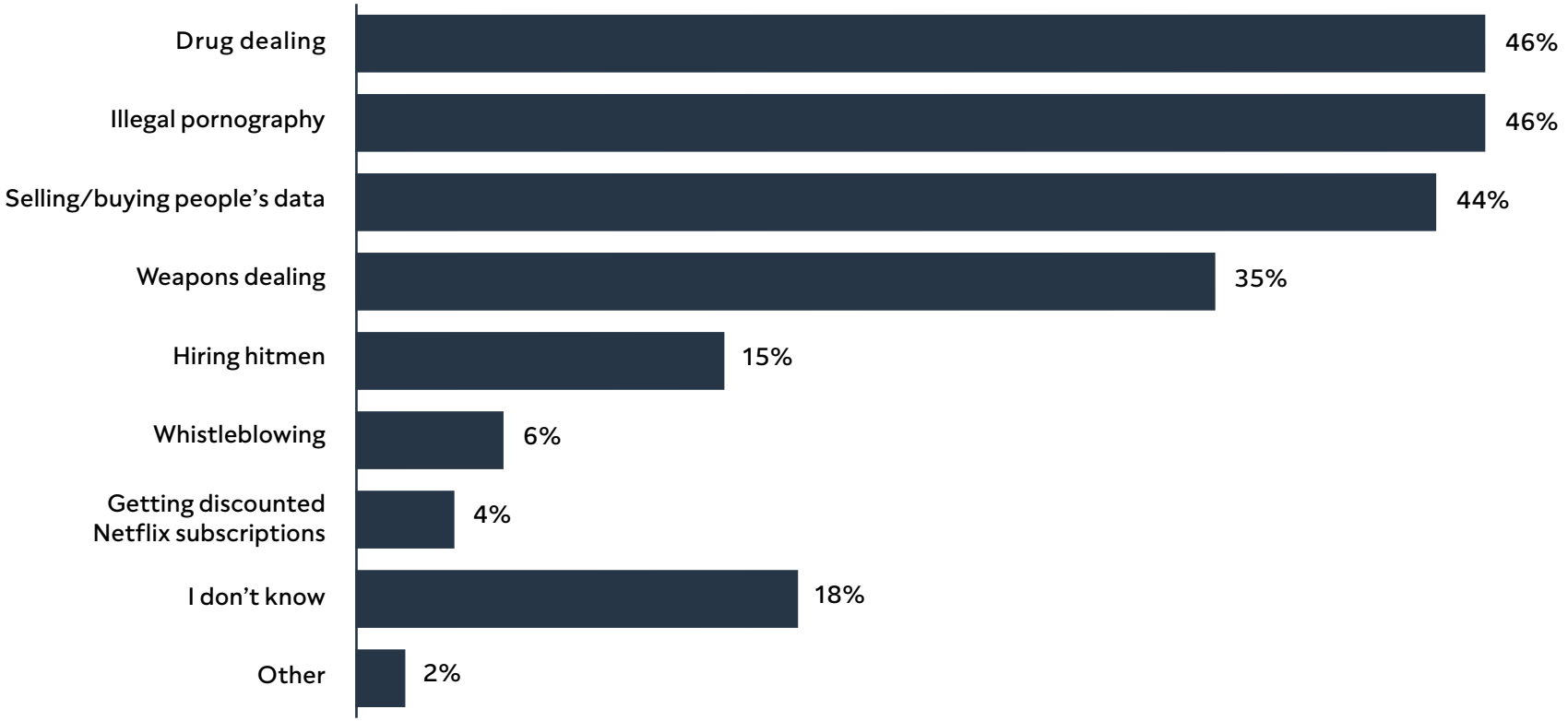
More than half of people in the UK think the dark web is run by criminals (52%), but a quarter of the general populace aren't sure.



52% Criminals
7% A distributed network of volunteers
3% The government
8% All of the above
5% No-one
25% I don't know

WHAT IS THE DARK WEB USED FOR?

When we asked our respondents what the dark web is used for, we gave them seven options to pick from (alongside "I don't know" and "Other") **all of which are in fact correct.**



SO...WHAT IS REALLY ON THE DARK WEB?

A study from 2015 by Gareth Owen and Nick Savage (both from the University of Portsmouth) on behalf of the Global Commission on Internet Governance collected data on the dark web for six months to analyse the type and popularity of its content. The study shows that while crime (especially drugs) is a big part of the dark web, there is also less insidious content like bitcoin, and its anonymity can be used for good, for example for whistleblowing and activism.[5]

Dark fact: No one actually runs or owns the dark web. It is known as a decentralised internet which means everyone owns and controls their own data. The invention of the dark web is typically thought to have taken place in the early 2000s, most notably with the release of TOR by the US government, who built it to help their own operatives remain untraceable.[6]

Key takeaways

1. The dark web is part of the deep web which can't be accessed using normal search engines like Google. It uses TOR (The Onion Router) in order to keep visitors and websites anonymous.

2. Despite 52% of Brits believing the dark web is run by criminals, it's actually run and owned by no-one.

3. The dark web is predominantly used for criminal activity like fraud but is also used for good, like whistleblowing and activism.

If you want to learn more about the dark web, check out this blog on the ClearScore website.

SECTION 2:

Fraud on the dark web

WHAT ARE DARK WEB CRIMINALS DOING WITH MY DATA?

As we saw in the last section, the third most common kind of content on the dark web is fraud related. But how does this affect people in the UK?

HOW MUCH DO UK RESIDENTS CARE ABOUT FRAUD?

A separate piece of market research conducted on behalf of ClearScore in March 2020 found that Brits' biggest financial concern is saving money, with 23% of the population placing this as their number one money worry. However, the second and third biggest stresses are identity theft and fraud (for example, their credit card information being used against them).

HOW BADLY IS THE UK AFFECTED BY ONLINE FRAUD?

Our data found that one third (33%) of the UK population admitted to being victims of online fraud.

Victims were more likely to be men (53% of whom were affected), aged between 25 and 34 (26% of whom were affected) and live in the South East (15% of whom were affected). Interestingly, wealth has nothing to do with it; there's only one percentage point difference in the proportion of those typically defined as the middle and working classes who have fallen victim to online fraud.

In terms of how much money is stolen from individuals in these cases, 31% of those surveyed who had fallen victim to online fraud lost between £101 and £500, 5% lost £1,001 to £2,000 and 3% lost over £2,000. Losing any amount of money to online fraud is incredibly stressful, not only because of the financial impact but also because of the time and effort it can take to try to reclaim money. In some cases, people may not be able to get their money back at all which can have a significant emotional and mental toll on individuals and their families.

HOW DOES ONLINE FRAUD HAPPEN?

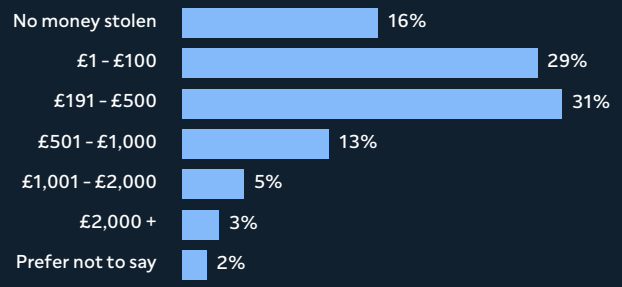
The easiest way for criminals to steal your money is to get access to your data, most importantly your financial information i.e. your debit or credit card details. Other data is also valuable, especially passwords which can give criminals access to your financial information, or other details like your date of birth or address which can help fraudsters "prove" your identity.

Data gets leaked in what is known as a "data breach". These can be huge, such as the 2018 breach of Under Armour-owned fitness app MyFitnessPal where 150 million user records were leaked. Or they can be very targeted, using a variety of methods to steal data from one individual.[7]

The most common causes of data breaches include:

- Hacking into a database or system because there are vulnerabilities (holes) in the software protecting it.
- Phishing attacks (scam emails that trick people into giving away their data or downloading malware / a virus that breaks into people's devices and steals their data).
- Poor password hygiene i.e. users having easy-to-guess passwords or using the same password across multiple accounts.

When you were affected by online fraud how much money (if any) was stolen from you?



These methods (amongst others) are constantly evolving to catch people out which means that data breaches are very common. To put this into perspective, in 2019, 46% of businesses in the UK suffered a data breach.[8]

As a result, the 305,000 users who have activated ClearScore Protect found that an average of seven passwords had been stolen and found on the on the dark web.

Our study found that people underestimate how common data breaches are, or assume they haven't been affected because they haven't suffered (or noticed) repercussions. In fact, only a quarter thought that their data could be for sale on the dark web, with 22% believing their data wasn't for sale on the dark web and 53% not being sure.

Dark facts about online fraud

Some information about what cybercriminals are doing with your data on the dark web from Acuris Risk Intelligence:

- A typical internet user's entire data worth has been calculated to be **£987** to hackers.[9] All of your data in one package is referred to as "**Fullz**" and would allow criminals to act completely as you online, e.g. opening new accounts, changing passwords and transferring money.
- But, the amount criminals pay for your data depends on factors like how much data is involved in a package (i.e. is it just your email address, or is there a password and credit card info in there as well) and how much money you have in your bank account.
- Passwords are especially precious when they're "**Fresh**" meaning they haven't been exploited before - this is because criminals will assume that your password to one thing will be the same as your passwords to other things, based on your age, gender etc. "Fresh" passwords can sell for $10 to $100 (**£8 to £80**).
- Once these "Fresh" passwords have been used, criminals will post them on dark web forums for use by anyone in order to cover their own tracks. Acuris picks up between **50 to 100 million** of these every day.
- **Personal information** like birth dates are also valuable as criminals can check these against birth registers to get answers to security questions like parents' names and maiden names.
- **99.9%** of dark web purchases take place using **Bitcoin** or similar anonymous **cryptocurrencies**.

Key takeaways

1. Identity theft and fraud are some of the UK population's biggest financial concerns.

2. 33% of the UK population have been victims of fraud.

3. Of our survey respondents, victims of fraud most commonly lost between £101 and £500.

4. The average ClearScore user found they had passwords from seven online accounts leaked onto the dark web.

5. The average person's full "data worth" to a hacker is £987.

SECTION 3:

A note on COVID-19

HOW THE CORONAVIRUS HAS IMPACTED FRAUD

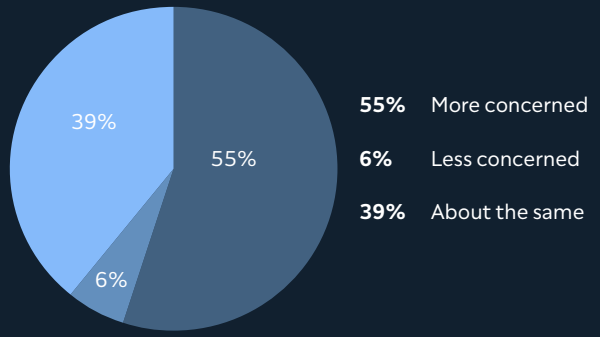
With this Darkpaper launching in April 2020, the UK (and the wider world) is experiencing significant challenges because of the coronavirus pandemic. Everything has been touched in some way by the virus, including online fraud, with cybercriminals adopting the insidious strategy of exploiting people's fears about COVID-19 for financial gain.

IS THE UK POPULATION NOTICING A DIFFERENCE?

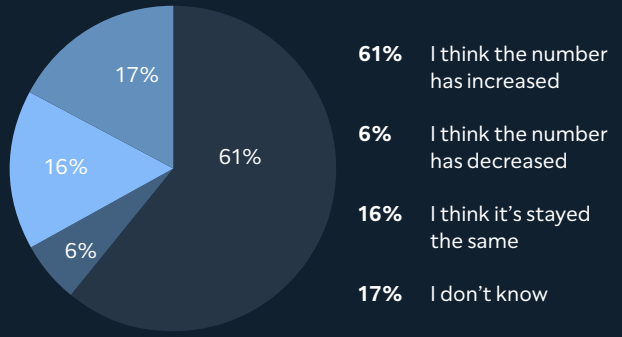
UK residents are feeling the impact of this change in online fraud, with more than half (55%) being more concerned about online scams and identity theft than before. Young people aged 18 to 34 in particular are feeling more concerned than before (63%).

The majority (61%) also believe the number of online scams and instances of identity theft have increased since the outbreak.

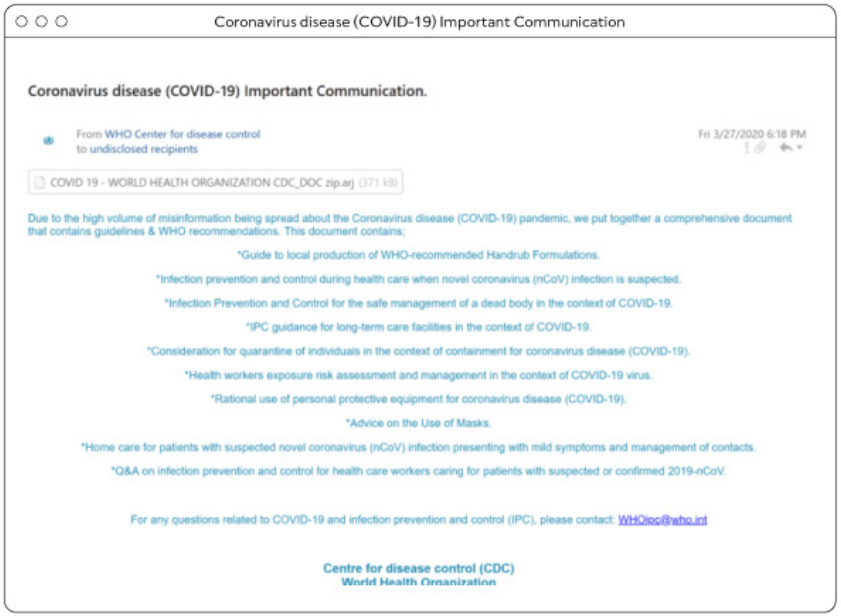
Do you feel more, or less, concerned about online scams and identity theft now that more people are working from home because of COVID-19?



Do you think the number of online scams and instances of identity theft has changed since the outbreak of COVID-19?



A FEW THINGS TO LOOK OUT FOR...



Source: Fortinet

Coronavirus-themed emails or websites that push you to download an attachment, like this example from a hacker posing as the World Health Organisation. Those who download the attachment will find their device infected with a data-stealing malware (virus).[10]

WHAT KIND OF COVID-19 RELATED SCAMS ARE OUT THERE?

The UK population is right to be concerned.

The National Fraud Intelligence Bureau (NFIB) reported that coronavirus-related fraud reports spiked by 400% from mid-February until the end of March, predominantly related to fake sales of face masks, hand sanitisers and other similar protective equipment.[11]

There has also been an uptick in cybercrime forum activity, with criminals offering discounts on COVID-19-related scams and phishing attacks.[12]

Dark fact: The NFIB reported in April that COVID-related fraud has scammed UK citizens out of £1.6 million since the start of the epidemic.[13]

A FEW THINGS TO LOOK OUT FOR...

UK Updates on COVID-19

----- Forwarded message -----
From: GOV UK Notify <danielnhs@pinkcontract.com>
To: "
Sent: Friday, 6 March 2020, 08:28:50 GMT
Subject: UK Updates on COVID-19

GOV.UK

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund* (*rebate*) of 128.34 GBP.

Access your funds now

The funds can be used to protect yourself against COVID-19(https://www.nhs.uk/conditions/coronavirus-covid-19/ precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

From Government Gateway

This is an automatic email - please don't reply.

Source: HMRC

Communications from insurance companies or HMRC that request your bank details or other personal information in exchange for what seems like an amazing offer like a tax rebate. If an offer seems too good to be true, it probably is.[14]

The variety of scams out there is immense, so it's wise to always remember the NCA's advice on how to avoid becoming a victim of fraud.

Stop: Taking a moment to stop and think before parting with your money or information could keep you safe.

Challenge: Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or cause you to feel panicked.

Protect: Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.[15]

For more information on addressing COVID-19-related financial concerns, check out ClearScore's COVID-19 hub.

Key takeaways

1. Over half of the UK population is more concerned about online scams and identity theft because of COVID-19 and the majority believe scams have increased since the outbreak.

2. These fears have been confirmed by the NFIB, with reports claiming that fraud has spiked by 400%, costing individuals £1.6 million since the start of the epidemic.

3. There are a variety of very creative scams out there, so it's important to be very vigilant when clicking on or downloading anything online or giving away any personal information.

SECTION 4:

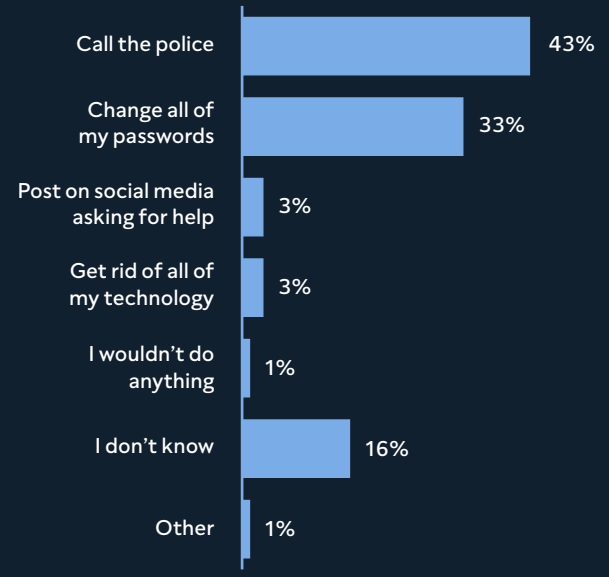
How can you protect yourself?

WHAT WOULD YOU DO IF YOU FOUND OUT YOUR PASSWORD WAS FOR SALE ON THE DARK WEB?

As this Darkpaper has illustrated, your passwords should be seen as codes to a safety deposit box that contains all of your wealth and potentially other precious information such as medical details and your address.

This section illustrates that people in the UK have relatively good password habits, but this may be breeding complacency. As we showcased in Section 2, it is worrying that only 25% of people think their data is for sale on the dark web when the average person who used ClearScore Protect found passwords from seven online accounts were available on the dark web.

What would you do if you found out your data was on the dark web?



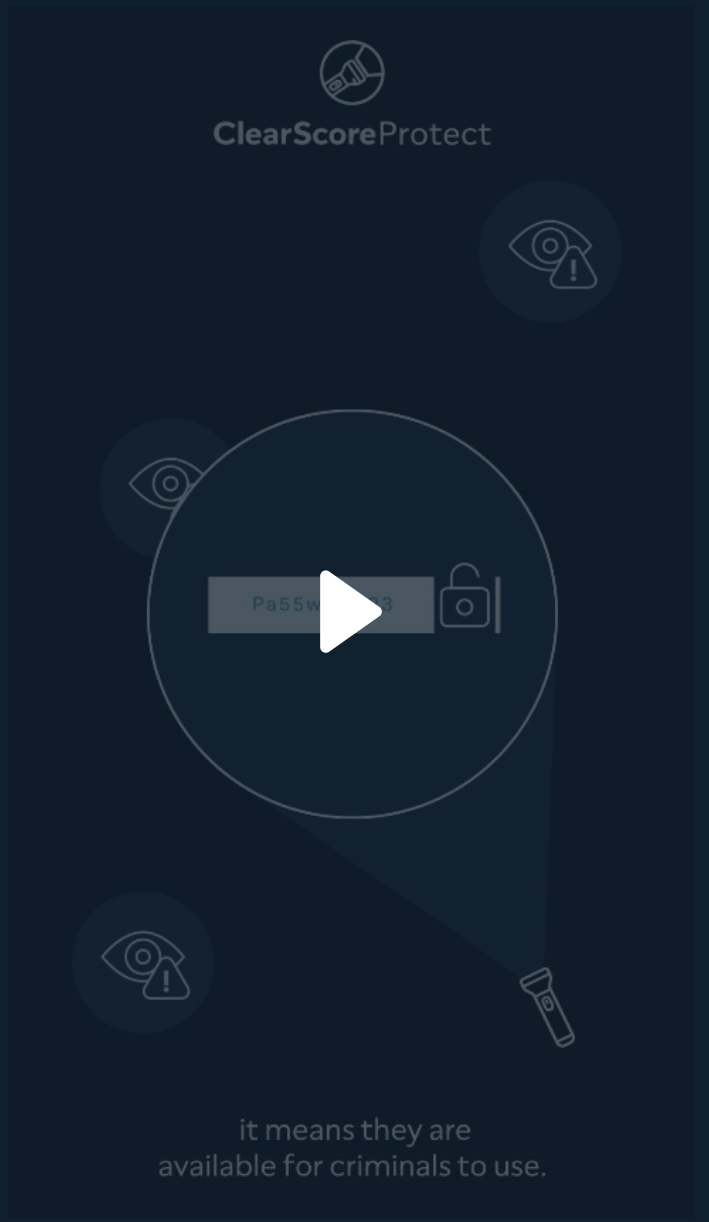
If you find out your password has been leaked onto the dark web, change all of your passwords right away.

WHAT IS CLEARSCORE PROTECT?

ClearScore Protect is a free dark web monitoring service provided to all ClearScore users, for free. Every three months, ClearScore privately and securely runs a scan of the dark web, monitoring for any stolen passwords associated with your ClearScore-registered email address. You'll be alerted by email if any of your data is found so that you can take action and secure your accounts against fraudsters. You'll also get personalised security tips to help protect your identity.

For enhanced identity protection, ClearScore also offers Protect Realtime - a subscription service for just £2.99 a month, which monitors the dark web daily for up to three of your email addresses. ClearScore will scan for names, phone numbers, postcodes and other data that has been compromised in addition to passwords.

ClearScore Protect, dark web monitoring, for free, forever.
[You can find out more about ClearScore Protect here.]



WHAT DO I DO IF IT'S TOO LATE AND I'VE ALREADY BECOME A VICTIM OF FRAUD?

1. Contact your bank and lenders

First, let them know what's happened. After they've completed their fraud investigations and confirmed the transactions to be fraudulent, they may be able to refund your money.

2. Contant Action Fraud

Action Fraud is the UK's national reporting centre for fraud and cyber-crime. You can file a report online or talk to their specialists by calling **0300 123 2040**. They'll provide you with assistance on next steps.

3. Contact Cifas - the leaders in fraud prevention

Cifas offers a 'Protective Registration' service which places a warning on your credit report, alongside your personal details. This will be visible to banks and lenders when you're applying for a product or service. When banks or lenders see this warning, they'll use extra security measures to ensure that the application is actually from you, not someone pretending to be you.

4. Contact Victim Support

Victim Support is an independent charity that helps anyone affected by crime. They provide free and confidential support 24-hours-a-day, whether you've reported the crime to the police or not.

5. Subscribe to Protect Realtime

For £2.99 a month, Protect Realtime sweeps the dark web daily to check if any information associated with up to three of your email address has been compromised. It also gives users tailored support if any data is uncovered on the dark web or if they unfortunately become victims of fraud.

6. Monitor your ClearScore report

Your ClearScore credit report is generated once a month, but with ClearScore's Alerts feature, you'll receive updates if there are any upcoming changes to your next credit report. Keep an eye on these updates. If you don't recognise these changes, or any other information on your credit report, you can dispute this directly with Equifax, our partner credit reference agency.

ARE THE UK'S PASSWORD HABITS GOOD ENOUGH?

1. Make your passwords as complicated as possible

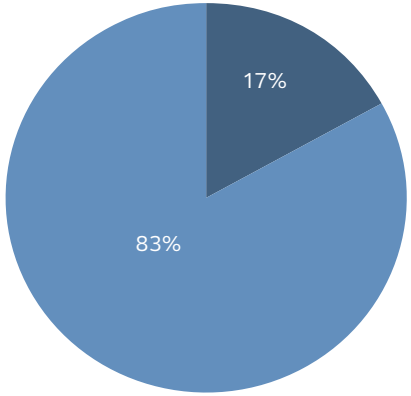
We asked the UK population a few questions to determine the average complexity of their passwords.

Starting with a positive note, only 17% of people have used the phrase 'password' or numerical sequence '123' in a password and 73% don't include any personal information in their passwords (for example, their birthday, children's names or address).

Have you ever included the phrase 'password' or number sequence '123' in a password?

17% Yes

83% No



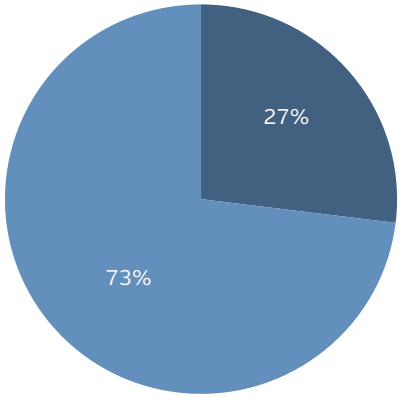
THERE ARE THREE GOLDEN RULES TO REMEMBER WHEN IT COMES TO PASSWORDS:

- Make your passwords as hard to guess as possible.
- Never use the same password twice.
- Get a password manager (for example 1Password) to help you remember your passwords.

Do your passwords include any of your personal information e.g. your birthday, child's name/birthday, your address, sports team, partner's or family member's name?

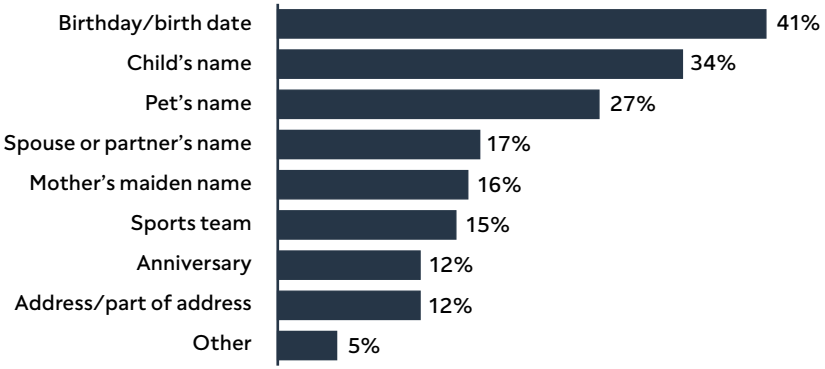
27% Yes

73% No



Of the 27% of people that do include personal information in their passwords, including a birthday or birth date was most common with 41% admitting to doing so.

Which of the following data have you included in your passwords?



Dark fact: Young people are the worst offenders when it comes to having simplistic passwords, possibly because they're more complacent having grown up with the internet. A third (32%) of 18 - 24 year olds have included 'password' or '123' in a password and 40% use personal information in their password.

So... what's the secret to a really complicated password?

- Never use obvious things like "**password**" or "**123**" or "**qwerty**".
- Don't include **personal information** - this could easily be found with a simple trawl through your social media accounts.
- Think long - passwords should be **fifteen characters** or more.
- Use a mix of uppercase and lowercase letters, numbers and symbols.
- Try adding three words together like 'FishSeventeen-Sky' to make a strong password.
- Use a **random password generator** - 1Password (a password manager available at a discounted price when you download ClearScore Protect).

2. Never use the same password twice

Everyone should have a different password for every account they have online.

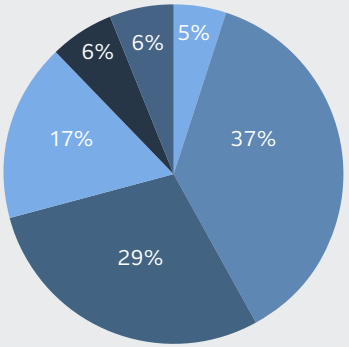
It's very reassuring that over half (53%) of people surveyed said they use a different password for every online service they use, with 29% of people having five to ten passwords and 17% having 11 or more.

However, it's worrying that just over a third of people in the UK (37%) have just two to three passwords which they rotate between accounts. This is better than the 5% who have only one password they use for everything, but it is still not safe enough to provide protection from fraud.

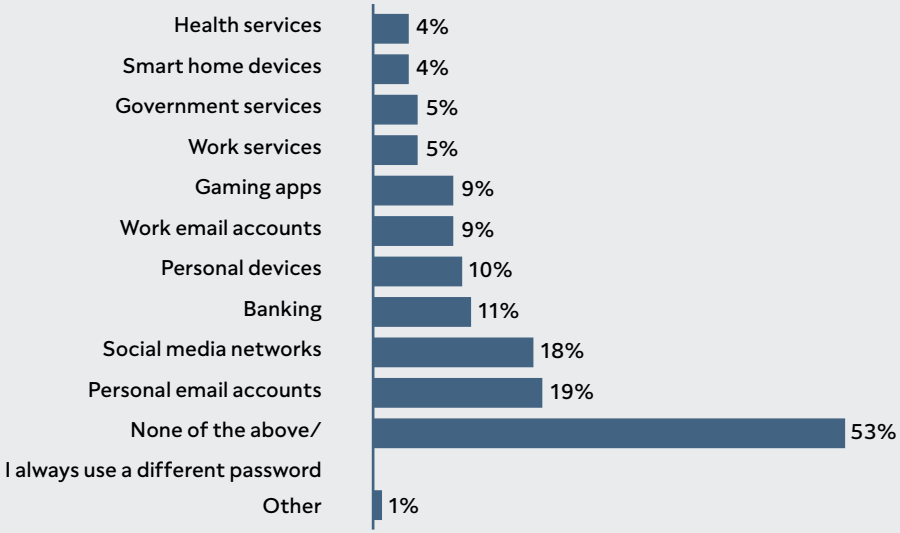
People are most likely to reuse the password they use for their personal email accounts (19%) and social media networks (18%).

How many different passwords do you have for all of your online accounts and apps (incl. email, Uber, online banking, Spotify, Netflix, etc)?

5%	1 password (I use the same password for everything)
37%	2-3 passwords (I rotate 2-3 passwords I can remember)
29%	5-10 passwords
17%	11+ passwords
6%	I don't know
6%	I'm not sure how many passwords I have because I use a password manager



For any of the following services, do you use the same password that you use for another service?



OTHER THAN GREAT PASSWORD HYGIENE, WHAT ELSE CAN I DO TO PROTECT MYSELF AGAINST FRAUD?

1. **Keep your social media private:**

   A hacker only needs three pieces of information to steal your identity - your name, address and date of birth. Once they have this, they can buy fake ID documents using your details. They can also use information you post on social media to guess your passwords. So be wary of oversharing online, and never put your birthday or address on your social media accounts.

2. **Check your bank statements:**

   Don't underestimate the importance of checking your bank statements regularly, and if you spot any suspicious transactions, report them to your bank or credit card provider immediately.

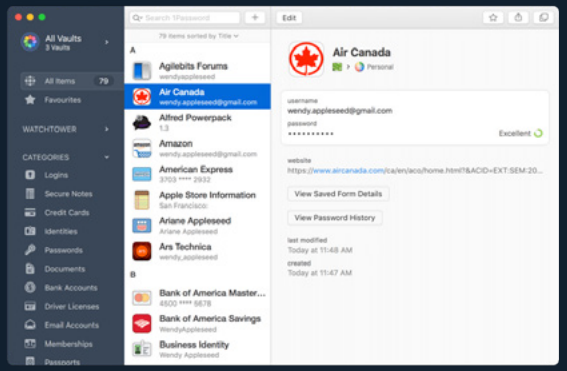
3. **Enable two-factor authentication on your important accounts:**

   If your account is only protected by a password, it's at risk of being hacked. Two-factor authentication adds another layer of protection by asking you to re-confirm your identity using something other than a password. This could be a text to your phone, or an authentication app. Two-factor authentication is a must for your email, banking, social, PayPal, ClearScore and password manager accounts.

Dark fact: Only 23% of UK residents use a password manager, with 17% saying they've never even heard of password managers.

It may seem like a lot of admin having a different password for everything... but that's what password managers have been invented for.

With password managers, you only need to remember one password to unlock all of your accounts (so it's worth making it really complex) and the manager locks away and remembers the rest of your passwords in a digital vault. Through ClearScore Protect you can get a discount on 1Password, a password manager with options for families and businesses which even tells you if services you have accounts with have suffered a data breach, or if they have a two-factor authentication option that you should be using.



Source: 1Password

4. Be wary when opening emails or answering phone calls:

Be vigilant of what lands in your inbox - if you're even a little unsure about something, don't reply or click on any links in the email. If the sender is pretending to be a real company, search for that company's details and get in touch with them this way, rather than replying to the email. The same goes for phone calls. Sometimes a scammer will use the information they've stolen from you to make the phone call or email seem more legitimate, for example by stating your full name and address.

5. Make sure your mail gets to you:

If you're moving house, make sure you redirect your mail to your new address so it doesn't fall into the wrong hands. You can set up your re-direction online, or visit your local Post Office branch. You should also consider locking your mailbox if someone could get access to it.

6. Shred your documents:

It's best practice to shred your utility bills, bank statements, and any other documents with personally identifiable information on them before you recycle them. While you might not think anyone has time to go through your bins, you'd be surprised at the lengths criminals are willing to go to to steal your money.

7. Check your credit score and report regularly:

With ClearScore's Alerts feature, you'll receive regular updates based on changes on your Equifax credit report. Keep an eye on any updates to spot suspicious activity early and take action quickly.

Key takeaways

1. Visit ClearScore Protect to find out if your passwords are for sale on the dark web.

2. If you find your passwords are for sale on the dark web, change all your passwords right away.

3. If you become a victim of fraud, contact your bank and lenders, Action Fraud, Cifas and Victim Support for help - also keep on eye on your ClearScore report to catch suspicious activity early.

4. The UK population is good at making complex passwords, with only 17% using the phrase 'password' or numerical sequence '123' in their password and 73% of people not including personal info in their passwords.

5. People in the UK also seem to largely adhere to the advice that it's wise to have one password for every online account, with 46% of those surveyed having five or more passwords.

6. Password managers are your friend. Only 23% of Brits use a password manager but these are invaluable tools to help ensure your password hygiene is tip-top.

Conclusion

THANK YOU FOR READING

ClearScore's first ever Darkpaper covered a lot of ground.

It started off by diving into people's conceptions and misconceptions about the dark web, before setting the record straight with the truth.

The Darkpaper then looked into the state of online fraud in 2020 and what that has to do with the dark web, namely that it is used as a marketplace to sell people's data and steal their identities. It was here that it unveiled the frightening statistic that a third of the UK population has fallen victim to online fraud. Then it explored the impact COVID-19 has had on the online fraud landscape, notably that it has generated a vast array of coronavirus-related scams looking to exploit people's fears, already robbing UK residents of £1.6 million

In the final part of the Darkpaper, the focus was on how individuals can protect themselves. This included information about ClearScore Protect, the new dark web monitoring service, which detects whether your passwords are located on the dark web so you can be proactive about changing all your passwords, helping to prevent online fraud.

From the team at ClearScore, we hope you finish reading this feeling empowered to share your knowledge so that more people know how to take precautions and protect themselves against online fraud.

With this in mind, see the checklist of measures that readers of this Darkpaper can take to protect themselves against online scams.

ONLINE FRAUD PROTECTION CHECKLIST

- **Get a ClearScore account** – with the ClearScore Alerts feature you'll receive regular updates based on daily changes on your Equifax credit report meaning you can take action quickly if you detect any suspicious activity. You can get started here.
- **Get ClearScore Protect** – once you have a ClearScore account you can activate ClearScore Protect, which will notify you if any passwords associated with your email address are on the dark web so you can proactively change all your passwords and avoid becoming a victim of fraud. Find out more here.
- **Change up all your passwords** – ensure they are as complicated as possible. That means no "password", "123" or any personal information.
- **Create one password for every online account** – keep track of your passwords with a password manager like 1Password which is available at a discounted price if you download ClearScore Protect.
- **Set all your social media sites to private** – stop criminals from trawling them for personal information about you.
- **Set a reminder to check your bank statements regularly** Flag any unusual activity with your bank.
- **Get a lock for your mailbox** – the only person who should have access to your mail is you.
- **Buy a shredder** – and destroy all documents that have any personal information on them before you recycle them.

ABOUT CLEARSCORE

ClearScore is the UK's number one free credit score and financial product marketplace. Founded in 2015 with the mission to help users take control of their financial health, ClearScore is the industry leader in giving everybody access to their credit score and report for free, forever.

Winners of prestigious awards such as the Queens Award for Enterprise and featuring on The Sunday Times Best Companies to Work For list, ClearScore combines a team of industry experts, sophisticated algorithms and clever tech with a trustworthy brand.

The result is a beautiful product that delivers an experience that is clear, calm and easy to understand. ClearScore uses data every step of the way to ensure that users see the most relevant financial products for them, giving them the tools to manage their finances in a way that suits them.

With over 9 million UK users, and a further 2 million worldwide, ClearScore constantly innovates to help their users on a journey to greater financial wellbeing. Co-founded by CEO, Justin Basini, ClearScore is based in London and is supported by investment from QED Investors, Blenheim Chalcot and Lead Edge Capital.

CONTACTS

If you have any questions about this Darkpaper and its contents, or would like to find out more about ClearScore or ClearScore Protect, please contact: Alice Spraggon or Mary Taylor at clearscore@clarity.com.

METHODOLOGY

Proprietary data comes from three sources in this Darkpaper. The majority of the data was produced from ClearScore's nationally representative survey with research agency Vitreous World, looking at the attitudes of 3,000 UK consumers in April 2020 around their understanding and experiences of the dark web, online fraud and password safety. Data was collected via an online survey with a margin of error of +/- 1.8%.

Data on financial concerns and basic understanding of the dark web was sourced from a nationally representative Medialab YouGov survey of 2,026 UK consumers. Total sample size was 2,026 adults. Fieldwork was undertaken between 7th - 10th February 2020. The survey was carried out online. The figures have been weighted and are representative of all GB adults (aged 18+).

Data on the average number of account passwords stolen and made available on the dark web was sourced directly from ClearScore Protect's early user base of 305,000 people.

Endnotes

1 Cambridge University Press, 'Meaning of dark web in English', The Cambridge Dictionary[web article], 2020, https://dictionary.cambridge.org/dictionary/english/dark-web, (accessed 15 April 2020).

2 Marshall, C; Vukcevic, A., 'What is the dark web? How safe is it and how to access it? Your questions answered', Techradar [web article], 11 June 2019, https://www.techradar.com/uk/news/what-is-the-dark-web-how-safe-is-it-and-how-to-access-it-your-questions-answered, (accessed 15 April 2020).

3 Shim, T., 'How to access the Dark Web: Browsing Dark Web, TOR Browser, and .Onion Websites', Web Hosting Secret Revealed [web article], 30 March, 2020, https://www.webhostingsecretrevealed.net/blog/web-tools/tourist-guide-to-dark-web-accessing-the-dark-web-tor-browser-and-onion-websites/, (accessed 15 April 2020).

4 Pagliery, J., 'The Deep Web you don't know about', CNN [web article], 10 March, 2014, https://money.cnn.com/2014/03/10/technology/deep-web/index.html, (accessed 15 April 2020).

5 Owen, G., Savage, N., ' The Tor Dark Net', The Global Commission on Internet Governance, Ontario, Canada and Chatham House (The Royal Institute of International Affairs), London, England, 2015, https://www.cigionline.org/sites/default/files/no20_0.pdf, accessed 15 April 2020.

6 Butler, S., 'Dark Web History: Where Did It Come From?', Technadu [Web Article], 23 December 2018, https://www.technadu.com/dark-web-history/52017/, (accessed 15 April 2020).

7 Aiello, C, 'Under Armour says data breach affected about 150 million MyFitnessPal accounts', CNBC [webarticle], 29 March, 2018, https://www.cnbc.com/2018/03/29/under-armour-stock-falls-after-company-admits-data-breach.html (accessed 23 April 2020).

8 MacRae, D., '75% of Large Businesses Suffered Security Breaches in 2019', Digit[Online Article], 27 March 2020, https://digit.fyi/75-of-large-businesses-suffered-security-breaches-in-2019/, accessed 15 April 2020.

9 Mansfield, J., 'How much is your data worth on the dark web?', SC Media[Online Article], 24 January 2020, https://www.scmagazineuk.com/data-worth-dark-web/article/1668693, accessed 16 April 2020.

10 Townsend, M., 'Fraudsters exploiting Covid-19 fears have scammed £1.6m', The Guardian [Online Article], 4 April 2020, https://www.theguardian.com/world/2020/apr/04/fraudsters-exploiting-covid-19-fears-have-scammed-16m, accessed 16 April 2020.

11 Corfield, G., 'Online face mask sales scams, 400% uptick of coronavirus phishing reports: Brit cops' workload shifts online along with the nation's', The Register[Online Article], 20 March 2020, https://www.theregister.co.uk/2020/03/20/coronavirus_scam_reports_police_up_400pc/, accessed 16 April 2020.

12 Ibid.

13 Townsend, M., 'Fraudsters exploiting Covid-19 fears have scammed £1.6m', The Guardian [Online Article], 4 April 2020, https://www.theguardian.com/world/2020/apr/04/fraudsters-exploiting-covid-19-fears-have-scammed-16m, accessed 16 April 2020.

14 HMRC, 'Guidance: Examples of HMRC related phishing emails and bogus contact', gov.uk [Online Article], 27 March 2020, https://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples/phishing-emails-and-bogus-contact-hm-revenue-and-customs-examples, accessed 16 April 2020.

15 NCA, 'Beware fraud and scams during Covid-19 pandemic fraud', National Crime Agency [Online Article], 26 March 2020, https://nationalcrimeagency.gov.uk/news/fraud-scams-covid19, accessed 16 April 2020.