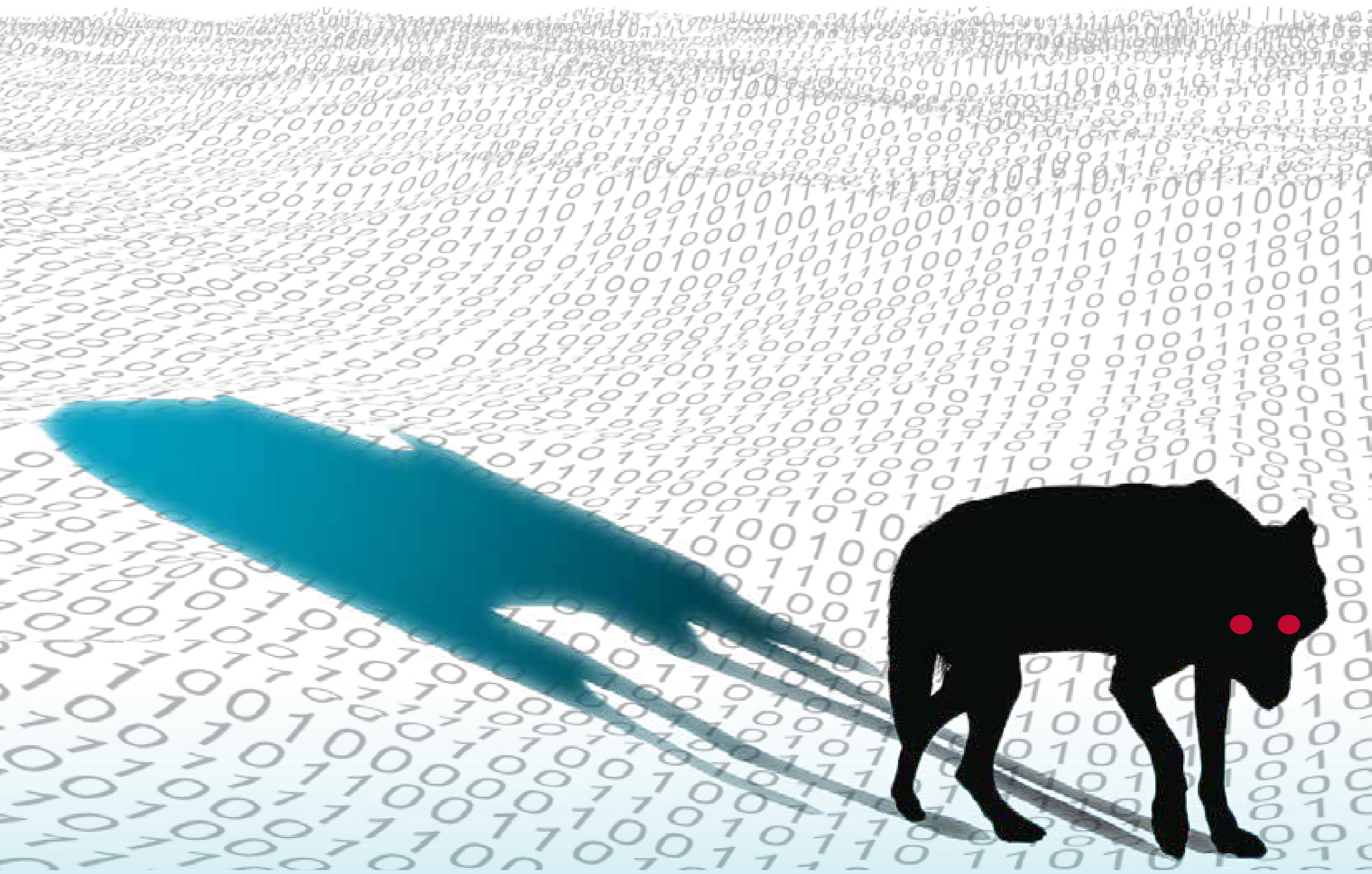
WOLVES OF THE INTERNET



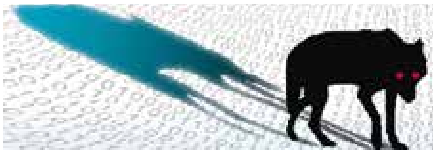
Where do fraudsters hunt for data online?

Cifas and Forensic Pathways

19 June 2018

Exclusive launch at the Cifas Annual Conference 2018

FOREWORD



“With identity fraud levels at an all-time high, the need to look at how criminals gain access to personal data is essential in trying to develop successful preventative measures. This collaborative research presented an exciting opportunity to combine the forensic expertise and investigative techniques of Forensic Pathways with the fraud knowledge of Cifas, together providing insight into how personal data can be pieced together from various online sources to commit identity fraud.

“The findings are eye-opening. This report not only demonstrates the vulnerabilities of personal data held on surface web platforms, but also highlights the pressing need to monitor these with more vigour, as well as look more closely at the use of software such as application programming interfaces (APIs), which allow for a mass of data to be obtained from these platforms. It also reminds us that although illegal activity occurs on the dark web, it is also prevalent on the surface web, where the selling of personal data through forums and online shops is clearly evident. We welcome further collaboration from all industries and sectors in the fight against identity fraud.”

Deborah Leary OBE, CEO, Forensic Pathways

“Cifas data shows that identity fraud accounts for the majority of fraud cases and in 2017, in 95% of the cases, the fraudster used the identity of an innocent victim of impersonation. The impact on the victim can be substantial. As a victim, not only has your personal information been abused, which for some can be incredibly psychologically damaging, but you will spend time and effort undoing the harm caused by a fraudster making applications in your name. On top of that, there is also the cost to the organisation suffering the fraud and to UK plc, which loses out through this fraudulent activity.

“As an individual, we can take steps to protect our identities online. The dilemma for those who want to promote themselves, either professionally or personally, is whether this promotion outweighs the risks of publicly revealing personal sensitive data. This research shows that many victims of impersonation have a public presence on social media and this, paired together with other publicly available information, can enable a criminal to perpetrate identity fraud.

“Organisations must take their responsibilities seriously too. As seen from this report, the personal information of victims of impersonation has been exposed through data breaches, not only facilitating those frauds but also damaging the reputation of the organisations involved and risking fines from the regulator. The protection of personal data must be viewed as a collective responsibility, with everyone playing their part, if we hope to curtail the harm caused by identity fraud.”

Mike Haley, CEO, Cifas

INTRODUCTION

Identity fraud continues to rise, as well as evolve.

In 2017, almost 175,000 cases of identity fraud were recorded to Cifas – a 125% increase compared with 10 years ago – and 84% of identity fraud cases occurred online. With this volume of cases being identified, and the effect that these cases have on both the victims of impersonation and the cost to the organisations that suffer the fraud, the value of prevention grows ever clearer.

There have been a number of campaigns put in place to educate the public on the risks of identity fraud, and steps that they can take to safeguard their identity details – notably the 'Cyber Streetwise', 'Take Five' and 'Not With My Name' campaigns. Yet identity fraud continues to rise to record levels. The question to ask is, where are criminals getting their data from in the first place? Although personal details may be sold on the dark web, how does it relate to behaviour and activity on the surface web? What role does phishing have to play, and how has it evolved?

Cifas has joined with Forensic Pathways to give insight to whether data compromise is due to online behaviour on the surface web, or whether it is an amalgamation of what criminals have collated and sold via the dark web. This research also provides insight as to what personal information is available on the Internet, and we explore some of the methods used to obtain it.

METHODOLOGY

Full details can be found in Appendix 1.

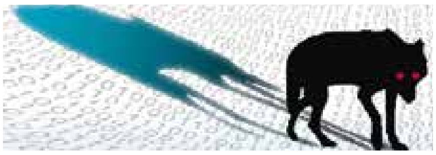
Cifas collated the details of victims of impersonation recorded by member organisations to its National Fraud Database. This data was processed for research purposes in line with data protection legislation. Any information containing personal information was communicated by both parties via a secure file exchange to ensure that the security of the personal data was observed at all times.

The data sent to Forensic Pathways included key information about victims, including their address at the time of the fraud, contact details and any banking information. Additional information included data about the case, such as when the case was filed by a member, which product was targeted and how many times that individual had been recorded on a case within the National Fraud Database.

Forensic Pathways then carried out a bulk search using an API. This was provided by pipl.com, which aggregates data from a number of sources and provides a collation of the data whereby a variation may have been used – for example, 'David' could be known as 'Dave'. 30,000 individuals were then selected from a random sample where name, date of birth, and either both telephone and email or where a telephone number only was present. These combinations were selected due to the high level of confidence associated with that individual being a match.

To carry out the dark web searches, Forensic Pathways used their own dark web 'crawler' to query the dark web search index. An important issue to note is that returns via the dark web were limited – this was due to the fact that a large proportion of access to data on the dark web has a transactional value. It was agreed by both Cifas and Forensic Pathways that no payment was to be made to be able to obtain such data – therefore if it was not being freely advertised, then it is possible that a victim would not be identified on a potential market place.

KEY FINDINGS



Personal information is sold both on the dark web and the surface web.

Data sold on the surface web is cheaper than on the dark web, however there is a higher risk of buying and selling on the surface web as it lacks the anonymity that the dark web provides. Personal information of victims of impersonation could be located on surface web forums, listed as 'Fullz'. These profiles have often been copied and pasted multiple times, containing information such as name, date of birth, banking details, security questions and answers. These profiles were often found on publicly open forums and on forums which have been taken over by sellers of personal data and not in line with the original creation of that forum.

If privacy settings are set to public, then a wealth of personal information can be obtained.

The increasing use and development of APIs on social media platforms and the surface web allows for the collection of a vast amount of publicly available data.

Nearly a third of victims are found to have visible 'digital footprint.'

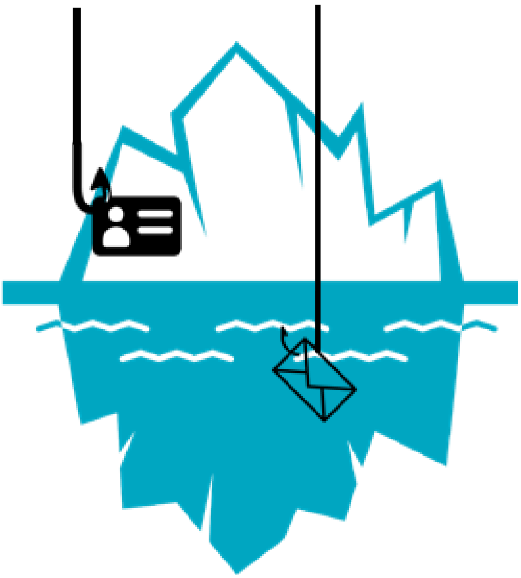
Of the sample of 30,000 individuals, 8,646 were found to have a digital footprint on the surface web, particularly on social media websites, giving a match rate of 29%. Younger victims had a high social media presence and presence on recruitment sites compared to older victims. Older victims had more of a presence on directory sites, such as phone directories or contact information for individuals and businesses.

The age of the victim is an indicator of the products subsequently applied for in their name.

Those victims aged under 21 found on a social media platform were more likely to have their details used to apply for mobile phone contracts, mail order products, personal store cards, and pay day loans. Those victims aged over 61 found on a social media platform were more likely to have their details used to apply for personal credit cards and personal current accounts.

Older people more likely to compromised by data breaches.

Those victims aged over 61 were least likely to be found on a social media sites, but more likely to have an account compromised through a data breach.



Company directors are at particular risk.

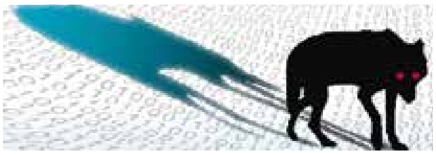
From the 8,646 individuals, 13% of those found on the surface web were company directors. 96% of these company directors could be found on Companies House, with 76% of these having their home address registered as their business address. For a number of them it was not the most current directorship that revealed this information but a dissolved directorship.

Two-thirds of victims compromised through a data breach or social media.

Based on the findings in this report, it can be approximated that 65% of victims of impersonation could be identified as having been compromised through a data breach or through social media.

Phishing remains a key method to obtain personal data.

Phishing may account for the 35% of victims of impersonation who have not been compromised through social media or data breaches. As well as 'kits' that are sold on the dark web which replicate well known banking and government brands, phishing also occurs on social media in the form of encouraging individuals to 'share' a phishing scam post in the hope of winning a prize. This tactic is supported by recent research that shows that scams offering a 'reward' to an individual, such as a prize or refund, rather than threatening them with restriction of access to a service, have a greater chance of success. This is because threatening scams are more likely to trigger a defensive response from the victim and be rejected.



CONCLUSIONS

There is a wealth of information freely available on an individual on the surface web, let alone what can be obtained through the dark web. The findings in this report show that the footprint we leave on the surface web, be it through social media, forums or publicly available data, can all be pieced together to potentially put us at risk of impersonation. For instance, an individual may take steps on a personal level to protect their identity by adjusting settings on social media platforms, but there are still publicly available directories such as the register of births, deaths and marriages, Companies House, and phone directory sites that all reveal additional pieces of information about an individual. In a world of increasing transparency and more access to public data, personal privacy can be compromised.

It is not just the presence on social media or publicly available data which can contribute to the risk of impersonation. A number of forums on the surface web have been flooded with individuals trying to sell personal data or selling their services as a hacker, often re-posting the same personal data a number of times. Although the dark web allows the buyer and seller a degree of anonymity, it is fairly restricted in terms of how products are advertised and it can be difficult to navigate. Although there is a higher risk for purchasing on the surface web, the products are cheaper and significantly more accessible than those available on the dark web.

There is a lack of regulation around forums, with some forums that had been originally created for one purpose now being used to advertising personal data for sale. Consideration needs to be given to the security and moderation of such forums, for example automatically rejecting posts containing particular key words. Similarly, old forums need to be shut down to prevent criminals taking advantage of posting within them.

Phishing remains a common method of obtaining personal data. Where victims of impersonation within the sample could not be found on social media platforms or in data breaches, other methods such as phishing may been the cause of the compromise of their personal data. Phishing attacks evolve over time, so they remain an effective way for fraudsters to trick their victims into revealing their personal information.

RECOMMENDATIONS

1 LISTEN

The monitoring and administration of forums should be enforced to ensure that old forums are removed and that there are sufficient channels to report abuse to the administrator.

2 CLEANSE

Old profiles on social network sites that are no longer used need to be deactivated and deleted.

3 DEFAULT

Profiles should be set automatically to the highest privacy settings so the individual can then select what information to be shared.

4 EXPLORE

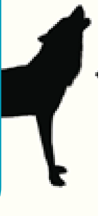
Further research should be conducted into the balance between transparency and proportionality of publicly available data.

5 INVESTIGATE

The way APIs can be obtained and used should be addressed. A standard of verification could be adopted by companies that offer API services to determine the legitimacy of the user and why they are using the service.

6 MONITOR

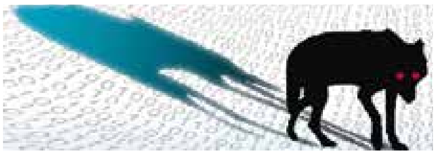
Hosts of platforms should follow in the steps of Facebook and shut down any profiles that are not used within a certain time period.



7 PROTECT

Individuals should regularly change their passwords, use two-factor authentication and look out for the secure site symbol.

THE INTERNET AND DATA

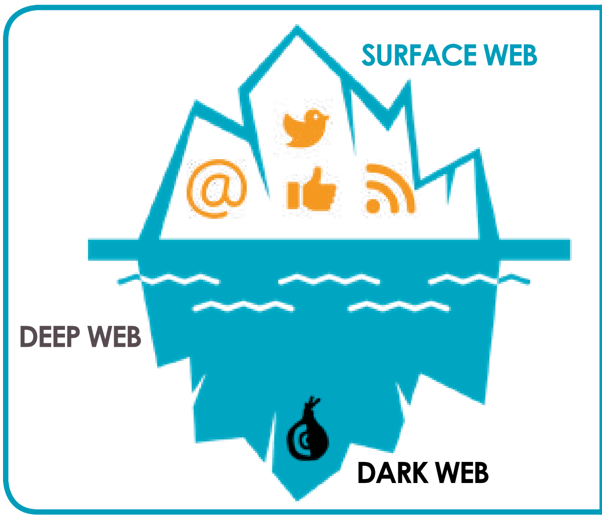


WOLVES OF THE INTERNET

Is it all we see it to be?

The Internet is made up of various layers. The ‘surface web’ layer makes up 10% and is a collection of websites which are indexed by search engines such as Google, Yahoo and Bing. These sites are easily accessible through normal browsers. There is also the ‘deep web’ layer, which makes up around 90% of the Internet: this is a collection of websites that are not indexed by search engines and where you need credentials such as a username or password to access. An example would be Facebook or online banking – you can still see it on the surface web, but you need credentials to access particular parts of it. The ‘dark web’ is a subset of the deep web.

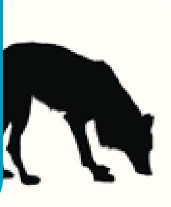
Put simply, the Dark Web is a collection of websites which exist on encrypted networks, such as The Onion Router (Tor) or Invisible InternetProject (I2P). Encrypted networks allow users to securely transmit information, permitting anonymity and the ability to spoof an individual’s location. However, due to the anonymity it provides, the dark web has now become a hub for illegal activity. According to Europol and the European Monitoring Centre for Drugs and Drug Addiction, two thirds of the dark web transactions involve the sale of drugs1. In May 2018, Forensic Pathways identified 21,000 live websites on the Tor network and 4,500 I2P websites[2]. Forensic Pathways carried out a search on the term ‘Fullz’ (financial personal information) and found over 10,000 posts which may contain multiple records of personal data for sale. However, due to the constraints of not paying to see the data, we could not identify what data was being sold on.



Surface Web:
- <10% of Internet
- Indexed Internet

Deep Web:
- >90% of Internet
- Unindexed Internet

Dark Web:
- Subset of Deep Web
- Hidden services



So how much is personal data worth? Your entire online identity could fetch around £800, according to the Dark Web Market Price Index 2018[3], which details the value of certain credentials as well as logins to social media, food delivery sites and online dating websites:

Information type	Price
Paypal Login	£279.74
Online banking details	£161.81
Credit card details	£56.50
Debit card details	£6.30
Proof of Identity	£46.14
Passport	£39.76
Ebay login	£26.20
Apple login	£10.98
Facebook login	£3.74
AOL login	£3.00
Hotmail login	£2.37
Deliveroo login	£3.74

Source: top10VPN: Dark Web market price index Feb 2018

Purchasing these personal details will enable an individual to fraudulently apply for products or services that they would not obtain otherwise, and commit fraud on a wide scale against a number of organisations. By purchasing via the dark web, it allows the individual a degree of anonymity and low level risk of traceability.

[1] *European Monitoring Centre for Drugs and Drug Addiction and Europol (EMCDDA) (2017), Drugs and the darknet: perspectives for enforcement, research and policy, EMCDDA–Europol Joint publications, Publications Office of the European Union, Luxembourg.*

[2] *Forensic Pathways web crawler, May 2018*

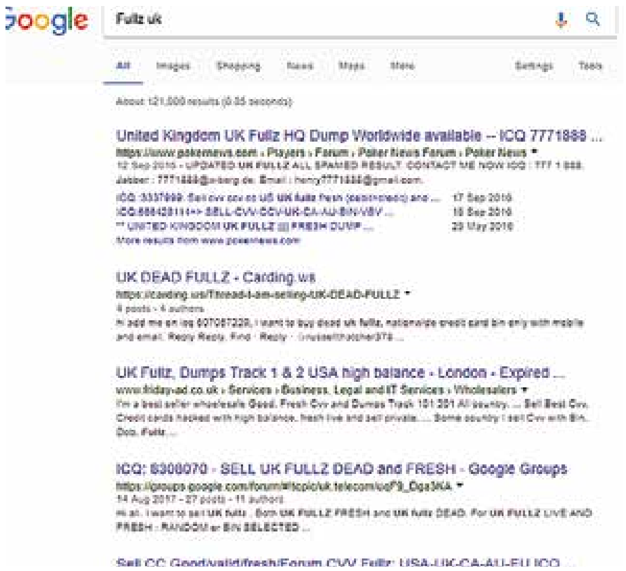
[3] *https://www.top10vpn.com/privacy-central/cybersecurity/dark-web-market-price-index-feb-2018-uk/*

Myth buster: personal data is only sold on the dark web

In the Netcraft April 2018 Survey, the surface web reached 1,783,239,123 websites[4] – which dwarfs the number of sites to be found on the dark web, and is a gateway for various activities to occur, both legal and illegal. A simple google search of the term 'Fullz' will bring up various online shops advertising personal details for sale. The Google search image below left shows how an example of results obtained from searching on the term 'Fullz UK'.

Through the searching process, postings containing profiles of personal information were identified. These all had a high level of detail attributed with them: detail such as full name and date of birth, online banking details, email addresses and passwords, as well as security questions and answers. Below right is a typical example of what a profile looks like.

Image: Google search 21/05/18



Fullz uk

About 121,000 results (0.35 seconds)

United Kingdom UK Fullz HQ Dump Worldwide available -- ICQ 7771888 ...
https://www.pokernews.com › Players › Forum › Poker News Forum › Poker News
12 Sep 2016 - UPDATED UK FULLZ ALL SPAMED RESULT. CONTACT ME NOW ICQ : 777 1 888. Jabber : 7771888@jabber.de. Email : henry7771888@gmail.com.
ICQ: 3337999. Sell cvv ccv cc US UK fullz fresh (balcheckeed) and ... 17 Sep 2016
ICQ:688428111=> SELL-CVV-CCV-UK-CA-AU-BIN-VBV ... 18 Sep 2016
** UNITED KINGDOM UK FULLZ ||| FRESH DUMP ... 29 May 2016
More results from www.pokernews.com

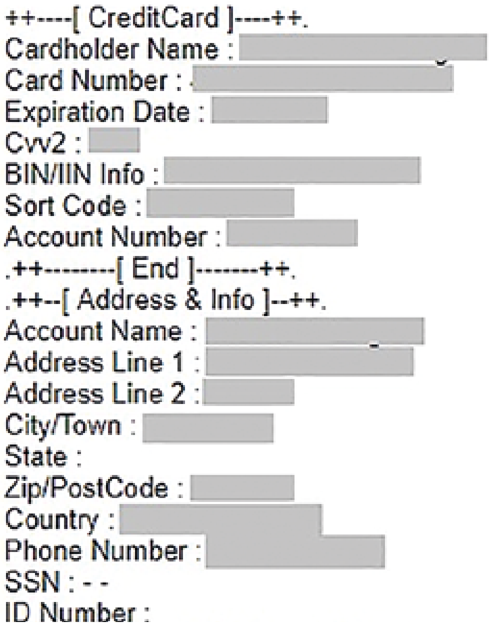
UK DEAD FULLZ - Carding.ws
https://carding.ws/Thread-I-am-selling-UK-DEAD-FULLZ
4 posts - 4 authors
Hi add me on icq 607087220, i want to buy dead uk fullz, nationwide credit card bin only with mobile and email. Reply Reply. Find · Reply · (russellthatcher378 ...

UK Fullz, Dumps Track 1 & 2 USA high balance - London - Expired ...
www.fridayad.co.uk › Services › Business, Legal and IT Services › Wholesalers
I'm a best seller wholesale Good. Fresh Cvv and Dumps Track 101 201 All country. ... Sell Best Cvv. Credit cards hacked with high balance, fresh live and sell private. ... Some country I sell Cvv with Bin, Dob, Fullz ...

ICQ: 6308070 - SELL UK FULLZ DEAD and FRESH - Google Groups
https://groups.google.com/forum/#!topic/uk.telecom/ucF9_Dga3KA
14 Aug 2017 - 27 posts - 11 authors
Hi all, I want to sell UK fullz . Both UK FULLZ FRESH and UK fullz DEAD. For UK FULLZ LIVE AND FRESH : RANDOM or BIN SELECTED ...

Sell CC Good/valid/fresh/Forum CVV Fullz: USA-UK-CA-AU-EU ICQ ...

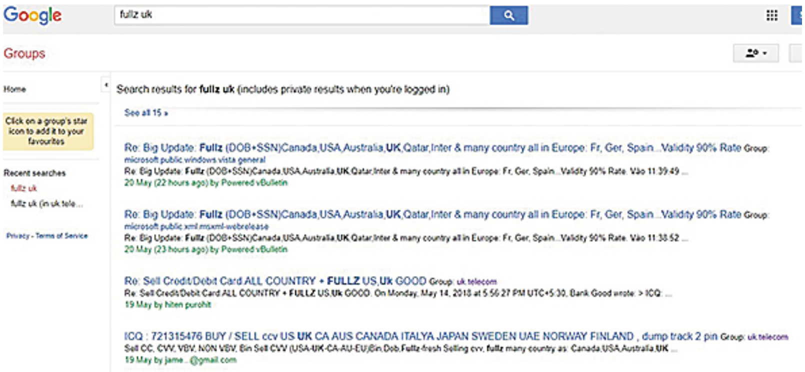
Image: extracted from a forum 21/05/18



++----[CreditCard]----++.
Cardholder Name : [redacted]
Card Number : [redacted]
Expiration Date : [redacted]
Cvv2 : [redacted]
BIN/IIN Info : [redacted]
Sort Code : [redacted]
Account Number : [redacted]
.++--------[End]-------++.
.++--[Address & Info]--++.
Account Name : [redacted]
Address Line 1 : [redacted]
Address Line 2 : [redacted]
City/Town : [redacted]
State :
Zip/PostCode : [redacted]
Country : [redacted]
Phone Number : [redacted]
SSN : - -
ID Number :

In terms of what is sold on the surface web, the snapshot above, as well as the findings below, indicate that forums are an active platform for those wishing to sell personal data. One of the reasons for advertising the selling of personal details on forums may be due to the enhanced level of exposure – forums on the surface web are more easily accessible than those on the dark web and therefore the possibility of more people seeing such posts is heightened. There is also a high turn-over of messages posted on forums. Below shows an example of how these are advertised in a forum:

In one forum (designed for the intention of sharing information around telecom advice) 454 of the 465 posts made during April 2018 made explicit references to be able to provide personal data or to advertise their hacking services. Phrases such as 'Fullz', 'dump' and 'tracks 1 and 2' are all referenced in the title of the posting, and relate to bank details and CVV codes. On another forum, labelled as a hub for Microsoft Internet Explorer news, all of the 118 posts for April 2018 were in relation to providing personal data or hacking services.



fullz uk

Groups
Home
Click on a group's star icon to add it to your favourites
Recent searches
fullz uk
fullz uk (in uk.tele...
Privacy - Terms of Service

Search results for **fullz uk** (includes private results when you're logged in)

See all 15 »

Re: Big Update: **Fullz** (DOB+SSN)Canada,USA,Australia,**UK**,Qatar,Inter & many country all in Europe: Fr, Ger, Spain...Validity 90% Rate Group: microsoft.public.windows.vista.general
Re: Big Update: **Fullz** (DOB+SSN)Canada,USA,Australia,**UK**,Qatar,Inter & many country all in Europe: Fr, Ger, Spain...Validity 90% Rate. Vào 11:39:49 ...
20 May (22 hours ago) by Powered vBulletin

Re: Big Update: **Fullz** (DOB+SSN)Canada,USA,Australia,**UK**,Qatar,Inter & many country all in Europe: Fr, Ger, Spain...Validity 90% Rate Group: microsoft.public.xml.msxml-webrelease
Re: Big Update: **Fullz** (DOB+SSN)Canada,USA,Australia,**UK**,Qatar,Inter & many country all in Europe: Fr, Ger, Spain...Validity 90% Rate. Vào 11:38:52 ...
20 May (23 hours ago) by Powered vBulletin

Re: Sell Credit/Debit Card ALL COUNTRY + **FULLZ** US,**Uk** GOOD Group: uk.telecom
Re: Sell Credit/Debit Card ALL COUNTRY + **FULLZ** US,**Uk** GOOD. On Monday, May 14, 2018 at 5:56:27 PM UTC+5:30, Bank Good wrote: > ICQ: ...
19 May by hiten purohit

ICQ : 721315476 BUY / SELL ccv US **UK** CA AUS CANADA ITALYA JAPAN SWEDEN UAE NORWAY FINLAND , dump track 2 pin Group: uk.telecom
Sell CC, CVV, VBV, NON VBV, Bin Sell CVV (USA-UK-CA-AU-EU)Bin,Dob,Fullz-fresh Selling cvv, **fullz** many country as: Canada,USA,Australia,**UK** ...
19 May by jame...@gmail.com

Image: forum search 21/05/18

Forensic Pathways found a sample of 80 of these postings, all provided as 'free samples' to indicate the detail of what could be provided to a potential buyer of personal information. Of these profiles, 50% were found on tailored forums, specifically created with the intention of sharing such personal information. 43% were found on 'appropriated forums'. This is where the forum has been created for one purpose and has then been taken over with posts not related to that purpose. The forums include tourist, healthcare, and leisure forums.

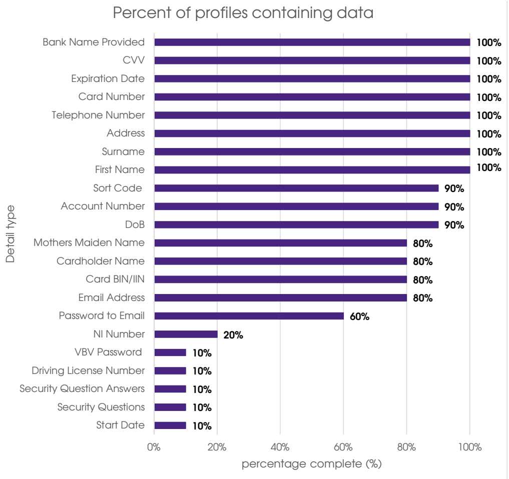
13% of these profiles related to individuals who had been recorded to Cifas as victims of impersonation (n10). All of the victim details had been used multiple times to apply for products and 76% used the genuine current address of the victim.

[4] *https://news.netcraft.com/archives/2018/04/26/april-2018-web-server-survey.html*

From the 10 postings found, 50% of them are most likely to have been obtained via phishing or malware, due to the additional footprint information left on the profile such as device, browser and IP address. These details suggest that a victim may have used their device to access a phishing website disguised as a legitimate website, such as a banking website, and then proceeded to enter their sensitive information.

Nine of the 10 profiles were posted prior to the victim being recorded to the Cifas database, with one application for a product made within 12 days of the identity being posted online. Furthermore, nine of the 10 were found on forums. Five were found on leisure forums related to online betting. three of the forums were Google Groups. All profiles had first name, surname, address, telephone number, card number and CVV number.

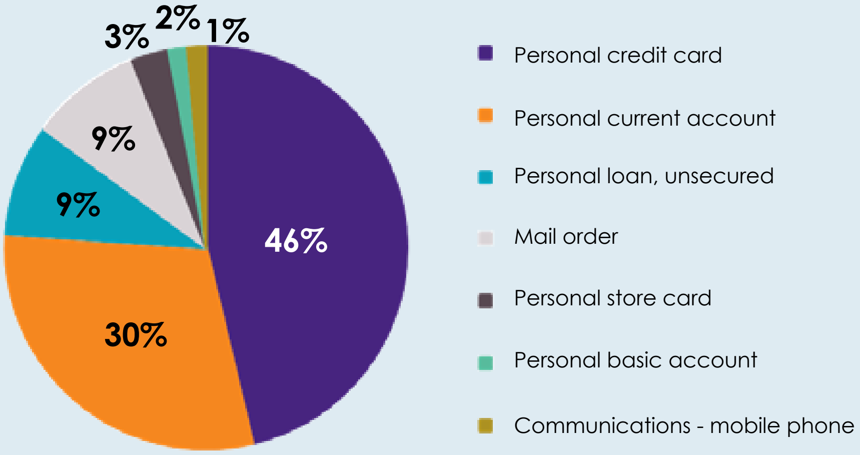
Interestingly, 80% of profiles also had mother's maiden name and 60% also included the password to the email account associated with that individual. The full breakdown of details found on these profiles is detailed opposite.



Breakdown of products applied for using details of victims that appeared in a freely available profile (Fullz)

The majority of products applied for using the identities of those found on freely available profiles were financial products, particularly personal credit cards.

Overall, a large number of applications were unsuccessful. This may be due to the fact that these freely available 'Fullz' profiles are typically copied and pasted, meaning those details have been used a number of times for applications. (46%).



To ascertain how much this personal data would be worth on the surface web, Forensic Pathways were able to identify and record 58 different adverts over a period of 50 months, covering 54 unique sellers. Once Forensic Pathways had documented a sufficient sample size, the data was collated, cleaned and an average price was calculated for the following 'products'; Fullz, BIN and Dumps Track 1 & 2. It seems that data available on forums tends to be cheaper than the prices seen above on the dark web:

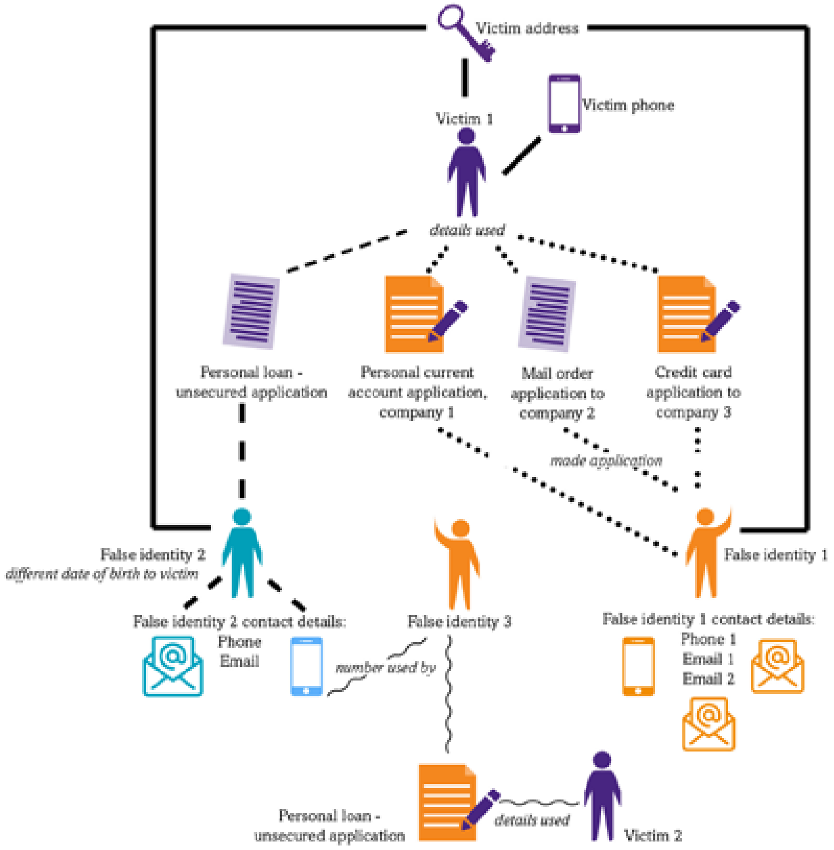
Product	Description	Price USD ($)	Price GBP (£)
Fullz	Personal data, including financial information.	$42.38	£31.63
BIN	Bank identification number – the first four to six digits of a bank card.	$21.74	£16.22
Dumps Track 1 & 2	Data held within the magnetic strip of bank cards.	$93.30	£69.92

Case study 1: High volume of applications made using the details from a 'Fullz' profile

This case study demonstrates how victim details from a freely available profile can be used in fraudulent applications:

One individual's details had been posted as a freely available 'Fullz' profile and used to apply for 22 products, all of which were financial products such as personal credit cards (36%) and personal current accounts (32%). The applications were made over a period of two years, with the most recent application being in 2018 and a third of the applications were successful. All of the applications were made using the genuine current address of the victim.

When looking at the details listed on the freely available profile for this individual, their first name, surname, date of birth and address were available, alongside telephone number, card details and banking details. These details had been posted on an online gambling forum 15 months prior to a case being recorded to the Cifas database. This individual's details have since been posted at least 41 times on google groups since 2016. Overall, there are at least 271 URLs linked to this profile.


Victim address
Victim 1
Victim phone
details used
Personal loan - unsecured application
Personal current account application, company 1
Mail order application to company 2
Credit card application to company 3
made application
False identity 2
different date of birth to victim
False identity 3
False identity 1
False identity 2 contact details:
Phone
Email
number used by
False identity 1 contact details:
Phone 1
Email 1
Email 2
Personal loan - unsecured application
details used
Victim 2

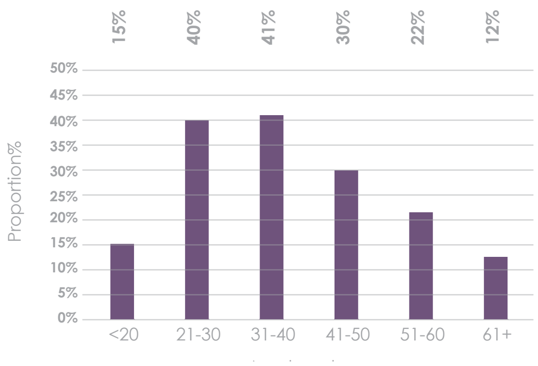
This individual's details could also be located on three social media platforms, however it was generally difficult to obtain any personal information other than a photograph and employment. What cannot be ascertained is whether the victim locked their profiles down before or after becoming a victim of impersonation. What can be determined from this case study is that criminals are prepared to use old details to obtain services or products fraudulently because it is simply free and has relatively low risk because it is freely available.

The question needs to be asked as to how these forums are being monitored and regulated? Should there be an automatic block on postings to forums with particular phrases or words? Although there is the perception that the selling of personal data occurs predominantly on the dark web, it is also prolific on surface web. To obtain the above examples, a sign-in to the forum was not needed, highlighting how easily accessible this data is.

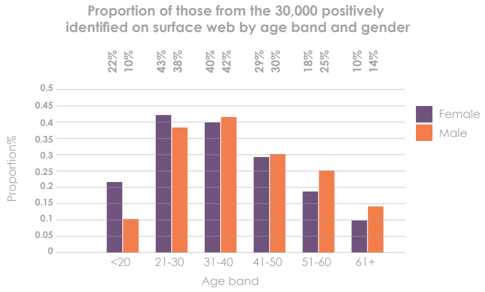
Impersonation and social media

Of the sample of 30,000 victims of identity fraud, 8,646 individuals were positively identified as appearing on social media platforms, a match rate of 29%. The age groups with the largest proportions of positively identified individuals were the 21-30 year olds (40%) and the 31-40 year olds (41%).

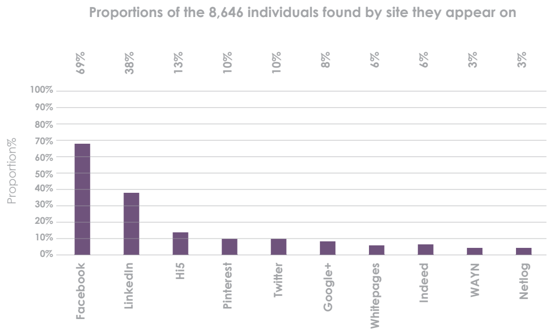
Proportions of those identified on surface web from the 30,000 sample by age band



However from the age of 31 years men were more commonly identified on social media than women, peaking for the 31-40 age group:


Proportion of those from the 30,000 positively identified on surface web by age band and gender

Of the social media sites used by the 8,646 individuals found, 69% had a Facebook footprint, followed by 38% on LinkedIn. Of note, all of those with a LinkedIn presence also had a Facebook presence.


Proportions of the 8,646 individuals found by site they appear on

When looking at the breakdown of each age group and sites (see the appendix 2 for a full breakdown):

- Those aged between 21 and 30 had the highest proportion of individuals that could be identified on Facebook (78%), followed by those aged between 31 and 40 years old and those aged under 21 (74% each).

- The age bands were fairly equal in relation to a LinkedIn presence, whereas the age groups with the highest a presence on Hi5 were those aged between 21 and 30 years old (19%) and 31 to 40 years old (19%). These age groups also had the highest presence on Pinterest with 12% and 11% respectively.

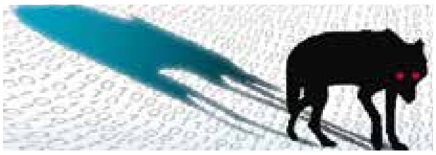
- The age bands on Twitter were also fairly equal in terms of a presence, however those under 21 had the highest presence on Google+* with 11% and job search website Indeed with 9%.

- Those aged 61+ had the highest proportion of those with a footprint on the Whitepages directory site with 17%.

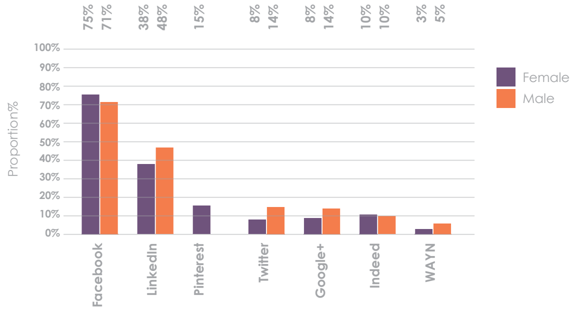
- Once again the age groups were fairly equal in relation to a presence on the WAYN (Where Are You Now?) website, but for those on Netlog the presence peaked slightly with 5% for those aged between 21 and 30 years old.

- The information above shows that there are differences in the type of social media and the age groups that use them. For instance, the younger age groups had a higher proportion of users on social media sites such as Facebook, Netlog and Google+, as well as recruitment sites such as LinkedIn and Indeed. Older age groups were found more on directory sites such as Whitepages.

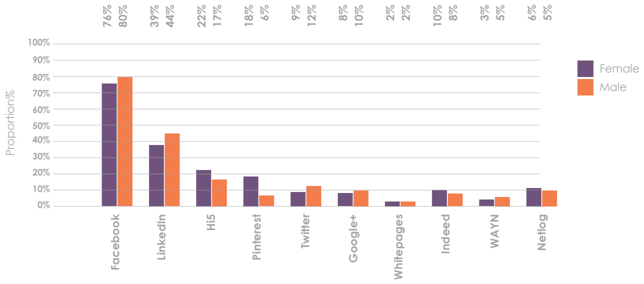
**Google+ is referred to as the plus.google domain name in the data*



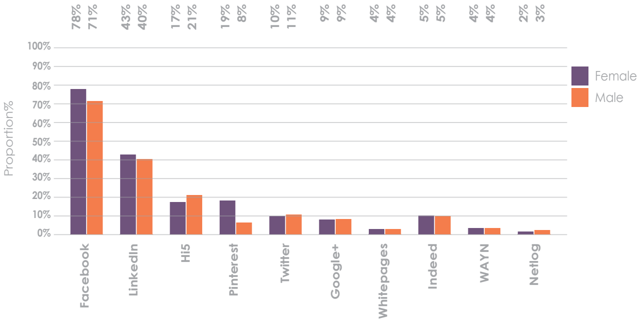
Proportions of presence on social media sites within the top ten sites by gender for for under 21's



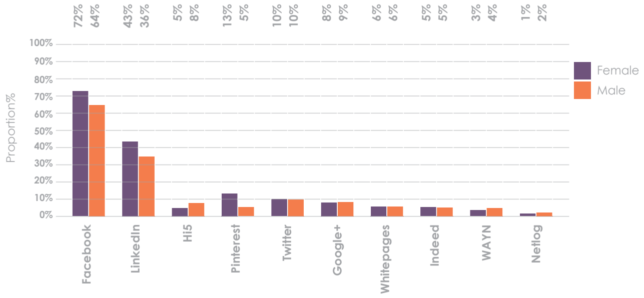
Proportions of presence on social media sites within the top ten sites by gender for those aged 21 to 30 years old



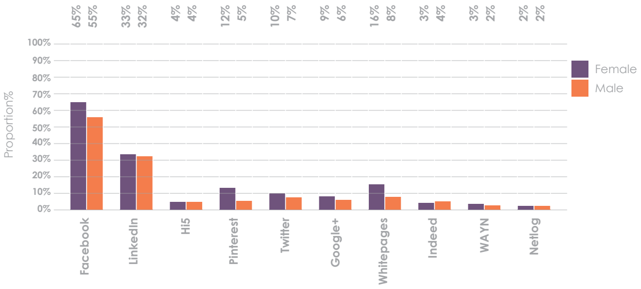
Proportions of presence on social media sites within the top ten sites by gender for those aged 31 to 40 years old



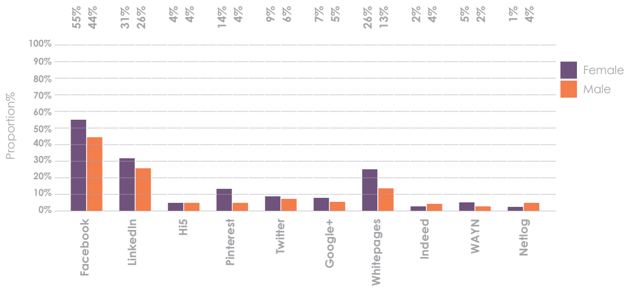
Proportions of presence on social media sites within the top ten sites by gender for those aged 41 to 50 years old

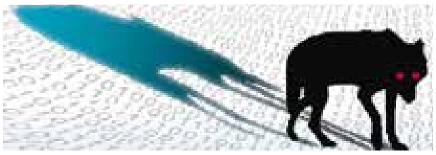


Proportions of presence on social media sites within the top ten sites by gender for those aged 51 to 60 years old



Proportions of presence on social media sites within the top ten sites by gender for those aged over 61 years old

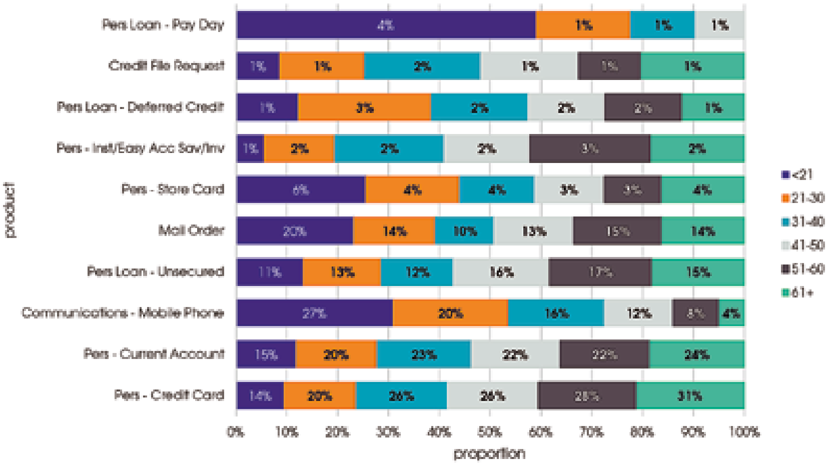




Of those victims found on surface web platforms, the majority of victims had their genuine current address used for fraudulent applications (82%). The majority of products applied for using the victims' details were personal credit cards (25%) and personal bank accounts (22%). The figure below shows the top ten products that had been applied for by age group, using the age of the victim at the time of the impersonation. Interestingly, those aged under 21 had the highest proportion of applications made for a mobile phone contract, a mail order product, personal store cards and pay day loans. Those aged over 61 had the highest proportion for personal credit cards and personal accounts.

Those whose details had been used for fraudulent pay day loan applications had a higher proportion of victims with a footprint on Facebook compared to other products. Interestingly, those aged under 21 had the highest presence on Facebook and were identified as more likely to have their details used for fraudulent pay day loan applications. Although those aged over 61 years old had a low social media presence, their details were more likely to be used for the fraudulent applications of personal credit cards and personal current accounts. This suggests that their details may have been found elsewhere and that social media platforms are less likely to the point of compromise of their data.

Top ten products applied for by age group of the 8,646 individuals with a surface web presence



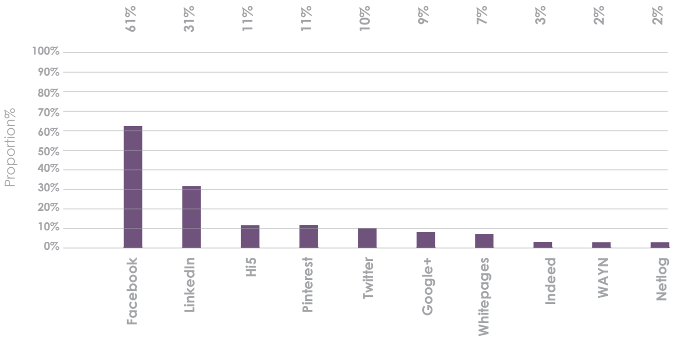
Company directors

An occupation was provided for 18% of those who were found on the surface web (n1588). The majority of those found were company directors (13%).

96% of those listed as a company director could be located on Companies House and of these, 76% had not only their name, with month of birth and year, but also their home address. For numerous individuals, the home address was not necessarily for the company that they had the most recent directorship, but for dissolved directorships. The majority had a Facebook footprint (61%) and perhaps, surprisingly, only 31% had a footprint on LinkedIn. Right is a breakdown of the sites in which a company director had a footprint.

Although a director may have taken steps to reduce their visibility on a social network site, the case study opposite shows how personal data can be pieced together from various sites such as Companies House, social media and blogs to have enough information to impersonate a director.

Proportions of company directors with a presence on surface web by website



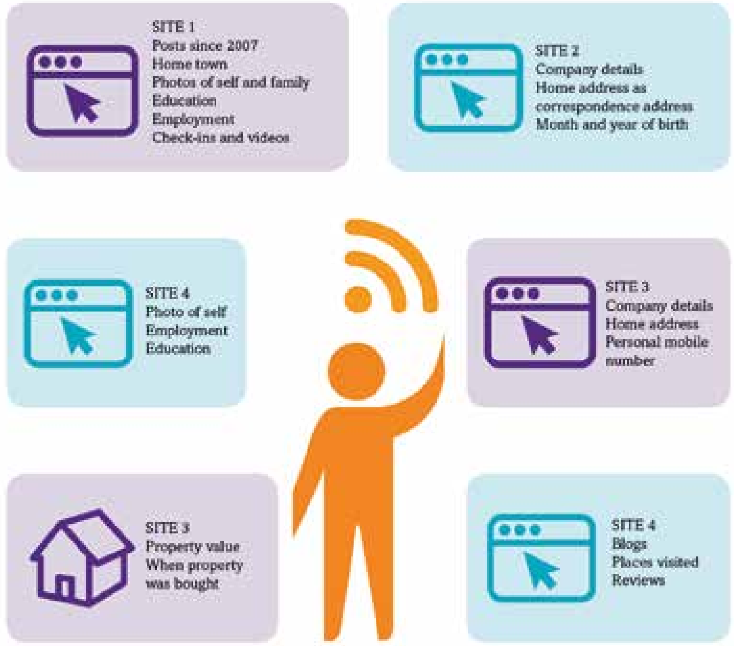
Case study 2: Gathering data on a company director

One individual had their details used to apply for products ten times between 2013 and 2018. 50% of those applications were successful. 90% of the cases involved the use of the victim's genuine current address but in 20% of the cases the birth date provided was incorrect. The majority of products were financial products such as personal credit cards and personal current accounts.

This individual happens to be a company director, who appears on Companies House and other director search engines. Even though the company was dissolved, all entries revealed the month and year this individual was born as well as their home address, which was used for the correspondence address. One site even has a street view of the home address.

This individual could also be found on at least nine different websites, but their email address had not appeared on a data breach according to haveibeenpwnd.com. This individual has an active digital footprint, often leaving a review on services that they have used, as well as places they have visited on travelling websites. The opposite diagram shows how this information can be collated to give a picture of an individual's identity.

Overall, there are several pieces of information available on the surface web to enable someone else to use this individual's identity. It is not just the factual information that can be used, such as current address, name, date of birth etc., but also there are key insights to this individual's life which could be an answer to a security question. This case study also shows that a wealth of information can be obtained from publicly available data sets.



How can data be harvested through social media?

Looking up potential victims one by one would be time consuming for a fraudster, but technology exists to do this more efficiently. Data that is harvested on a large scale is more than likely obtained through the use of an API. A recent, high profile example of this is the use by Cambridge Analytica of an API to harvest personal data. Although Facebook changed the way this API could be used in April 2015, it can still be used to collate publicly available data, including information held on company social media pages. If an individual's privacy settings are still set to public, then their personal information can be accessed.

Twitter also has a public API which works like a search function, providing information about specific users based on searching a specific term or keyword search to find users. Data that can be returned includes name, location, when the account was created, a link to a profile picture, any description included, which may include employment details, as well as a count on what they have tweeted and what they have 'liked' and 'bookmarked'.

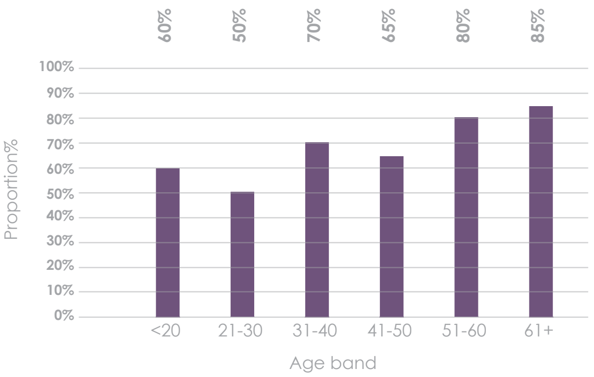
There is a question around what verification is needed to be able to use the API tools. For instance, in the case of Cambridge Analytica, the data was obtained through perfectly legitimate methods – the system was not hacked into, controls to access the data were not bypassed. It was more about how that information was then used and how the usage of that data is controlled.

What role do data breaches play?

Over recent years there have been an increasing number of high profile data breaches where organisations have lost large amounts of personal data. A sample of 20 individuals from each age group of those who could be found on social media was searched to ascertain if their email had been involved in a data breach. The search also revealed the source of the breach. Of the 120 individuals sampled, 68% had a compromised email account. 83% of those emails which had been compromised had been part of a single breach which exposed 711 million unique email addresses in August 2017. That breach exposed both emails and passwords and is one of the largest collections of breached information[5].

Overall, a higher proportion of the males from the sample had a breached email account compared to females (72% to 65%). In terms of age groups, those aged 61 and over had the highest percentage of email accounts which had been compromised. Also, those aged 61 and over had the highest proportion of those with five or more breaches, despite this age group having the lowest presence on social media.

Proportions of emails compromised by age group



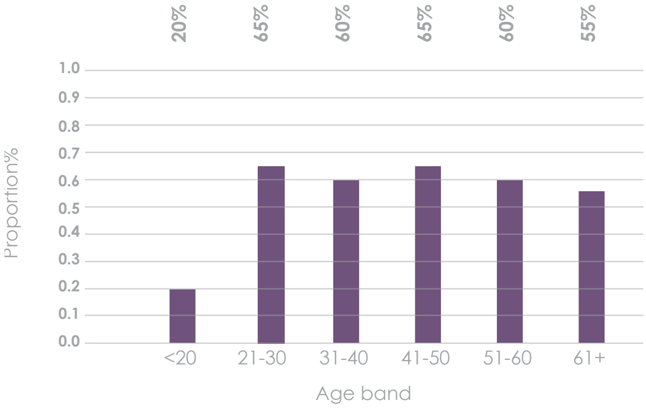
Of those where their account had been compromised, 77% of cases involved the use of the genuine current address of the victim and 20% involved the use of a previous address of the victim. This is interesting as Cifas' ***Fraudscape*** report in 2017 identified that only 5% of all impersonation cases involved the previous address of the victim. This suggests that either the data breached is old, or the victim had not updated their address with the provider which was the source of the breach.

For those that did not have an email account compromised, all of the frauds identified involved the genuine current address of the victim, suggesting that the details would have been obtained by other means.

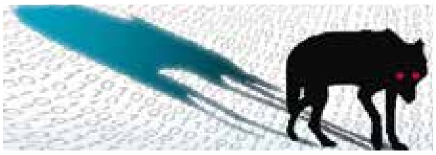
It should be noted that 71% of the 30,000 sample could not be identified as having a social media presence. The reason for this is that there was either insufficient confidence that the return from the search was them, or they simply did not have a social media presence, suggesting that this was not the point of data compromise for these individuals. A sample of 120 was also taken from those who could not be determined to have a social media presence, 20 from each age group. Of these, 54% of individuals had their email account released through a data breach, lower than those who did have a social media presence (68%) and all age groups were fairly even in relation to proportions of those who had a compromised account, except for those aged under 21 who had the lowest proportion of breached accounts with 20%. Those aged 61 years and older had a lower proportion of those with a breached account (55%) compared to their counterparts who had a social media presence (89%).

Based on these findings, approximately 35% of victims are not on social media and are not known to have been victims of a data breach. The question that needs to be asked is how are their details used for fraudulent applications?

Proportions of emails compromised for those not appearing on social media platform by age group

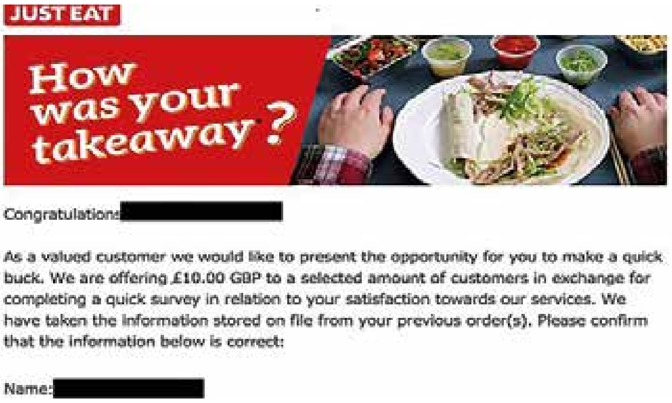


[5] *http://www.bbc.co.uk/news/technology-41095606*



How else can data be stolen?

Through one investigation, police uncovered an individual who sold details from 165,000 people and 63,000 credit and debit cards via the dark web. These details had been obtained via a 'phishing' email to customers of users for food delivery website Just Eat:



JUST EAT

Congratulations [redacted]

As a valued customer we would like to present the opportunity for you to make a quick buck. We are offering £10.00 GBP to a selected amount of customers in exchange for completing a quick survey in relation to your satisfaction towards our services. We have taken the information stored on file from your previous order(s). Please confirm that the information below is correct:

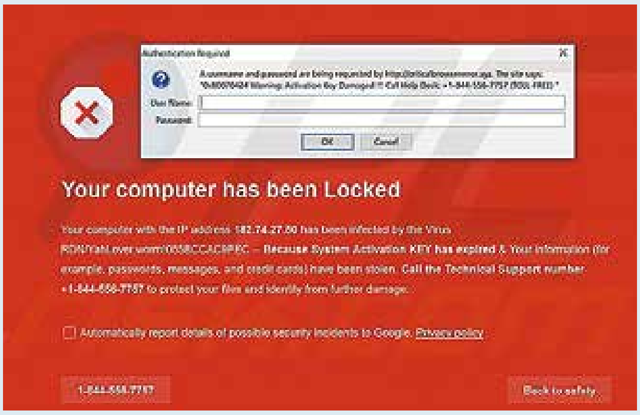
Name: [redacted]

Image: http://www.bbc.co.uk/news/uk-43965622

Despite the campaigns and awareness about phishing, a number of people still fall victim to them. Phishing campaigns appear to have evolved over time. Akamai gave some insight into some of the most prominent phishing attacks[6] and found that they could be classified into 'negative' campaigns and 'positive' campaigns, with a growing trend in the use of the latter.

The image below left is an example of a 'negative' campaign, which is designed to trigger fear, such as loss to access of a service. Akamai notes that it can also trigger some doubt from the victim as to how genuine it is.

Below right is an example of a 'positive' campaign, which interacts with the victim. It is designed to lead them to believe they can gain a benefit from playing a game and then sharing the link across their social network to win a prize. The creators make it seem more genuine by having a fake social network user comment on the post and strengthen trust in the victim. This enables those who have created the phishing campaign to harvest personal details to potentially sell on the dark web with anonymity.



Authentication Required

A username and password are being requested by [illegible]. The site says: "[illegible] Warning: Activation Key Damaged !! Call Help Desk: +1-844-556-7757 (TOLL FREE)"

User Name:

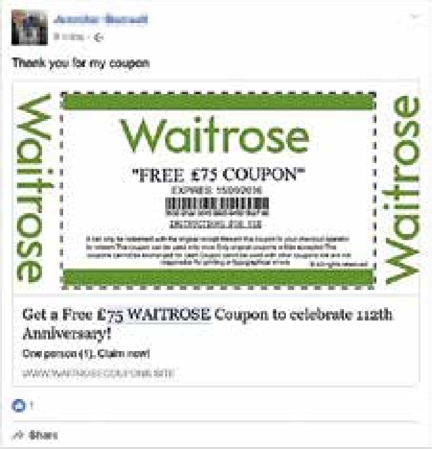
Password:

Your computer has been Locked

Your computer with the IP address 182.74.27.50 has been infected by the Virus [illegible] – Because System Activation KEY has expired & Your information (for example, passwords, messages, and credit cards) have been stolen. Call the Technical Support number +1-844-556-7757 to protect your files and identity from further damage.

☐ Automatically report details of possible security incidents to Google. Privacy policy

Image: https://www.pcrisk.com



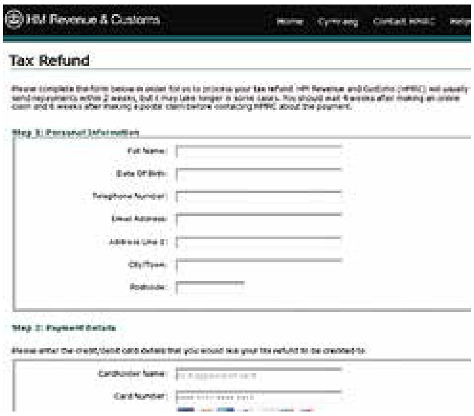
Thank you for my coupon

Get a Free £75 WAITROSE Coupon to celebrate 112th Anniversary!

One person (1). Claim now!

WWW.WAITROSECOUPONS.SITE

Image: http://www.thatsnonsense.com



Tax Refund

Please complete the form below in order for us to process your tax refund. HM Revenue and Customs (HMRC) will usually send repayments within 2 weeks, but it may take longer in some cases. You should wait 4 weeks after making an online claim and 6 weeks after making a postal claim before contacting HMRC about the payment.

Step 1: Personal Information

Full Name:

Date Of Birth:

Telephone Number:

Email Address:

Address Line 1:

City/Town:

Postcode:

Step 2: Payment Details

Please enter the credit/debit card details that you would like your tax refund to be credited to.

Cardholder Name:

Card Number:

In fact, there are 'phishing kits' available to buy on the dark web. They vary in price, typically ranging from $5 to $100 and use banks' and government brands. These products are very similar to the genuine sites they mimic, making it very difficult for a member of the public to spot the difference.

Phishing is a particularly effective tool in collecting data and one of the most well-used methods. The Microsoft Security Intelligence Report 2017[7] stated that phishing was the biggest threat to Office 365 products, with more than 75% of phishing emails consisting of a link to a site encouraging the victim to enter their personal data.

Image: Active Cyber Defence – One year on, Dr Ian Levy, February 2018: https://www.ncsc.gov.uk/information/active-cyber-defence-one-year, p10

[6] *A New Era in Phishing – Games, Social, and Prizes, Or Katz, May 2018: https://blogs.akamai.com/2018/05/phishing-in-the-wild-a-new-threat-research-paper.html*

[7] *Microsoft Security Intelligence Report, Volume 23 https://info.microsoft.com/rs/157-GQE-382/images/EN-AU-CNTNT-eBook-Security-GDPR-Microsoft-SIR-Volume-23%5B1%5D.pdf*

GLOSSARY

‘Fullz’ – Financial information that includes the full information of the victim, including name, address, credit card information, National Insurance number, date of birth, and more.

‘Dumps’ – Raw information on a debit or credit card’s magnetic strip; can be obtained in a variety of ways, including the physical skimming of the credit card, capturing the data through a point-of-sale device that has been infected with malware, or hacking into a retailer’s internal network.

URL – Stands for Uniform Resource Locator; it is an address that identifies a particular file on the Internet.

CVV – Three-digit number on the back of a debit or credit card.

API – Stands for Application Programming Interface.

Dark web – A collection of websites which exist on an encrypted network, such as The Onion Router (Tor) and Invisible Internet Project (I2P).

The Onion Router (Tor) – An encrypted network which uses ‘onion routing’ to provide encrypted and anonymous network traffic.

Invisible Internet Project (I2P) – An encrypted network which uses ‘garlic routing’ to provide encrypted and anonymous network traffic.

Phishing – The attempt to obtain personal information by posing as a trustworthy source through the use of deceptive emails or websites.

APPENDIX 1

Methodology

The demographics of the sample sent to Forensic Pathways were as follows:

- 14% were female, 21% were male and 65% did not have a gender provided.
- 1% were under 21, 16% were between 21 and 30 years old 21% were aged between 31 and 40 years old, 22% aged between 41 and 50 years old, 21% between 51 and 60 years old and 20% were aged 61+.
- Additionally, as well as name and date of birth, 39% had no telephone number nor email, 34% had only a telephone number, 25% had both email and telephone number and 1% only had an email.
- Only 1% had a bank account listed with them.

Forensic Pathways used these details to identify additional insightful information available online around these individuals. They split the data into four groups:

- Those who had a name, date of birth, neither email or telephone number.
- Those who had name, date of birth, telephone number, no email.
- Those who had a name, date of birth, no telephone number.
- Those who had name, date of birth and both telephone number and email.

A 250-record size random sample from each group was taken and a bulk social media search was performed and each result was manually checked against the victim's personal information to establish the quality of the results. The results of the search were as follows:

Combination of available data	Count of Cifas records	Hit rate	Confidence level
Name, date of birth, neither telephone nor email	32.038	15%	30%
Name, date of birth, only telephone	28,035	22%	90%
Name, date of birth, only email	834	n/a	n/a
Name, date of birth, neither telephone nor email	20,563	35%	90%

Based on these findings Forensic Pathways took a uniform random sample of 30,000 individuals: 15,000 individuals who had name, date of birth, telephone number and no email; and 15,000 from those with name, date of birth, and both telephone number and email address. These combinations were selected due to the high level of confidence associated with that individual being a match.

To conduct the dark web search, Forensic Pathways carried out searches using the account details and the term 'Fullz' (a reference term used to sell packages of personal information). Another search was then carried out using the postcode associated to the victim and search results were then manually examined. Finally, a search using email addresses associated with the victim was carried out, with the resulting search hits being manually examined to ascertain whether the details belonged to the victim information provided by Cifas.

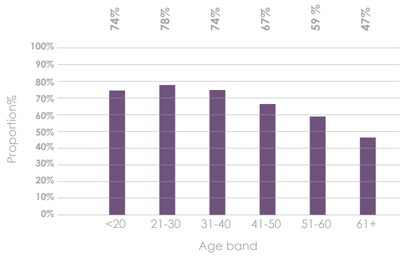
To identify 'Fullz' profiles available on surface web, Forensic Pathways opted to use generic search query terms and not use specific individual information from within the database of victims of impersonation provided by Cifas. Forensic Pathways used terms such as 'Fullz' and 'Fullz UK' to identify unique profiles which were freely available on surface web. A screenshot of each 'Fullz' profile was taken and documented along with the website that the 'Fullz' was located on.

To identify whether an individual's email account has been compromised, the email was entered onto the search engine for haveibeenpwned.com. This is a site which has been developed by Troy Hunt, a regional director for Microsoft and the author of security courses for web developers on Pluralsight. The site is a free resource for members of the public who want to check if their email account has been compromised. It aggregates email addresses from breaches which have been shared with the site. Although it may not capture every data breach, it does hold data on 5,043,777,890 breached accounts.

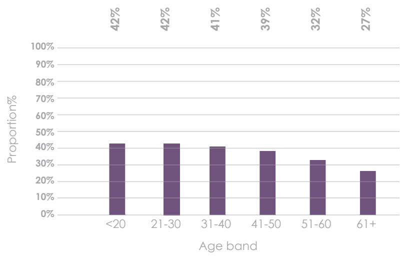
APPENDIX 2

Distribution of age groups and social media sites

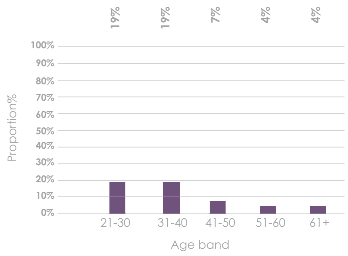
Proportions of those on Facebook by age band



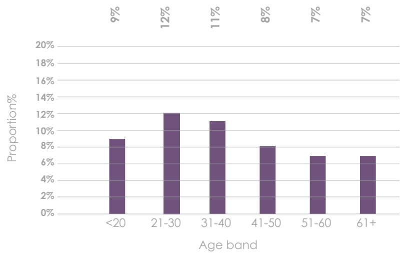
Proportions of those on Linkedin by age band



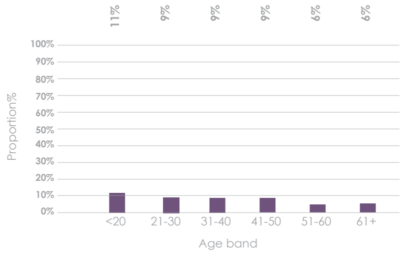
Proportions of those on Hi5 by age band



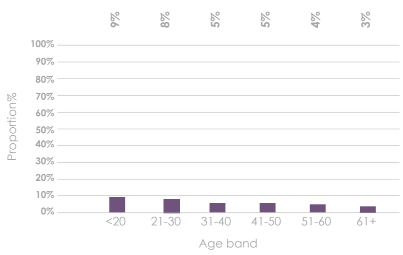
Proportions of those on Pinterest by age band



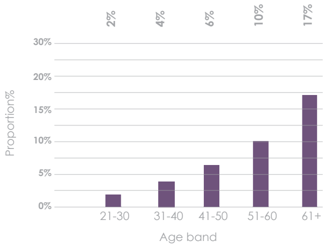
Proportions of those on Google+ by age band



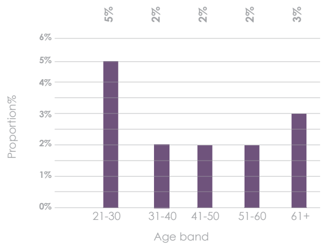
Proportions of those on Indeed by age band



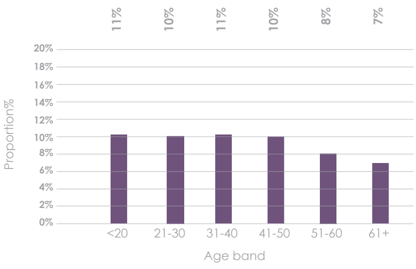
Proportion of those on Whitepages by age band



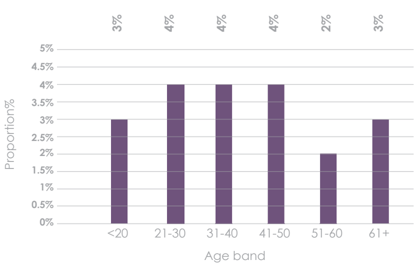
Proportions of those on Netlog by age band



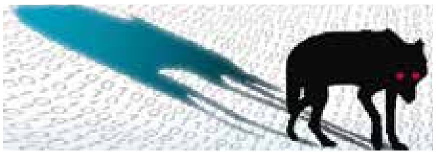
Proportions of those on Twitter by age band



Proportions of those on WAYN by age band



COMPANY INFORMATION

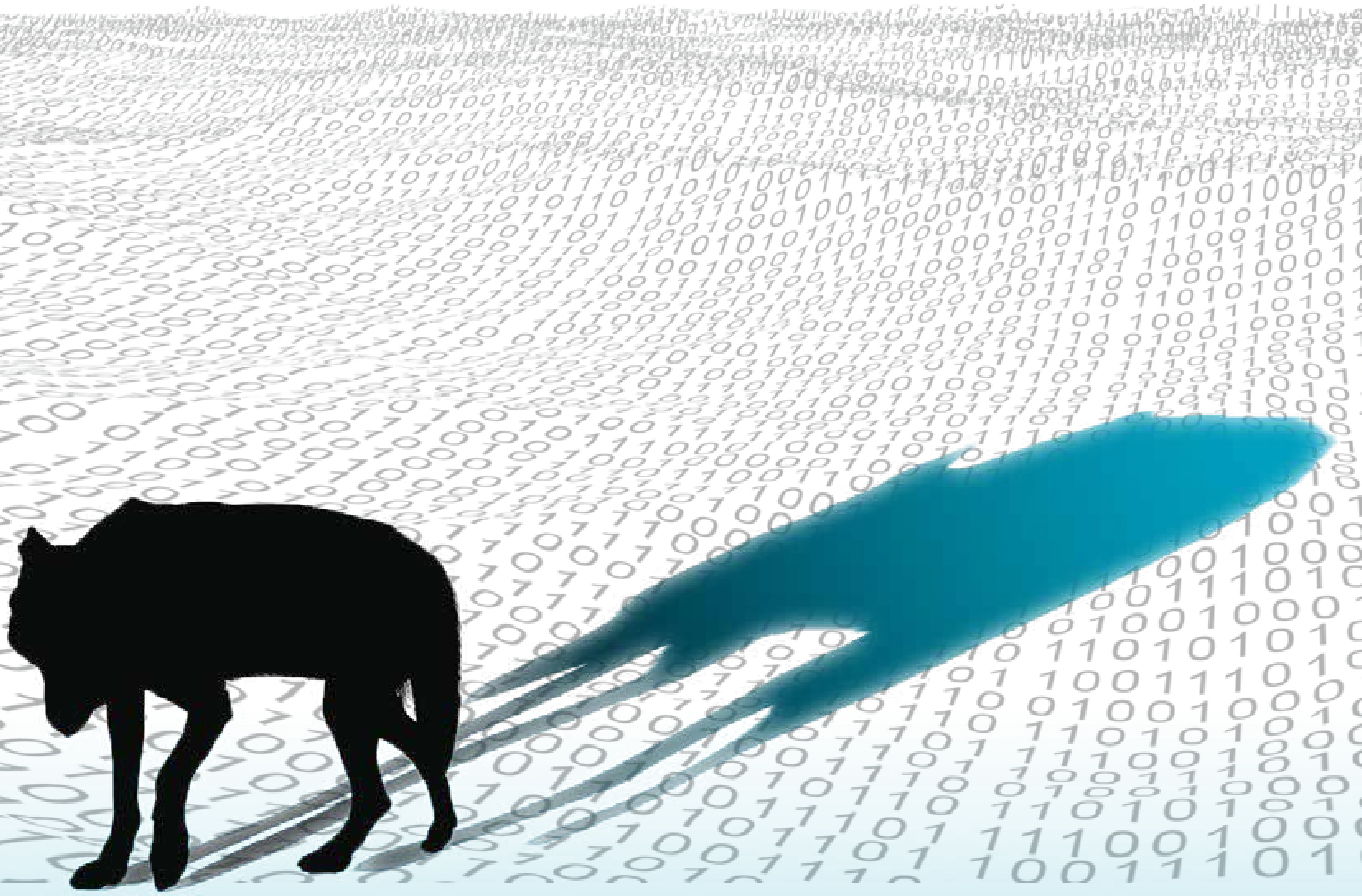


Cifas is a not-for-profit organisation, managing the UK's largest database of fraudulent conduct, known as the National Fraud Database. Currently over 400 members file cases onto the database and details are shared across the membership to help prevent and detect fraudulent activity. Since 1988, Cifas has collaborated with organisations from across the public and private sectors to create a non-competitive fraud prevention environment, focused on working with rather than against each other to defeat fraudsters. Our methods utilise a number of products and services including fraud databases and networking opportunities for our members and law enforcement partners. Cifas works alongside the Home Office led Joint Fraud Taskforce, and has recently produced fraud education lesson plans in association with the PSHE Association. Cifas also provides the Secretariat for the All Party Parliamentary Group on Fraud and Scamming.

Forensic Pathways is an internationally recognised organisation operating at the forefront of Digital Forensics. Forensic Pathways works with forensic professionals, government agencies and private organisations in the global cyber security and digital evidence industry, providing a range of services including digital forensic investigation, dark web investigation, cyber security services, and Due Diligence services. They have received a number of awards, including the Corporate Vision, 2018 UK Best in Business Innovation Award for Digital Forensics and the Orange National Business Awards – Best Use of Technology in Business. Forensic Pathways has also been appointed 'Export Champion' by the UK Government's Department for International Trade and is a signatory to the United Nations Global Compact on Corporate Social Responsibility. They have worked with leading law enforcement agencies, academia and corporate clients.

WWW.CIFAS.ORG UK

WWW.FORENSIC-PATHWAYS.COM



Leaders in fraud prevention