COVID-19 AND CRIME SURVEY PART I: SURVEY OVERVIEW AND ONLINE SECURITY BEHAVIOUR

UCL

DAWES CENTRE
FOR FUTURE CRIME

NEIGHBOURHOOD WATCH

COVID-19 and crime survey Part I: Survey Overview and Online Security Behaviour

Overview

This research is funded by UK Research and Innovation and is a collaboration between the Dawes Centre for Future Crime at UCL and Neighbourhood Watch. The aim of the research is to understand how the COVID19 pandemic has affected crime in the UK, and the public's perception of it. Data were collected between the 2nd and 23rd of December 2020. The survey had an amazing turnout with 20,784 total respondents across the country. Of those who participated, 14,741 (or 71%) provided answers to every question.

The pandemic has disrupted everyday life in many ways, some of which could increase the risk of crime, some of which could decrease it. The survey was thus designed to assess changes to people's activities, as well as their perceptions and experience of crime for the periods before and during the pandemic. The survey contained questions on the following general themes:

Routine activities: We asked if and how people's daily activities changed during the pandemic so that we could see if changes were associated with changes in crime risk or perceptions of it.

Online habits and online safety: We asked about people's day-to-day online security behaviour, ownership of internet connected devices and their use of the Dark web. These questions were asked so that we could see if people's online routine activities correlate with their risk of online crime. We also asked questions to assess awareness of two government initiatives intended to help keep consumers safe online

Victimisation and perceptions of crime: We asked participants about their experience and perceptions of crime for the 12 months before the pandemic and for the first lockdown period (23 March 2020 - 4th July 2020). With respect to victimisation, we were particularly interested in online crime such as fraud and computer misuse. For perceptions of crime, we asked about a much wider set of offences.

Handling of the pandemic: We asked about people's trust in the police and their handling of the pandemic, the Government's clarity of message, and any decisions that may have made respondents angry. We also asked about the social acceptability of various scenarios in relation to policing that might be implemented to keep communities safe during lockdown. These questions were asked to assess levels of satisfaction with law enforcement and governance during the pandemic, which can help improve policies now and also in the future.

DNA tests, Covid-19 certificates and vaccines: We asked about respondent's awareness of and demand for these health-related goods and services as these may be targeted in scams or may be counterfeited.

Demographics and Social media use: Finally, we asked demographic questions – so that we could understand the characteristics of respondents – and questions about social media use. The latter focused on social media engagement with respect to crime prevention and law enforcement so that we could understand which platforms respondents engage with to find out about crime or how to reduce their risk of it.

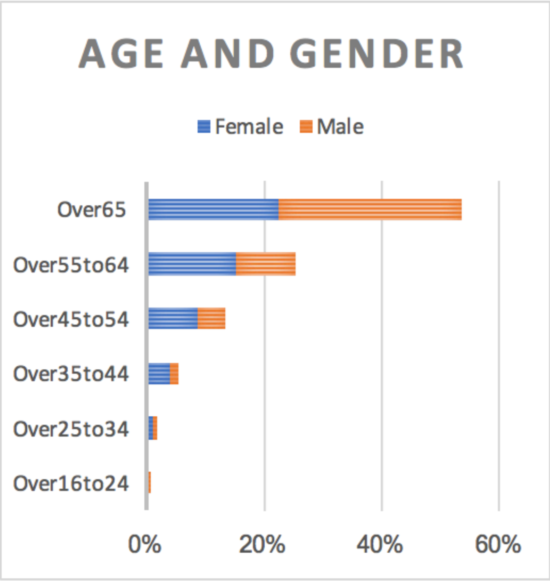
In this briefing, we describe the overall characteristics of those who completed the survey and discuss some of the findings. In particular, we focus on respondent's awareness of two crime prevention campaigns and provide a little detail about them for those that are not aware of them. Subsequent briefings will cover topics to include perceptions of crime, victimisation experience and the handling of the pandemic.

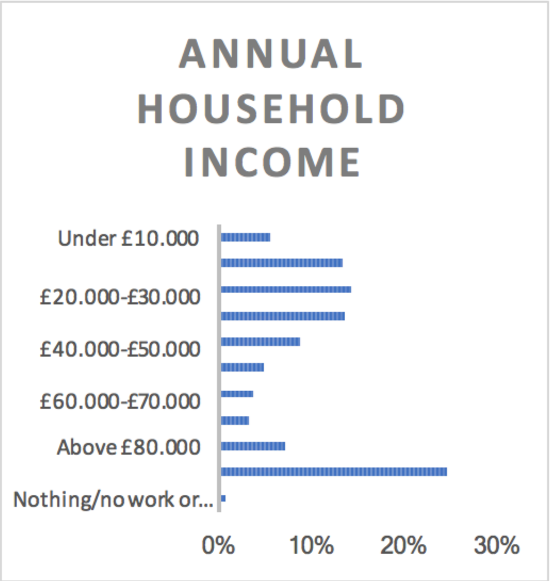
Demographics

We start with a description of the characteristics of those who completed the survey in full as this provides important context for the findings discussed in this briefing and those that will follow.

- As shown below, slightly more than half of all respondents (53%) were over 65 years old and around half were Female (52%).

- The figure below also shows the household income of respondents. For comparison, the UK median income is £29,900.





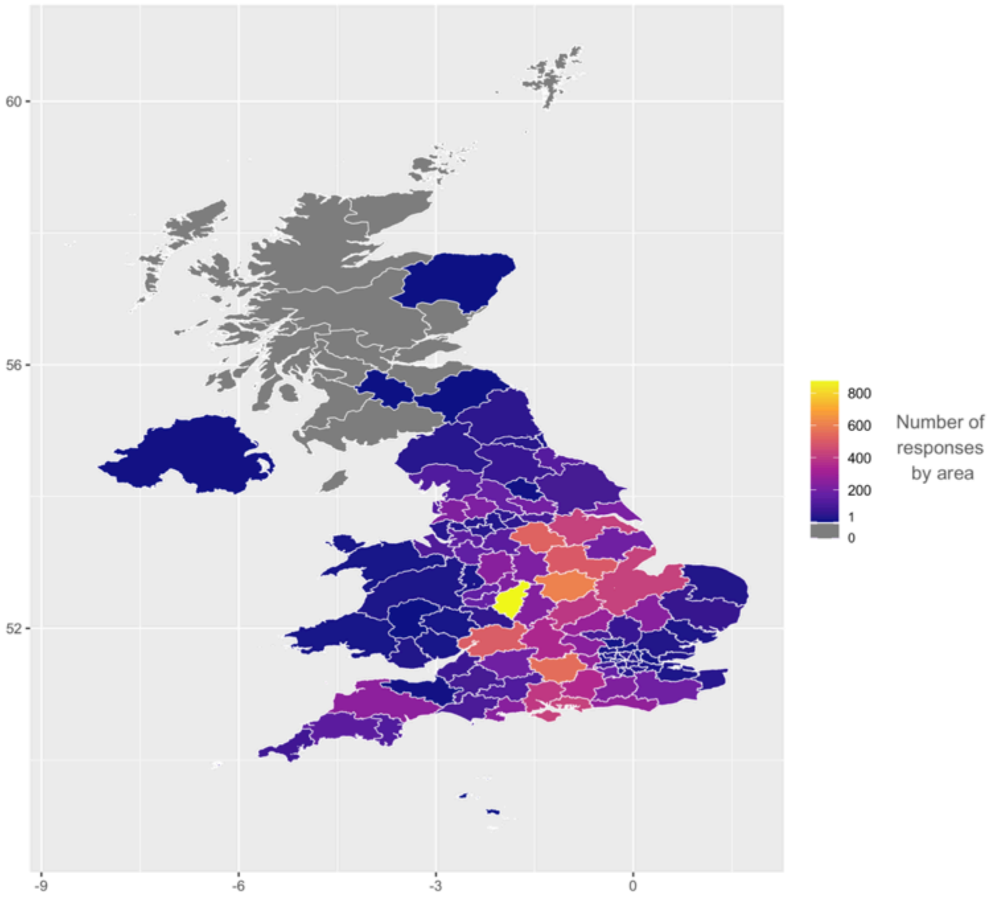
•In terms of geographic representation, the map above shows the frequency of responses for UK postcode areas (there are just over 120 of these in the UK). The largest numbers of responses came from the South East (23%), East Midlands (17%), West Midlands (16%), South West (13%), North West (12%), North East (6%).

•More than half of the respondents reported that they lived in a Village/Town (67%), while 37% reported living in a Suburb, and only 3% in a city centre.

•A slight majority of respondents were retired (59%), and 18% were in full-time employment.

•The majority of respondents reported living in a 2-adult household (61%), while just under 12% live with children.

•Most of the respondents (74%) use social media. The most prominent social media used among the sample is Facebook (88%), followed by Instagram and Twitter, with around 30% of respondents using these latter two platforms.

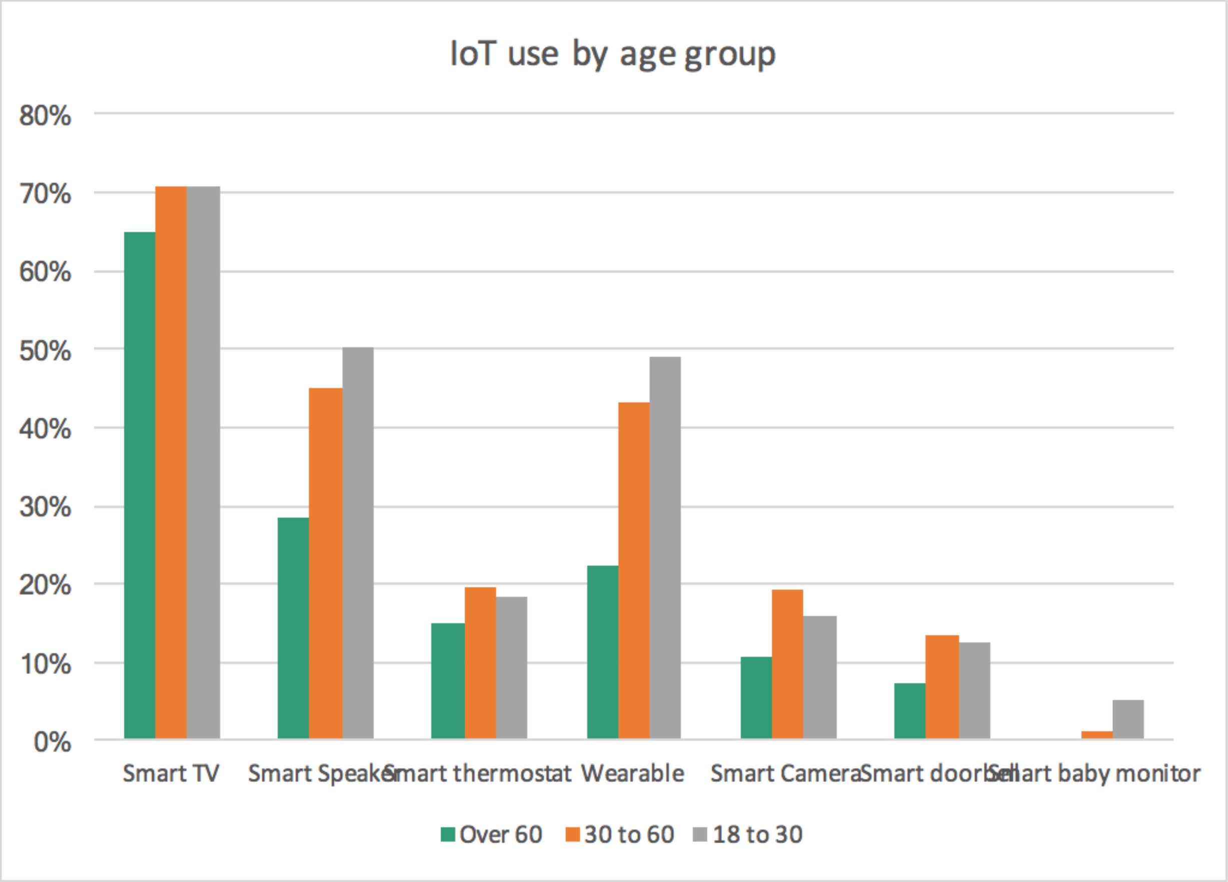


Neighbourhood watch membership

- •58% of respondents reported living in a Neighbourhood Watch area, while 42 % either did not live in a NW area or did not know whether they did or not.
- •Of the respondents who live in a Neighbourhood Watch area, more than half (64%) identified as members of Neighbourhood Watch.
- •Overall, 38% of the total number of respondents identified as members of Neighbourhood Watch.

Ownership of Internet Connected Devices

Almost all respondents (99%) reported using at least one Internet connected device. Such devices are collectively referred to as the Internet of Things (IoT). For a discussion of the security of IoT devices, see https://www.ucl.ac.uk/jill-dando-institute/research/dawes-centre-future-crime/policy-briefs/policy-brief-how-secure-consumer-iot. As shown in the figure below, most respondents reported using a Smart TV, Smart Speaker or a Wearable device (e.g., a smartwatch). Ownership varied across some age groups for some devices (e.g., wearables and smart speakers) but very little for others (e.g. Smart TVs, smart thermostats).



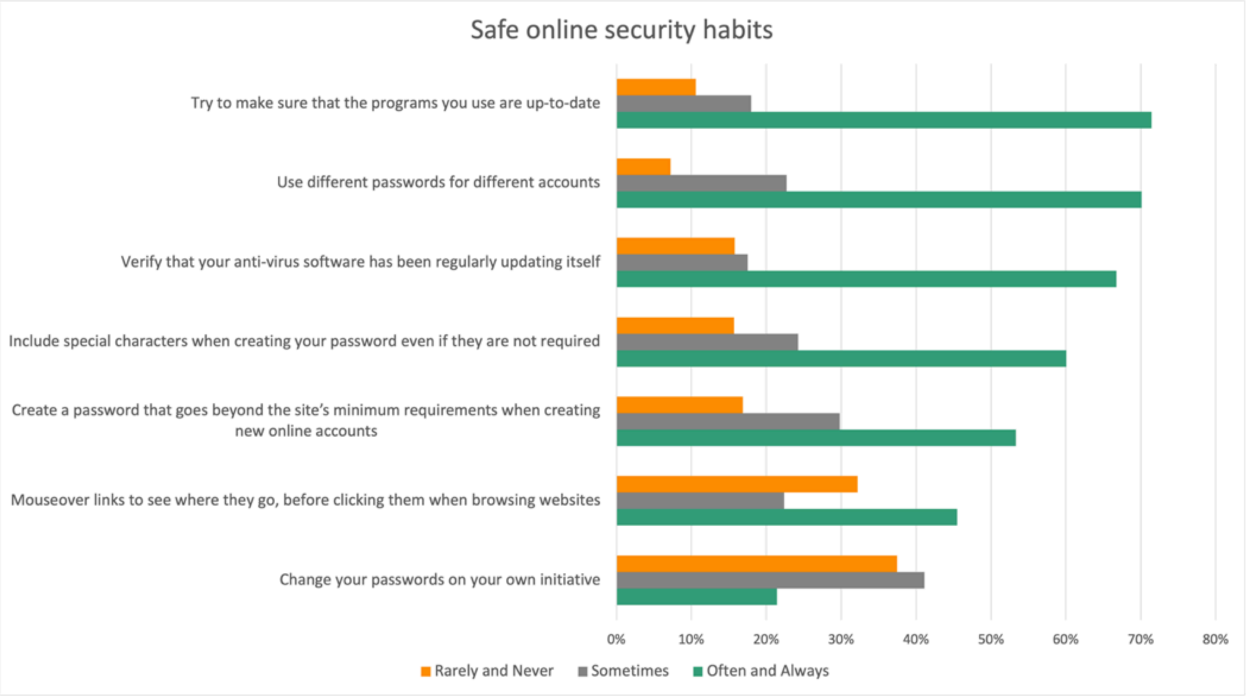
Online habits and online safety and trust

In this section we present findings regarding respondent's online security and safety habits.

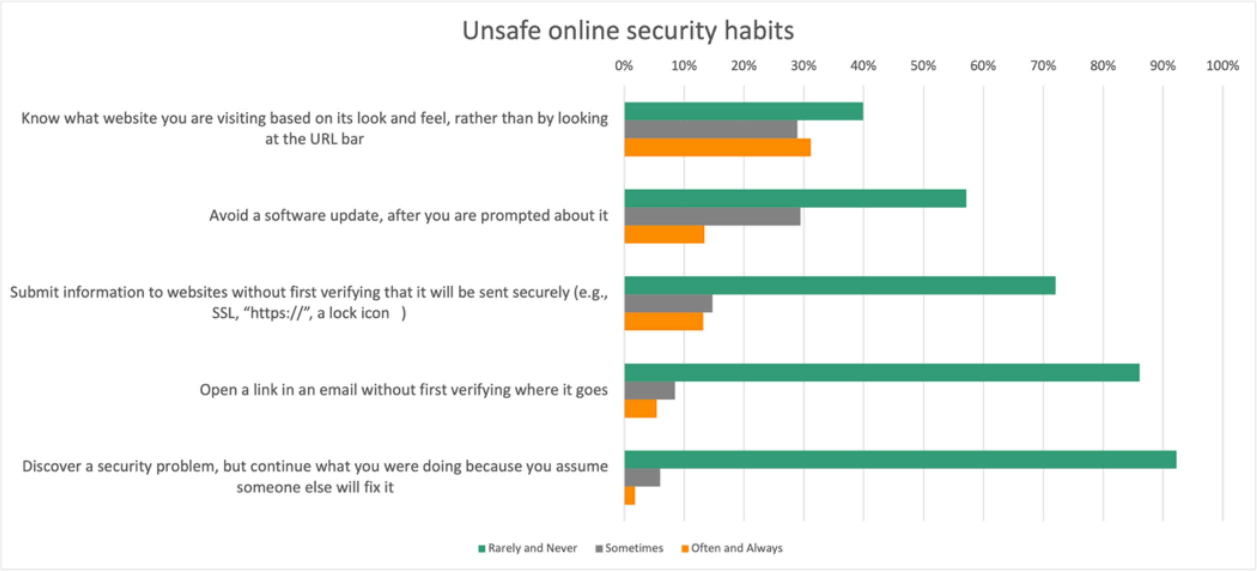
Online security habits

We first asked respondents 12 questions – developed by security researchers – regarding their daily online habits. We asked how often they perform positive online security actions (such as changing their passwords on their own initiative) and how often they engage in negative ones (e.g. ignoring a discovered security problem on their device).

The figure below shows the findings for "safe" security practices. Overall, respondents generally report practicing safe online security habits, but not everyone did. Moreover, there is variability across the different types of behaviour. For example, while 70% reported using different passwords for different accounts "often or always", less than half (46%) reported always moving their "mouse over links" before clicking on them. Regarding the creation of passwords, it can be seen that about 60% of respondents routinely use techniques to improve the quality of passwords (e.g., improving password strength by including special characters even if they are not required). However, only 21% report that they change their password on their own initiative.



With respect to unsafe online security habits, the results were varied. For example, most respondents reported that they established what website they were visiting based on its look or feel rather than by looking at the URL bar (around 60% answered that they do this sometimes, often or always). Websites can be "spoofed" so this can be dangerous. Just over 40% reported that they avoided a software update after being prompted about it sometimes, often or always. On the other hand, few respondents reported that they opened email links without verifying where this would take them first, and few reported ignoring identified security issues.



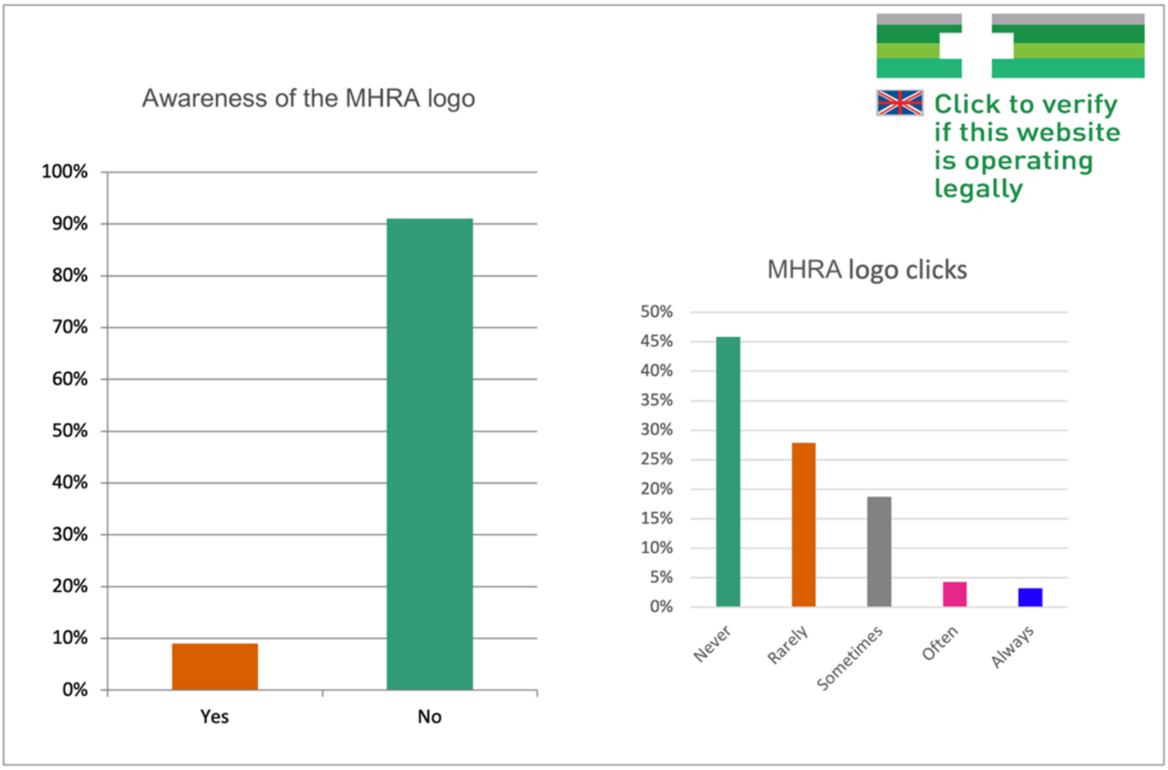
The Dark web is part of the World Wide Web that is only accessible by means of special software, such as "the Onion router" – often referred to as ToR (see, http://bbc.in/3ewsGOV). The technology used allows users and website operators to remain anonymous or untraceable. The dark web was originally developed by the US Naval Research Laboratory and has many legitimate uses. For example, the BBC has recently launched a mirror website on the darkweb to enable people to access it in countries where the content might otherwise be censored (see, http://bbc.in/3bGIpcu). However, entering the Dark web can be unsafe, as many criminals frequent and trade in illegal goods in this environment. We asked respondents whether they use ToR (the Onion router) to access the Dark web. Most reported that they do not (80%), 17% were not aware of the Dark web, and only 3% reported that they had used it.

Online Security Training

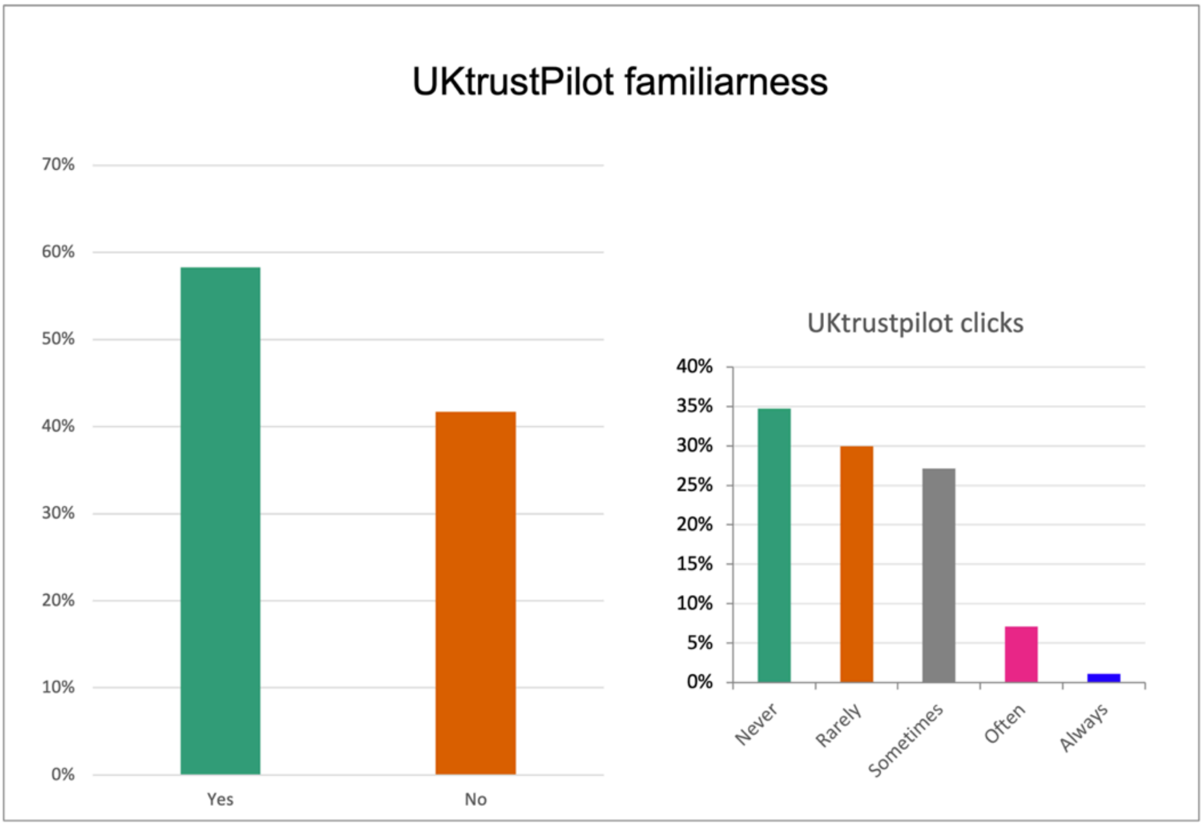
When asked about training, most respondents reported that they had not completed online security training (73%). However, we also asked respondents if they were aware of the National Cyber Security Centre's "*Cyber Aware*" guidance about keeping safe online. More than half of the respondents (55%) were aware of it. For those not aware of this, the National Cybersecurity Centre, which is the UK's independent authority on cybersecurity, provides information for individuals (and businesses) about how to keep safe online and we would recommend visiting the website (which can be found here: https://www.ncsc.gov.uk/cyberaware/home).

Online safety awareness

To keep people safe online, there are a number of other services and government run schemes. As falsified and unauthorised medicines and unapproved devices have become increasingly widespread during the pandemic, we asked respondents if they were aware of the EU logo used (in the UK) by the Medicines and Healthcare products Regulatory Agency (MHRA) as a verification badge for all certified online suppliers of medicines. The MHRA is sponsored by the UK Department of Health and is the executive agency responsible for regulating all medicines, devices and blood components for transfusion in the UK. Prior to Brexit, it was a legal requirement for legitimate online sellers of medicines to display this logo. As the figure below shows, 90% of respondents were not aware of this logo, and the majority of those who were reported that they never or rarely clicked on it (more than 70%). This is concerning given the potential risk of purchasing falsified or unauthorised medicines online.



As a comparison, we also asked respondents whether they were aware of *UK Trustpilot*. Trustpilot is a consumer review website where consumers can leave reviews for products, services and companies. Its aim is to help consumers shop with confidence and to help companies improve their business. With nearly 1 million reviews posted each month, the website provides a way for the public to check if other websites are likely to be legitimate. As shown in the figure below, awareness of this website was much higher. When asked how often respondents search Trustpilot, most rarely or never did so (64%). One reason for this may be that many websites post their Trustpilot ratings as a badge on their home page. However, relying on this information may be unsafe, as anyone can fake such a badge. Without clicking on it, users cannot know whether the badge itself is legitimate (clicking a legitimate badge should lead to the company/service official UK Trustpilot page). Regardless, awareness of UK Trustpilot was relatively high.

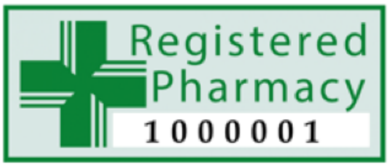


In addition to examining awareness for the whole sample, we examined whether this varied according to age, gender, whether respondents identified as members of neighbourhood watch, or whether their self-reported online security habits were below average. We do not present the statistical analysis here, but the findings suggest that members of neighbourhood watch were slightly (and statistically significantly) more likely to be aware of the online pharmacy logo and the Cyber Aware campaign (after we account for differences in age, gender and online security habits). They were no more likely to be aware of UK Trustpilot. Respondents who reported having below average online security habits were less likely to be familiar with the pharmacy logo, the Cyber Aware campaign or UK Trustpilot. Interestingly, younger respondents tended to be less aware of the Cyber Aware campaign, but more aware of the pharmacy logo and UK Trustpilot. Female respondents were more aware of the pharmacy logo but there were no gender differences for the Cyber Aware campaign or UK Trustpilot.

Conclusion

Use of social media and Internet connected devices is now an integral part of people's everyday lives, and 99% of our respondents reported owning an internet connected device (not including a desktop or laptop). The need for healthy online security habits and online safety awareness is especially pronounced in disruptive times, such as the Covid19 pandemic, as criminals might exploit the situation. Most respondents to the survey reported adopting safe online habits, but the picture was far from perfect. As such, we would encourage the community to practice the safe online habits discussed above on their own initiative as much as possible, and to avoid the unsafe online behaviours highlighted above. Furthermore, we would encourage readers to complete online security training and to follow the advice provided by the NCSC as part of their Cyber Aware campaign, and to keep up to date with changes to this.

Similarly, it would be wise to check the authenticity of online pharmacies (and other traders). Unfortunately, since 1 January 2021, Great Britain based online sellers are no longer required to display the EU Distance Sellers Logo (the logo remains in place in Northern Ireland). However, all pharmacies in the UK, including those providing internet services, must be registered with the UK General Pharmaceutical Council (GPhC). The GPhC operates a voluntary internet pharmacy logo scheme which is unaffected by Brexit and its purpose is to provide reassurance to customers who are purchasing medicines online that the pharmacy in question complies with GPhC standards. The logo is shown below and we would recommend consumers look for this (and click on it to check the registration), particularly if they are using an online pharmacy for the first time.



The GPhC logo

In addition, a recent campaign by the MHRC provides advice to help consumers avoid purchasing fake medical products when shopping online. For more information please visit: https://fakemeds.campaign.gov.uk/.

About the authors

This research was conducted by Dr. Manja Nikolovska and Prof. Shane Johnson at the Dawes Centre for Future Crime at UCL in collaboration with Neighbourhood Watch.

Acknowledgements

We would like to thank everyone who participated in this survey, your time is much appreciated. This research was funded by the Economic and Social Research Council sponsored research under the UK Research and Innovation open call on COVID-19 under grant ES/V00445X/1.

Contact Us: This research is funded by UK Research and Innovation and is a collaboration between the Dawes Centre for Future Crime at UCL and Neighbourhood Watch. For further information please contact Dr. Manja Nikolovska at m.nikolovska@ucl.ac.uk.

UCL
DAWES CENTRE
FOR FUTURE CRIME

UKRI
Economic
and Social
Research Council

NEIGHBOURHOOD
WATCH