In Search of Day 2 and Day 8 Tests: a personal account

Yi Ting Chua
24 May 2021

Executive summary

CCC COVID Briefing Papers are an ongoing series of short-form, open access reports aimed at academics, policymakers, and practitioners, which aim to provide an accessible summary of our ongoing research into the effects which the coronavirus pandemic (and government responses) are having on cybercrime.

This report is a personal account of purchasing the COVID-19 testing mandated for international travel. The author encountered a number of features which raise questions about opportunities for fraud within the current testing requirements.

Researching COVID test provider websites

The current guidelines for international travellers to the UK require a COVID-19 test on or before day two and on or after day eight of quarantine, with the day of arrival as day zero. These tests need to be booked prior to travel as the booking reference number is required on the passenger locator form. However, the websites of suggested test providers contain a number of concerning errors in design which could pose potential opportunities for scammers.

The government web page provides information on region (for in-person tests), prices, telephone number and a contact email address, alongside a direct link to the providers’ websites. There are 234 providers on the list, of which 151 offer tests nationwide. I examined the listed providers to compare aspects such as pricing, the complexity of return procedure for samples, and accreditation. However, this process soon proved to be frustrating for a number of reasons:

Registration. A small number of test providers do not allow direct access to the information I needed. Some require registration to access their websites at all, while others require visitors to fill out inquiry forms. This raises several issues. First, there is the matter of accessibility – of particular importance for a service mandated by government. Second, this approach continues to perpetuate the norm of exchanging personal information for service access. Last but not least, mandated registration is a technique commonly used by phishing websites [2].

Format and layout. The format and layout of the providers’ websites varied widely. It ranges from standardised and professional design, to websites that look like they were created in a rush. According to ‘Which?’, one tip for spotting fraudulent websites is for consumers to browse through the website and:
Watch out for poor English, such as spelling and grammar mistakes, or phrases that don’t sound quite right. It could mean the site isn’t genuine and was put together by someone abroad looking to make a quick profit.

Some websites failed this heuristic, despite being government-approved suppliers. For example, on the Frequently Asked Questions page of one provider (see Figure 1), I found inconsistencies in the format of the content, as well as minor grammatical errors.

Images and logo. To show legitimacy, the most common sign is an image or logo stating approval by the government. However the cost of this signal is low and it can be easily copied by scammers. As a consumer, I encountered different types of logos.

In addition, test providers are required to be accredited. For most websites, this information is on display along with contact information. For a few, I failed to locate an accreditation and had to refer to an external organisation, the United Kingdom Accreditation Service, to re-confirm.

Trust signals, legitimacy, and phishing

I observed clear issues with trust signalling which create vulnerabilities for phishing. Even criminals rely on signals to determine the trustworthiness of actors in highly uncertain underground markets. These signals have associated costs which lead to different interpretations by actors in the market [1]. For example, for online marketplaces, positive comments may be seen as a weaker signal compared to length of operation for a seller since it is relatively easy to generate positive comments.

Phishing websites set up to trick victims would use similar signals to achieve legitimacy. In an analysis of websites for work-at-home scams, Turner and colleagues found shared features such as registration, some form of participation fees and mentions of legitimate companies [2]. ‘Which?’ also advise consumers to pay attention to the domain name, website content (for spelling or grammatical errors), the returns policy and the padlock sign [3]. Issues with these features and trust signals on some of the test providers’ websites are concerning as finding these problems on legitimate websites undermines consumers’ ability to spot fakes.

Conclusions

As guidelines ease within the United Kingdom for international travel, the demand for mandated testing kits is likely to increase. Such increasing demand for a novel product can be easily exploited by scammers, given the lack of standards for the test providers’ websites and the relatively low cost of trust signals. This is alarming since detailed personal information (including passport information) are required when making appointments. We suggest that the government set minimum standards for the websites of firms whose use it not only promotes but mandates.


At the Cambridge Cybercrime Centre we make our research data available to other academics, sometimes before we have looked at it ourselves! Researchers can be provided access to our ‘CrimeBB’ dataset of (26 and counting) underground cybercrime forums, our extensive collections of chat channel data, and our new collections of forums relating to online right-wing extremism and radicalisation. We can also share email spam and sensor data related to DDoS and IoT malware. All these collections are regularly updated and can be rapidly provided under licence – for full details see: https://cambridgecybercrime.uk

The full set of CCC COVID Briefing Papers can be found at: https://cambridgecybercrime.uk/COVID
This work is licensed under CC BY 4.0. To view a copy of this licence visit: https://creativecommons.org/licenses/by/4.0