JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2020, 1–8
doi: 10.1093/cybsec/tyaa019
Research Paper

Research Paper

What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?

Tommy van Steen ,[1,*] Emma Norris,[2] Kirsty Atha[3] and Adam Joinson[4]

[1]Institute of Security and Global Affairs, Leiden University, The Hague, The Netherlands, [2]Department of Health Sciences, Brunel University London, London, UK, [3]Centre for Behaviour Change, University College London, London, UK and [4]School of Management, University of Bath, Bath, UK

*Correspondence address. Institute of Security and Global Affairs, Leiden University, The Netherlands, Turfmarkt 99 Room 4.03, 2511 DP The Hague, The Netherlands. Tel: +31 (0) 70 800 9965; E-mail: t.van.steen@fgga.leidenuniv.nl

Received 28 June 2019; revised 31 January 2020; accepted 14 October 2020

Abstract

With the surge in cyber incidents in recent years, many linked to human error, governments are quite naturally developing security campaigns to improve citizens' security behaviour. However, it remains not only unclear how successful these campaigns are in changing behaviour, but also what established behaviour change techniques—if any—they employ in order to achieve this goal. To investigate this, we analysed 17 government-sponsored cybersecurity campaign materials. We coded the materials for their intervention functions according to the Behaviour Change Wheel and their behaviour change techniques in accordance with the Behavioural Change Technique Taxonomy (version 1). Our findings show that security campaigns are often focused on education and increasing awareness, under the assumption that as long as citizens are aware of the risk, and are provided with information on how to improve their security behaviour, behaviour will change. Additionally, there is a lack of published effectiveness studies investigating the direct effects of a governmental cybersecurity campaign. Proposed improvements to security campaigns are discussed.

Key words: awareness campaigns; behaviour change; cyber-security

Introduction

Consumers (and citizens) are common victims of cybercrimes. A recent study by the Center for Strategic and International Studies [1] estimated the annual global cost of cybercrime to be $600bn, approximately 1% of global GDP. The FBI division tasked with cybercrime (IC3) estimated that US citizens paid in excess of $1bn per annum on ransomware alone, and that currently cybercrime reporting covers only around 10–12% of the actual cybercrime committed [2]. The most recent statistics from the UK's Office for National Statistics estimated that citizens of England and Wales were victims of 4.5 million cybercrimes in the year ending March 2018. Of these, the majority (3.2m) were fraud-related, with the remaining (1.2 m) victims of computer-misuse (e.g. hacking). While rates of victimization through computer viruses have fallen [3]—mostly due to the increase in use and capabilities of anti-virus solutions—cybercrime remains the most likely crime to be suffered by UK citizens [4], with an estimated £4.6bn stolen from UK citizens alone [5].

Amongst national governments, there is a recognition that creating a secure digital environment requires not only technical solutions but also for responsibility to be taken by both businesses and citizens. For instance, the UK Governments' National Cybersecurity Strategy 2016–2021 [6] notes that, 'we lack the

skills and knowledge to meet our cybersecurity needs …. The public is also insufficiently cyber aware' [6]. The National Cyber Strategy published in 2018 by the US Whitehouse similarly notes a priority as being to, 'improve awareness and transparency of cybersecurity practises to build market demand for more secure products and services' [7].

As a response, many governments run cybersecurity awareness and skills campaigns with the goal of improving citizens' cybersecurity hygiene, awareness and skills, often at considerable cost. For instance, the UK Government's 'cyber aware' campaign was reported as costing £12m, equalling over £6 per website visitor [8]. The Canadian Centre for Cyber Security, formed in 2018, has a budget of over 500m CAD over 5 years, and increasing public understanding (via the 'Get Cyber Safe') as a large part of its remit [9]. It therefore is reasonable to ask if these kinds of campaigns use the best evidence-based approaches to behaviour change, and if they are effective in changing citizens' awareness or behaviour in such a way as to increase their protective behaviour or reduce risk-taking in terms of cybersecurity. More specifically, we wonder if the preponderance of terms such as 'aware' and 'awareness month' in reviewing public cybersecurity campaigns suggests a focus on raising awareness as the prime behaviour change mechanism.

Traditionally, governmental campaigns to influence citizens' behaviour are based on the assumption that making people aware of a risk will lead them to act to counter that risk. In the past, this has taken the form of fear-based messages, sometimes accompanied by additional information to remove the threat (e.g. around smoking cessation; e.g. see [10]), sometimes not [e.g. early AIDS awareness campaigns; see [11]. In keeping with findings from other domains, awareness campaigns alone are not enough to change cybersecurity behaviour [12], and there have been recent calls to expand awareness campaigns, so that they are aimed at *changing* security behaviour [13, 14]. Indeed, there is research in this area that shows that mainstream behavioural change components such as self-efficacy [15, 16] or applying the health belief model [17] can positively influence cybersecurity behaviour. Increasingly the focus of intervention studies in the field of cybersecurity has moved towards *skills* rather than simply *awareness* or *fear messages* [14]. For instance, a recent study of over 2000 people across five EU countries [18] found that messages focused on coping strategies were more effective than threat appeals in encouraging more secure behaviour. The goal of the present research is to explore the techniques used in cybersecurity campaigns in order to investigate if this research and extortions towards best practice have influenced the design of governmental cybersecurity campaigns. In order to do this, we adopt and apply a standardized taxonomy of behaviour change techniques. In recent years, there has been a move towards standardization of behavioural change techniques so that interventions can be more easily coded for techniques, their quality assessed and future interventions developed. One of these taxonomies, the Behaviour Change Technique Taxonomy version 1 (BCTTv1), identified 93 different techniques to change behaviour [19]. Included techniques range from basic (instruction on how to perform the behaviour) to more complex concepts such as self-affirmation, cognitive dissonance and 'comparative imagining of future outcomes'. As cybersecurity is a wide area (campaigns we surveyed included behaviours ranging from cyberbullying to fraud prevention alongside the usual password guidance), and as governmental campaigns are designed to reach all layers of society, we would hope that governmental cybersecurity campaigns would incorporate a wide range of behavioural change techniques to maximize their effectiveness. In this study, we investigate if this is the case. More specifically, to investigate current campaigns we surveyed 17 ongoing campaigns and collected evidence on: (i) the goal of governmental cybersecurity campaigns; (ii) The extent to which these campaigns use evidence-based behavioural change concepts; and (iii) If there was evidence on the effectiveness of these campaigns presented publicly.

Methods

Search strategy

To obtain the relevant materials, we searched the web (using the Google Search Engine) for government-sponsored cybersecurity campaigns. We define government-sponsored cybersecurity campaigns as any (temporary or ongoing) initiative that aimed to improve cybersecurity in end-users through means of mass communication or the creation of toolkits that could be used by more local entities to influence smaller communities. Campaigns were included if they were (partly) in English, the campaign materials were suitable for the (general) public, and came from either government departments or wider agencies such as the European Union Agency for Network and Information Security (ENISA). An initial search was conducted in January 2017, followed by additional searches conducted in October 2018 and December 2019 as in recent years, more organizations are developing their own awareness campaigns. This way, the campaigns from these organizations could be included in our analysis and rudimentary comparisons across years become possible. Websites that introduced cybersecurity awareness month and then linked to existing campaigns were excluded (but the source campaign was included). This led to 17 campaigns being identified for coding (Table 1).

Information extraction

We recorded the following information for each of the campaigns: country of origin, governmental department or organization, website content, other available content, and whether or not effectiveness studies had been published. If possible, materials were downloaded, otherwise screenshots were used to store the relevant materials.

Campaign coding

First, the extracted information was formalized, and the campaign materials were coded for type of content (e.g. website, videos, text and posters). These materials were then coded for behaviour change content. Content was coded by reviewing all website pages, as well as embedded videos and attachments provided. First, materials were coded for their intervention functions according to the Behaviour Change Wheel [20]. This framework posits nine intervention functions as super-ordinate approaches to behaviour change: education, persuasion, incentivization, coercion, training, enablement, modelling, environmental restructuring and restrictions. To identify the more fine-grained 'active ingredients' of the identified campaigns, materials were also coded for their presence of Behaviour Change Techniques, using the Behaviour Change Techniques Taxonomy version 1 (BCTTv) [19]. BCTTv1 provides terms and definitions for 93 different behaviour change techniques, clustered into 16 different groups [19]. For example, Group 1 'Goals and planning' consists of nine behaviour change techniques such as 'Goal setting (behaviour)' (BCT 1.1) and 'Action planning' (BCT 1.4). Presence of an intervention function and BCT was coded for each given campaign if it was present at least once in any material. Up to three examples of identified intervention functions and BCTs were recorded for each campaign. Coding of intervention functions and behaviour change

Table 1: Overview of government-led cybersecurity awareness campaigns

Campaign name	Country	Organization	Top-level URL	Target group	Website content	Additional materials	Type of materials	Intervention coded
Connect Smart	New Zealand	Government	www.connectsmart.govt.nz	General public and organizations	Information	No	N/A	No
Cert NZ	New Zealand	Government	www.cert.govt.nz	General Public	Information	Yes	Campaign stationary	Yes
CPNI Security Awareness Campaigns	UK	Centre for the Protection of National Infrastructure	www.cpni.gov.uk	Organizations	Information	Yes	Campaign stationary, videos, information sheets	Yes
Cyber Aware	UK	Government	http://cyberaware.com	General Public	Information	Yes	Campaign stationary	Yes
Cyber Security Hun South Africa	South Africa	Government	www.cybersecurityhub.gov.za	General Public	Information	Yes	Campaign stationary	Yes
Cyber Security Information Portal	Hong Kong	Government	www.cybersecurity.hk	General Public	Information	Yes	Campaign stationary	Yes
Cyber Security Malta	Malta	Government	http://cybersecurity.gov.mt	General Public	Information	Yes	Videos	Yes
Cyber Streetwise	UK	Government	http://cyberstreetwise.com	N/A	N/A	N/A	N/A	No
Cyber Tips 4 You	Singapore	Government	www.csa.gov.sg	General Public	Information, real-world examples, videos	Yes	Campaign stationary, videos, information sheets	Yes
European Cyber Security (CyberSec Month)	European Union	ENISA	http://cybersecuritymonth.eu	General Public	Information, real-world examples, videos and interactive tests	Yes	Campaign stationary	Yes
Data Privacy Day	USA	National Cyber Security Alliance	https://staysafeonline.org/data-privacy-day/	General Public	Information	Yes	Campaign stationary	Yes
Get Cyber Safe	Canada	Government	www.getcybersafe.gc.ca	General Public	Information, videos	Yes	Campaign stationary	Yes
Get Safe Online	UK	Government-sponsored public/private partnership	www.getsafeonline.org	General Public	Information, videos	Yes	Videos, chatbot	Yes
Information Security Awareness	Canada	Government	www.gov.bc.ca	General Public	Information	Yes	Campaign stationary, information sheets	Yes
National Cyber Security Awareness Month (NCSAM, 2012–2014)	USA	Government	http://niccs.us-cert.gov	General Public	Information	Yes	Campaign stationary	Yes
NICCS	USA	Government	http://niccs.us-cert.gov	General Public	Information	Yes	Campaign stationary, trivia game	Yes
Quarterly Cybersecurity Awareness Campaigns	USA	Department of Energy	www.energy.gov	General Public	Information	Yes	Campaign stationary	Yes
Stay Smart Online	Australia	Government	www.staysmartonline.gov.au	General Public	Information	Yes	Campaign stationary	Yes
Stop.Think.Connect	USA	Government	www.stopthinkconnect.org	General Public	Information, real-world examples, videos	Yes	Campaign stationary, videos, information sheets	Yes

techniques was independently performed by two reviewers who are experts in behaviour change coding (E.N., K.A.), with discrepancies resolved through discussion. Identified intervention functions and behaviour change techniques were then collated at campaign level. Inter-rater reliability of which intervention functions and BCTs were present in each campaign was calculated using Prevalence-Adjusted and Bias-Adjusted Kappa (PABAK) [21]. PABAK is used for judgements with 2 raters against 3/+ nominal categories and has been used in previous research coding behaviour change content [22, 23]. Results were interpreted using Altman's guidelines: ≤0.20 poor, 0.21–0.40 fair, 0.41–0.60 moderate, 0.61–0.80 good and 0.81–1.00 very good reliability [24].

Results

The web search identified 19 governmental cybersecurity campaigns from across the world. Campaign materials were accessible for 17 of these campaigns. All of these campaigns ran a website where people can find information about cybersecurity, with some adding real-world examples or videos. The available materials were limited in diversity. While some provided videos or information sheets that could be shared, most focused solely on what we call 'campaign stationary'. Campaign stationary includes posters, leaflets, bookmarks, postcards, etc. that, in many cases, are either variations on a theme or merely the same message or image in a different format. While these materials are helpful as reminders (e.g. a poster that can be put on display in a community centre, postcards that can be sent to relatives, or Facebook 'badges' that can be added to profile pictures for increased exposure), they often do not contain a complete behavioural change attempt. For an overview of the campaigns and types of materials, see Table 1.

The coding of the materials for intervention function showed that all 17 campaigns contained content to educate people, such as advising readers to regularly change their passwords (e.g. Data Privacy Day campaign). Most campaigns (9/17) featured persuasion, such as imagery of hackers to induce negative feelings (e.g. Cyber Security Information Portal, Fig. 1).

Many campaigns (6/17) featured training content with specific, structured guidance on improving their cybersecurity, such as giving instructions on how to use specialized file deletion software (e.g. Information Security Awareness). Fewer campaigns included coercion (2/12) and modelling (1/12) intervention functions. Four of the nine intervention functions posited by the Behaviour Change Wheel were not found in identified campaigns; none of the campaigns attempted to incentivize security behaviour, and no campaign tried to enable people to become more cyber secure beyond education or training, i.e. by increasing means or reducing barriers. Given the distance between government and the end-user, it is unsurprising that no campaigns attempted to restrict end-users or to restructure the environment.

A range of different behaviour change techniques (in total, 13) were present in the campaigns, ranging from zero to seven identified techniques per campaign. Most campaigns (15/17) included 'instruction on how to perform the behaviour' (BCT 4.1), such as the provision of checklists for staying safe online (e.g. Cyber Safe 4 You; Get Cyber Safe,Figure 2) and 'information about social and emotional consequences' (14/17; BCT 5.3), such as giving details on potential personal and company-level financial loss at not maintaining cybersecurity (e.g. Get Cyber Safe). Some campaigns included practical social support (4/17; BCT 3.2) such as encouraging parents to work with their children to install safe Internet usage (e.g. NCSAM Campaign; 2012–14), recommendations and guidance from a 'credible source' (4/17; BCT 9.1) on how to adopt cybersafe behaviours (e.g Quarterly Cybersecurity Campaigns) and 'imaginary punishment' (4/17; BCT 16:1), such as videos depicting scenarios where fictional individuals get hacked while using insecure Wi-Fi (e.g. Stop Think Connect). For an overview of the coded intervention functions and behaviour change techniques per campaign, see Table 2.

Inter-rater reliability was assessed to be very good (0.81–1.00) for 4/5 identified intervention functions and 9/13 identified behaviour change techniques, good (0.61–0.80) for 3/13 identified behaviour change techniques, moderate (0.41–0.60) for 1/13 behaviour change techniques and fair (0.21–0.40) for 1/5 identified intervention functions (Table 2). Effectiveness measurements were found in the public sphere for only two campaigns, the 2017 National Cyber

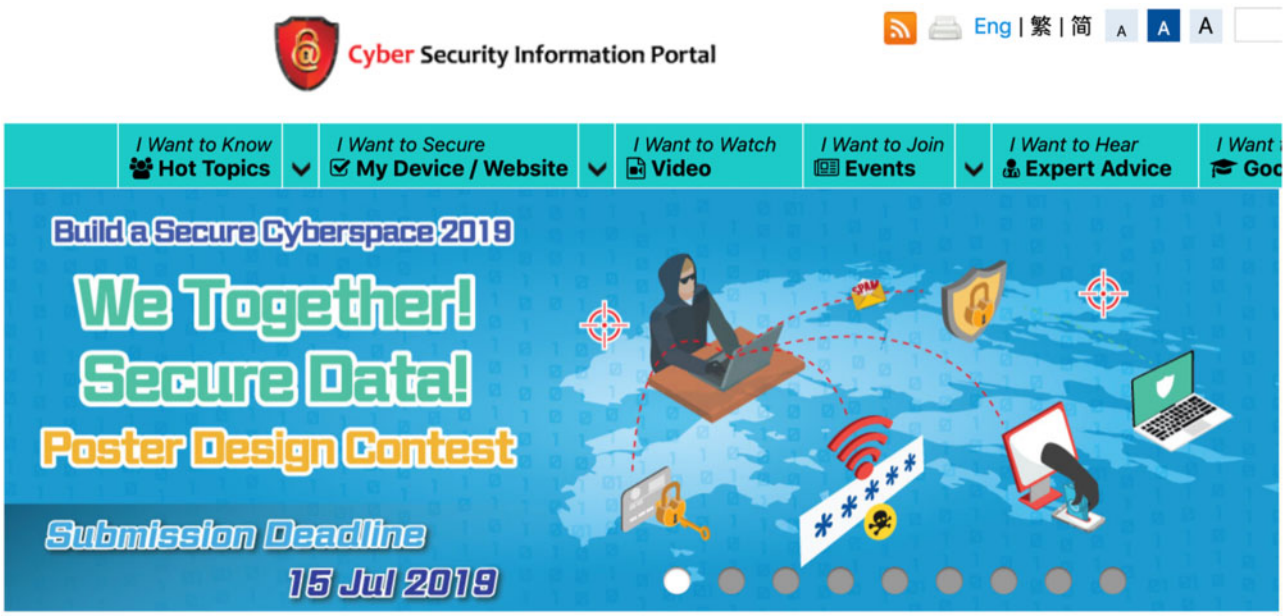

Figure 1: Landing page, CSIP (Hong Kong), accessed in 2018.

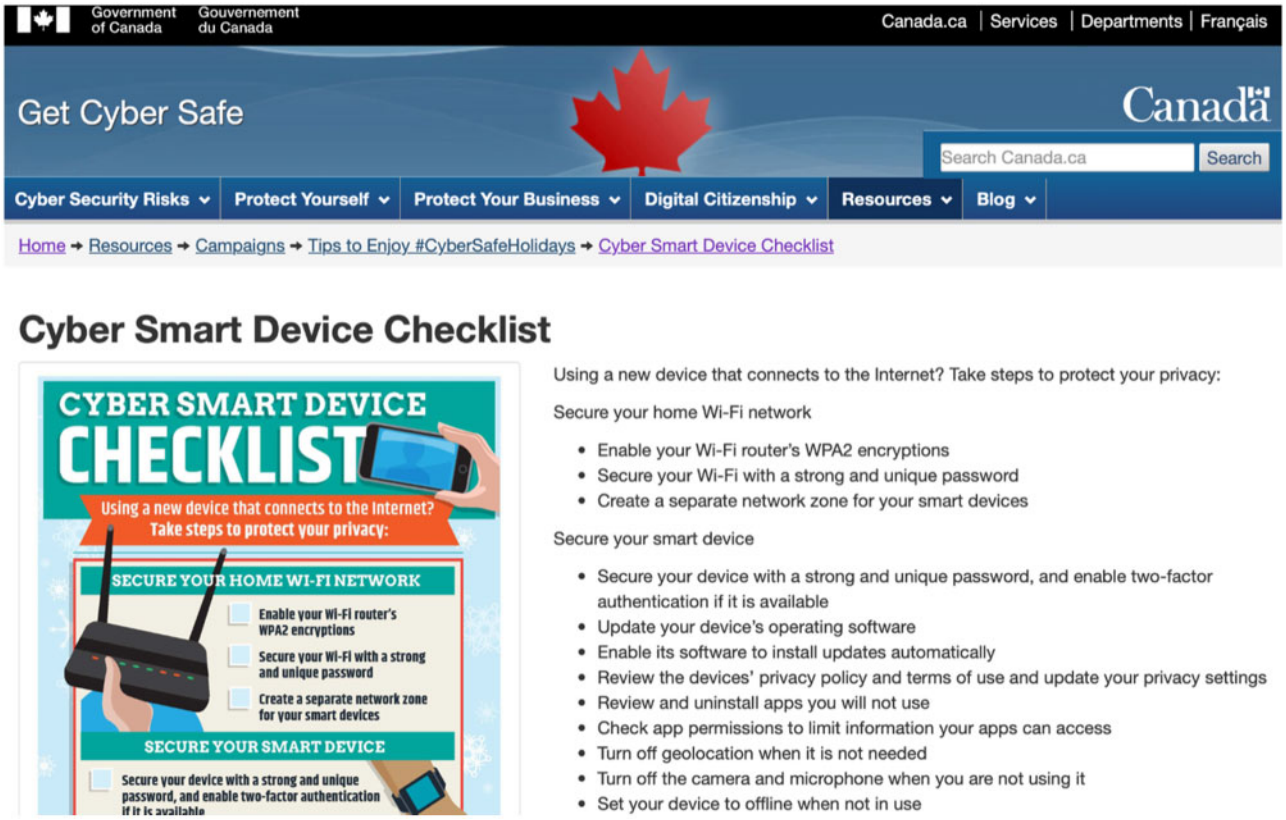

Figure 2: Get cyber safe (Canada) smart device checklist, accessed in 2017.

Security Awareness Month and the Data Privacy Day initiative, both in the USA. This measurement consisted of qualitative and quantitative results relating to various factors such as the reach of the campaign, the number of visitors to various websites and the number of (corporate) partnerships. No measurements relating to (objective) security behaviours were published.

Discussion

The contents of these identified cybersecurity campaigns suggest that their goal is mainly to increase awareness, with some explicitly stating so (e.g. the NICCS campaign and other NCSAM initiatives). This raises the question of why increasing awareness is an important goal to strive for. Traditionally, awareness campaigns have the larger goal of changing behaviour through increased awareness [25], even if they do not explicitly state so. By itself, raising awareness does not improve the security of end-users or society as a whole and for this to happen, end-users will need to change their behaviour so they put more safeguards in place that protect them from (cyber) harm and that improves their safety when they are online. If the stated goal is to increase awareness, while actually aiming to improve cybersecurity of end-users, merely attempting to raise awareness will not be effective. There is no evidence that merely increasing awareness leads to behavioural change. There are various other factors that need to be taken into account if the goal is to change behaviour, as mapped by the intervention functions in the Behavioural Change Wheel. This means that governments that aim to improve cybersecurity need to move beyond awareness campaigns and start incorporating behavioural change theories in their efforts.

Another factor that suggests that the awareness campaigns might not be sufficient in changing cybersecurity behaviour is that there seems to be no substantive change between the campaigns in our most recent searches compared to earlier searches. The number of behavioural change techniques and intervention functions used in more recent campaigns mirrors those of the older ones, and the same holds true for the actual list of techniques and intervention functions found in the newer campaigns. This suggests that awareness campaigns generally follow the same structure and focus on similar methods of improving awareness.

When the goal is to improve people's cybersecurity behaviour, a starting point would be to upgrade the awareness campaigns so they focus on specific behaviours. For example, there are fundamental differences in the threats—and solutions—of romance scams and ransomware attacks. These different crimes require not only different methods to shield end-users from their potential harm, but also require the targeting of vastly different populations, with their own pitfalls when it comes to being persuaded by scammers to transfer money, or to click on a link that installs ransomware on their computer.

The analysed campaigns seem to target the general public, rather than focusing on specific populations within society that might be at a higher risk to become a victim of cybercrime. For example, campaigns that aim to prevent cyberbullying might be more applicable to school-age children, while campaigns addressing romance scams might be most effective when designed to target lonely people who are in need of social contact. The current awareness campaigns hardly differentiate between vulnerable groups and seem to adopt a 'one size fits all' in the manner in which they convey their awareness message. A similar approach is seen when looking at the range of cybercrimes they intend to prevent. The found intervention functions and behavioural change techniques seem to be applied to all

Table 2: Intervention Functions & Behaviour Change Techniques identified in included cybersecurity campaigns ($N = 17$)

Intervention functions identified using Behaviour Change Wheel	Cert NZ	CPNI Security Awareness Campaigns	Cyber Aware	Cyber Security Hub South Africa	Cyber Security Information Portal	Cyber Security Malta	Cyber Tips 4 You	Data Privacy Day	European Cyber Security Month	Get Cyber Safe	Get Safe Online	Information Security Awareness	NICCS	NCSAM Campaign (2012–14)	Quarterly Cybersecurity campaigns	Stay Smart Online	Stop Think Connect	Sum	PABAK
Educational	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	17	1.00
Persuasion		■	■		■					■		■		■	■	■	■	9	0.23
Training		■			■		■			■		■					■	6	0.90
Coercion		■																2	1.00
Modelling							■											1	0.83
Behaviour Change Techniques (BCTs) identified using Behaviour Change Techniques Taxonomy v1 (BCTTv1)																			
Action planning (1.4)	■																	2	0.67
Self-monitoring of behaviour (2.3)																	■	1	0.83
Social support (unspecified) (3.1)				■													■	2	0.83
Social support (practical) (3.2)		■						■		■				■				4	0.83
Instruction on how to perform the behaviour (4.1)	■	■		■	■	■	■	■		■	■	■	■	■	■	■	■	15	1.00
Information about social and emotional consequences (5.3)		■	■	■	■	■	■			■	■	■	■	■	■	■	■	14	0.90
Anticipated regret (5.5)					■									■			■	3	0.50
Demonstration of the behaviour (6.1)					■													1	0.83
Prompts / cues (7.1)		■																1	0.83
Credible source (9.1)						■							■	■	■			4	0.67
Restructuring the physical environment (12.1)					■												■	2	1.00
Adding objects to the environment (12.5)		■																1	0.83
Imaginary punishment (16.1)		■			■		■										■	4	0.67

cybercrimes in similar manners, rather than adopting tailor-made solutions for each different type of cybercrime.

Not only are the campaigns generic in their assumption that increasing awareness results in a meaningful change in behaviour, but the majority of campaigns relied on an assumption that awareness and fear of consequences lead to behaviour change, so long as it is outlined what the required behaviour is. This approach relies not only on the target audience being knowledgeable on how to change their behaviour in order to be more secure, but also on them understanding that action A (e.g. updating software) leads to outcome B (e.g. reducing threat of identity theft). While it is becoming accepted that awareness itself is not enough to lead to behaviour change [12, 14], there was less evidence that providing 'coping' skills (or information on the efficacy of relatively simple actions) had increased in response to recent research and guidelines [14, 18].

Moreover, the coding for behaviour change techniques shows that the campaigns we surveyed were limited in the range of behaviour change techniques they used in order to achieve a change in security behaviour. Only a small number of techniques were present in the campaigns, and as most campaigns focused on instructing people how to act, and explaining possible consequences of (in)secure cyber behaviour, they did not move particularly far beyond awareness-raising. As the analysis showed, education was the only intervention function present in all campaigns. Persuasion was used in half of the campaigns, training was used occasionally, coercion and modelling were used rarely, and incentivisation, enablement, environmental restructuring and restrictions were completely absent in the campaigns. While not all intervention functions might lend themselves to successful online behaviour change interventions, this finding shows that there is much ground that can be covered by carefully planning, designing and executing new cybersecurity campaigns based on a wider range of intervention functions.

The seeming lack of publicly available evaluations of the success or otherwise of the campaigns we surveyed is not surprising. As the campaigns are treated as a way to increase awareness rather than the more complex goal of changing tangible behaviour, no clear key performance indicators are present, and presumably internal metrics focussed on the number of site visits, or perhaps interactions with social media postings. It is possible that other, more complex metrics are shared internally, but no publicly available information was discovered that provided further insights into the effectiveness of these campaigns. Given the distance between governments and end-users, measuring the effectiveness of such large-scale cybersecurity campaigns beyond reach, the number of website visitors and the like would be difficult, but not impossible (particularly if designed during the planning stages of a campaign).

There are several recommendations to improve governmental cybersecurity campaigns. First, it is vital that any campaign seeking to improve citizens' security behaviour adopts a structured approach in which each aspect of the decision process to (not) behave securely is covered, and that seeks to incorporate as many different methods of influencing these decision processes as possible, in order to reach a wide audience. To achieve this, campaigns could be created that focus on specific cybersecurity behaviours and threats, rather than the wide-ranging awareness campaigns that are used now. These campaigns can then be more focused on specific target groups, incorporating messages that resonate more strongly with these populations, and also helps to decide on the best platforms to communicate those messages through.

Secondly, the existing knowledge on how to change security behaviours needs to be incorporated in these campaigns so that the chance of a campaign being successful is maximized. There is no one-sizefits-all approach in this, as different behavioural change techniques can target different aspects of cybersecurity behaviours, and it is dependent on the focus of the campaign which techniques should be incorporated. However, a mixture of techniques that cover the different intervention functions of the Behavioural Change Wheel seems a sensible starting point for cybersecurity behaviours that might not have been investigated thoroughly yet.

Thirdly, increasing awareness does not equal a change in behaviour. Therefore, the effectiveness of security campaigns needs to be assessed beyond awareness and reach metrics. Only by direct, behavioural measurements can the effectiveness of any security campaign be assessed. A recent ENISA report [14] reviewing evidence of effective behaviour change interventions to improve cybersecurity behaviours suggests that rather than focusing on improving threat perceptions, the focus should lie on coping appraisals. Persuading people of the effectiveness of specific behaviours to improve cybersecurity standards, and providing them with the tools and confidence to perform these behaviours is more likely to be an effective way of sustainable cybersecurity behaviours than the focus on the impact and likelihood of cyber threats.

As it might be difficult to reach the target group to measure their behaviour in response to the security campaigns, alternatives could be sought. For example, the campaigns could be distributed in small samples, controlling exposure to, and interaction with, the materials. Then, the direct effects of these campaigns on security behaviour can be tested. These effects should be tested on various levels so that in the case of an unsuccessful cybersecurity campaign, the effectiveness measures can provide insights as to why the campaign did not change actual behaviour. To ensure this, a combination of direct behavioural measures (e.g. number of people signing up for a training, or the percentage of people reporting a potential phishing email), intentions (e.g. questions on how an individual would act, if they find themselves in a potentially harmful situation), attitudes (e.g. attitudes towards the likelihood and severity of cyber threats such as ransomware) and awareness (e.g. reach of the campaign, whether people remember the message of the campaign materials) is needed. Combined, these tests can lead to an evidence-based approach to cybersecurity that incorporates various pathways to influence a diverse target group such as the general population. Additionally, rather than campaign stationary being used as reminders of campaigns, they could be designed so that they are standalone interventions that do not require additional knowledge, information or access to specific websites. This way, every part of the campaign that is distributed can independently add to the end goal of improved cybersecurity.

Funding

This work was supported by the Engineering and Physical Sciences Research Council (EP/P011454/1).

Conflict of interest statement. None declared.

References

1. The Center for Strategic and International Studies: Lewis J. *The Economic Impact of Cybercrime: No Slowing Down*. Santa Clara, CA, 2018.
2. Woolf J. The real reasons why cybercrimes may be vastly undercounted. Slate, 2018.
3. Muncaster P. UK cybercrime falls but stats are still shaky. Infosecurity Magazine, 2017.
4. Office for National Statistics. Crime in England and Wales: year ending March 2018. *Newport*, 2018.

5. Hern A. Cybercrime: £130bn stolen from consumers in 2017, report says. Guard, 2018.
6. HM Government. *National Cyber Security Strategy 2016-2021*, 2016.
7. *National Cyber Strategy of the United State of America*, Washington D.C., US, 2018.
8. Waterson J. Government's cybercrime website that costs £6.30 per visitor branded an 'expensive flop', Buzzfeed, 2017.
9. Gowling W. Canada hits 'refresh' on cyber in 2018 with the Canadian Centre for Cyber Security, Lexology, 2018.
10. Durkin S, Brennan E, Wakefield M. Mass media campaigns to promote smoking cessation among adults: an integrative review. *Tob Control* 2012;**21**:127–38.
11. Sherr L. An evaluation of the UK government health education campaign on AIDS. *Psychol Health* 1987;**1**:61–72.
12. Bada M, Sasse MA, Nurse JRC. Cyber security awareness campaigns: why do they fail to change behaviour?. *Proc Int Conf Cyber Secur Sustain Soc* 2015;118–31.
13. Ashenden D, Lawrence D. Can we sell security like soap? A new approach to behaviour change. *New Secur Paradig Work 2013* 2013;87–94.
14. ENISA. Cybersecurity culture guidelines: behavioural aspects of cybersecurity. *Athens*, 2019.
15. Rhee HS, Kim C, Ryu YU. Self-efficacy in information security: its influence on end users' information security practice behavior. *Comput Secur* 2009; **28**:816–26.
16. Kumaraguru P, Rhee Y, Acquisti A *et al.* Protecting people from phishing: the design and evaluation of an embedded training email system. *Proc ACM CHI 2007 Conf Hum Factors Comput Syst* 2007;**1**:905–914.
17. Ng BY, Kankanhalli A, Xu Y(C). Studying users' computer security behavior: a health belief perspective. *Decis Support Syst* 2009;**46**:815–25.
18. van Bavel R, Rodríguez-Priego N, Vila J *et al.* Using protection motivation theory in the design of nudges to improve online security behavior. *Int J Hum Comput Stud* 2019;**123**:29–39.
19. Michie S, Richardson M, Johnston M *et al.* The behavior change technique taxonomy (v1) of 93 hierarchically clustered techniques: building an international consensus for the reporting of behavior change interventions. *Ann Behav Med* 2013;**46**:81–95.
20. Michie S, van Stralen MM, West R. The behaviour change wheel: a new method for characterising and designing behaviour change interventions. *Implement Sci* 2011;**6**:42.
21. Byrt T, Bishop J, Carlin JB. Bias, prevalence and kappa. *J Clin Epidemiol* 1993;**46**:423–29.
22. Black N, Williams AJ, Javornik N *et al.* Enhancing behavior change technique coding methods: identifying behavioral targets and delivery styles in smoking cessation trials. *Ann Behav Med* 2019;**53**:583–91.
23. Wood CE, Hardeman W, Johnston M, *et al.* Reporting behaviour change interventions: do the behaviour change technique taxonomy v1, and training in its use, improve the quality of intervention descriptions?. *Implement Sci* 2016; **11**. doi:10.1186/s13012-016-0448-9.
24. Altman DG. *Practical Statistics for Medical Resarch*. London: Chapman & Hall, 1991.
25. Keating J, Meekers D, Adewuyi A. Assessing effects of a media campaign on HIV/AIDS awareness and prevention in Nigeria: results from the VISION Project. *BMC Public Health* 2006; **6**. doi:10.1186/1471-2458-6-123.