Online safety behaviours – background paper

Introduction

Research that we highlighted in paper 1 of this series clearly illustrates that the **motivation** of people who are not currently online is affected by their concerns about their online safety and privacy.

We know that there is **good practice and training available** for projects to develop the capability of Digital Champions to support people to stay safe online. We would like to understand why it appears from our joint work and focus groups that cybersecurity is still considered a significant issue within digital inclusion projects.

Why look at behaviours?

Observational project visits for One Digital have suggested that **people who are new to using the internet limit their usage and remain narrow users due to concerns about online safety**. In some instances it appears that this narrow usage is being actively supported by Digital Champions, perhaps because they themselves have concerns about how to stay safe online and/or because of their perceptions of the potential risks for those who lack competency and digital skills.

We know that security concerns demotivate those who are not currently online (see paper 1). There appears to **be little research that focuses on non-internet or narrow internet users' attitudes to internet privacy and security in detail**, a significant amount of work has been done to look at current attitudes and behaviours amongst those who are online. As the wider views of those who are online are likely to have an overall impact on non-user views of the internet it seems useful to better understand what this research tells us about people's attitudes to maintaining their security and privacy online.

We hope that along with the project questionnaire we have distributed, that this paper may also be useful in guiding digital skills projects in how best to support new learners to stay safe online.

The core of this paper is a review of some relevant research, specifically on behavioural insights into people's attitudes to staying safe online.

In conclusion the paper will consider any potential insights which may be useful in developing practice within digital inclusion projects.

Research review – key learning on online safety & behaviour

Understanding online safety behaviours:

- 75% of the UK public are at least fairly concerned about privacy and security of their personal data online, with 72% self-reporting they are confident to manage access to their personal data. There is a lack of independently assessed information on people's competency to stay safe online. A review of the 2019 Ofcom data is given below.

- People do try to protect their own personal privacy online, but there appears to be growing apathy about their ability to do so.
- There may be a ‘privacy paradox’ where the steps that people are likely to take to keep themselves secure do not match their level of concerns about online safety (with less action taken than might be suggested as being necessary to address concerns).
- There is no one behaviour that will keep people secure online but multiple interrelated behaviours (which tackle different risks), each of which can be influenced by different factors.
- The reasons why people are non-compliant with cyber security best practice is very complex (and well-illustrated in the table on page 5 below), and includes factors such as cost, risk assessment, and high levels of effort.
- People are influenced by environmental, social and personal factors. Creating an environment which values cyber secure behaviours could be critical.

What might help to improve people’s behaviours and attitudes to online safety?

- Mass communication campaigns with security messages and advice need to be fully integrated (at point of interaction), targeted and tailored. Delivering key safety messages at the point they are relevant, rather than a blanket approach.
- Ready-made and available security packages at low cost.
- Community programmes including Digital Champions supporting key messages to improve impact.
- Learned helplessness may arise from campaigns if people do not feel they can do anything to change. Designing-in security could be better practice and the tech sector and those designing services online should be encouraged to take this approach.
- Providing people with information on how to manage (cope) with online threats (practical information), was more likely to be effective than just highlighting the threat of unsafe cyber behaviour.
- A digital ‘nudge’ to more secure behaviour which is simple, and provides consistent, easy to follow information about how to deal with cyber-threats would be most successful.

If you are interested in more information about the research reviewed for this paper please see the ‘research review’ section below.

Conclusion: Practice implications

- Keep learning messages about how to stay safe online short and simple (as digital nudges). Research suggests that providing positive messages and easy solutions is the most effective way to provide support and advice.
- Encourage all Digital Champions to do online safety training so that they feel confident in their own skills. This training should be part of core training for Champions.

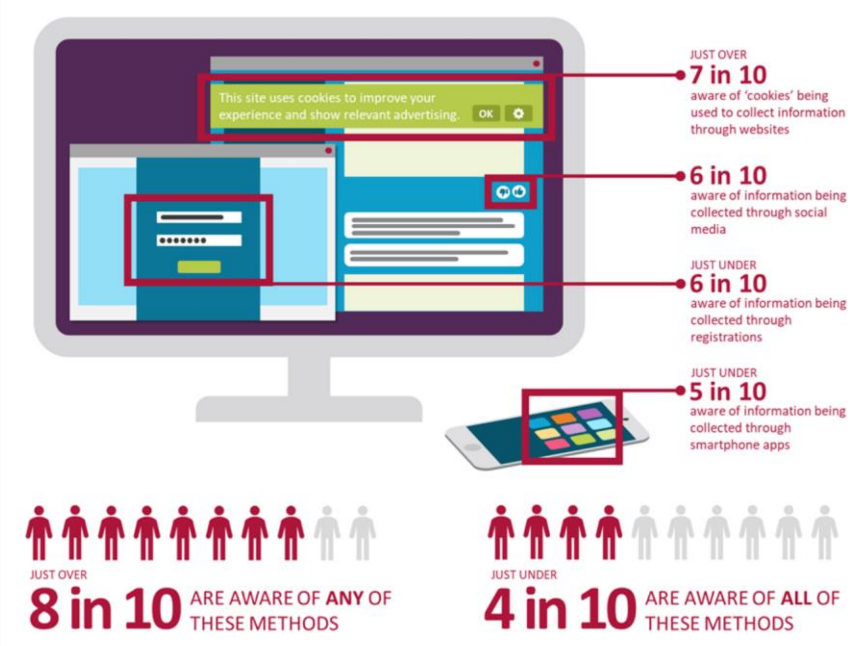
- Encourage Champions to use websites such as Get Safe Online.
- Train Digital Champions to be aware that people can feel overwhelmed by online safety concerns and help them to understand how this may limit their learners' use of the internet. Provide support so that they are able to work with learners to reduce the impact of these concerns.
- Encourage Champions and learners to consider online safety as each new digital skill is gained, providing necessary linked advice rather than overwhelming people.
- Look for cost effective (or maybe already integrated into the device) security software, and help people to set it up and understand how it is updated.
- Create a positive cyber secure culture within your project, with project leads showing good leadership skills around the importance of staying safe online.
- If your project is involved in developing a new digital service for customers ask the developers to build in online safety messages about usage into it (for instance a pop up about how to create secure passwords).

Research review

Online data privacy & safety

The latest Ofcom research Adults media use and attitudes (2019) includes a section on protecting personal data that gives a useful insight into people's understanding of one element of online safety: protecting personal information. They highlight that 'although most internet users are aware of at least one of the ways in which their personal data might be collected online, less than four in ten are aware of all the ways we asked about.' The diagram below illustrates this more detail. This research gives more insight into how competent people really are to keep themselves safe online.

Internet users' awareness of ways in which companies can collect personal information online


This site uses cookies to improve your experience and show relevant advertising.
OK
JUST OVER
7 in 10
aware of 'cookies' being used to collect information through websites
6 in 10
aware of information being collected through social media
JUST UNDER
6 in 10
aware of information being collected through registrations
JUST UNDER
5 in 10
aware of information being collected through smartphone apps
JUST OVER
8 in 10 ARE AWARE OF ANY OF THESE METHODS
JUST UNDER
4 in 10 ARE AWARE OF ALL OF THESE METHODS

An IPSOS Mori commissioned report for Carnegie UK Online Data Privacy from Attitudes to Action published in August 2018 asked three very relevant questions:

1. What do people think about online data privacy?
2. What actions do people take in relation to their online privacy?
3. What trade-offs are people willing to make relating to their data privacy?

The report highlighted the lack of consensus on definitions, interpretations and boundaries of online data privacy. What is clear from their review of over 50 pieces of literature from the previous three years was that concern around data privacy is significant. On average the reports showed 75% of the UK public are at least fairly concerned about the privacy and security of their personal data online.[1]

They report that 'despite concern, personal confidence in managing access to personal data online is also high, with similar proportions of the public (72%) suggesting they are either fairly or very confident.' They highlight that this is self-reported confidence and the genuine ability to do this was not investigated.

They reference that levels of apathy are rising with people's concerns about data privacy decreasing over time. The reasons for this have not been explored, and some speculate it may be linked to people becoming 'resigned to the inevitability of it'. Recent high profile data breaches may have a further impact on trends towards disempowerment.

Their findings suggest that the 'public do take precautions to keep their information safe in terms of employing a variety of privacy 'tactics', the most common being related to passwords and internet browsing security measures.' They suggest that there is a 'privacy paradox' which has not been explored in research in the UK (but has in the USA), which suggests that the steps that people take to keep themselves secure do not reflect the public's levels of concern. They consider the reasons why and suggest: 'people feel powerless given the amount of personal data now being collected; they lack awareness of the tools/techniques which would offer greater protection.' People also have low understanding and awareness of what the standards of 'good privacy protection' actually are.

The report considered whether any demographic factors provided indicators for behaviours of particular groups (including age). They could find no significant differences, although there is evidence of older and young people being both more, and less protective of their online privacy. There is a small amount of data suggesting that 'those at the lower end of the socioeconomic scale are more vulnerable to behaving in unsecure ways online'.

Insights into maintaining secure internet behaviour

A report by the Government Office for Science, Using behavioural insights to improve the public's use of cyber security best practices published in 2014 defines cyber security as 'the protection of globally connected electronic data or equipment

[1] The report highlights that estimates vary widely, and that lack of consistency on terms across the studies exists with key attitudinal questions.

against criminal, unauthorized or accidental use and the technology and processes required to achieve this protection'.

The report is keen to highlight that 'there is no single behaviour that will keep people secure online, but rather cyber-security requires multiple interrelated behaviours, and each one is potentially influenced by different factors. For instance what influences a user to use a strong password may not be the same as what influences a user to follow a phishing link.'

As with the Carnegie research, the authors pose very relevant questions on:

- What behaviours should people display to reduce their vulnerability to cyber-security attacks?
- Why do people not behave securely online?
- What can theories of behaviour tell us about how to effectively influence behaviour?
- What is the role of communication campaigns in changing behaviour?
- How can interventions be designed to motivate appropriate cyber-security behaviour?

They consider behaviour change theories and discuss the impact of environmental, social and personal factors in helping to better understand how people are influenced.

They present a useful perspective on **why people are non-compliant with cyber security best practice** as illustrated in the table below.

The priority is always being connected - it outweighs the risk of an insecure connection in a public place	People are habituated – they click to confirm acceptance of conditions without considering the consequences
Convenience wins over security	The desire to be connected wins over security
The financial cost is too high of security software	Security risks are ignored as concrete gain is greater than potential abstract risk
The effort required is too high – to remember multiple passwords, or use different tools to stay safe online	People do not perceive that their behaviours will benefit their security
People downplay the risks	People do not perceive the need to change – if they have not experienced negative consequences
People lack knowledge and skills – and are not able to keep constantly updating information	People simply forget to behave securely
Social etiquette leads people to share security information such as passwords	How susceptible you believe you are drives security behaviour
Attackers use threats and fears – with quick response times	People over-estimate their ability to understand and respond to security threats

People delegate security responsibility to others who they perceive as more knowledgeable	The link between security behaviours and the consequences (of not behaving securely) are not clear enough that people are incentivised to behave appropriately.

How people are influenced

Environmental	Design of websites and online services influences the behaviour of users. Secure design needs to be the default so that people can make choices and websites encourage secure behaviours
	Economic factors – impact on people's behaviour (if the website offers a good deal people will accept the risks)
Social	People are influenced by those around them – friends, family, and colleagues. Leadership – especially in a workplace can be a strong influence.
Personal	Knowledge, skills and understanding: • We need to know what the risks are and what they look like (this is difficult when these are constantly changing) • We need consistent/useful information – although this is not enough to change behaviour
	Perceptions, attitudes and beliefs influence security behaviours.

Communication campaigns

The report accepts the need to improve knowledge and information on how to stay safe online, but emphasises that people who are provided with information do not necessarily use it and that other factors (influencers) highlighted above also have an impact. Campaigns are generally accepted to be more influential if they target messages at specific groups. With internet security most messages given out are general and not targeted.

Research suggests that campaigns are more likely to be successful if they are supplemented with:

- 'Concurrent community programmes
- Policy and law changes
- Readily available products and services to support the target behaviours
- Tailored messages for specific audiences.
- Messages being built-in to many different delivery mechanisms
- Role models and champions exhibiting the behaviour'

They point to the limitations of mass communication campaigns, which may 'backfire' with unintentional implications. To give an example

- A campaign suggests there are substantial risks
- Users do not directly have negative experiences, or if they do they are unclear as to how their behaviour may have caused the experience.
- As a result they are unclear about how they could have had the 'power to change' the experience and, so
- They come to believe that there is little they can do to protect themselves, and lack confidence in the expert advice they are being given.

This then may mean that they 'may even adopt a coping strategy of **learned helplessness -** and simply assume there is nothing they can do to change the situation.'

The role of the 'messenger' and how trusted/respected they are then becomes potentially relevant.

The report questions whether the tech sector should be tasked to make it possible that 'the secure option is the default option and design in security from the start'. This would mean that we made positive use of the environmental factors through the design of technology.

As with other publications the report emphasises the lack of research into 'controlled' behaviour responses to online safety and security messages and responses. This means that we remain 'unclear about what works' to change cyber security behaviours.

Protection Motivation Theory (PMT), developed by Rogers et al makes clear that the likelihood of people adapting their behaviour in response to a threat will be influenced by the degree of the harm (perceived and actual), and the rewards there are for changing their behaviour. In PMT theory these are known as 'threat appraisal' (focused on the threat itself) and 'coping appraisal' (the ability to act against the threat). A coping appraisal process will also take into consideration people's own 'self-efficacy' in achieving a change, linked to the costs of making a change.

Using protection motivation theory in the design of nudges to improve online security behaviour René van Bavela,∗ , Nuria Rodríguez-Priegoa,d , José Vilab , Pam Briggsc (Joint Research Centre, European Commission), March 2019

The report highlights that awareness campaigns and warnings about cybersecurity rely on people making 'very informed or rational decisions' about how to overcome the challenges and risks. Raising awareness is not sufficient, decisions need to be made by the user.

The research carried out aimed to look at 'whether small changes in the design of online notifications (i.e. a nudge according to the behavioural economics literature; Thaler and Sunstein, 2008) can seamlessly trigger more secure behaviours.'

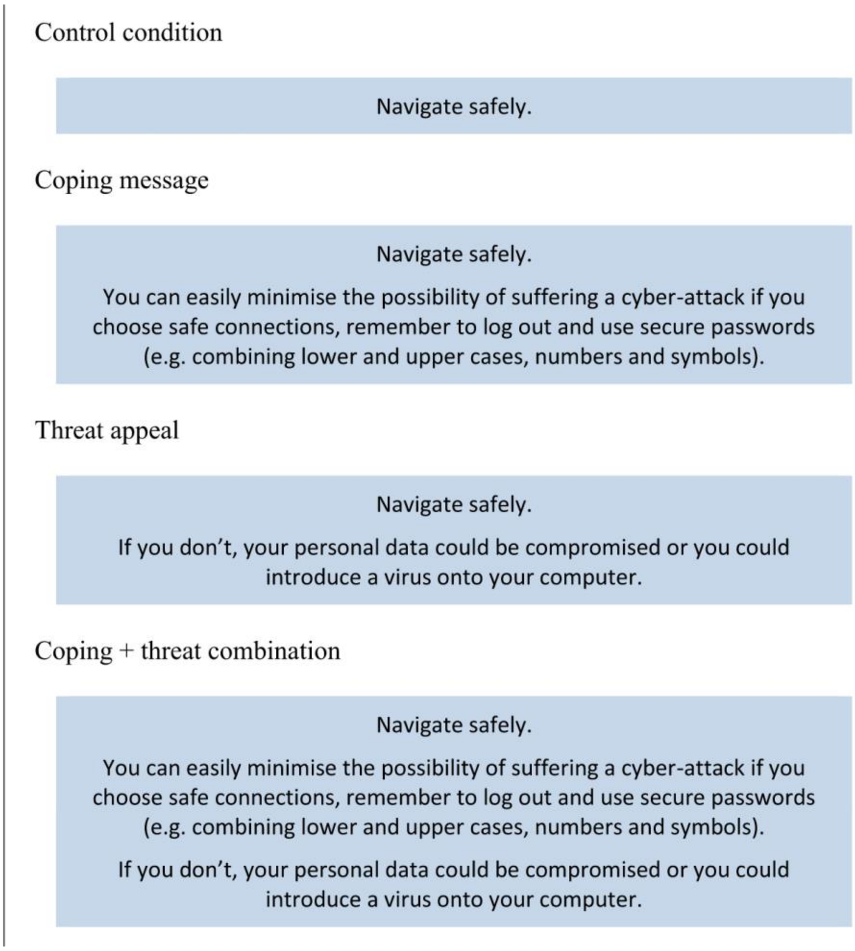
PMT was used by the researchers who were interested in what precautionary action people would take in response to a threat, how maladaptive behaviours such as denial or avoidance come into effect as people assess if the recommended action will remove the threat (response efficacy) and how confident they are to carry out the action (self-efficacy). Adaptive behaviours may then occur following appraisal but can be influenced by the response costs.

The study looked at whether ‘people will behave more securely online if (a) their awareness of the threat is heightened (threat appraisal) and (b) they are made aware of the appropriate protective responses to take (coping appraisal).’

Study participants were asked to navigate an e-commerce site securely with the aim of seeing which of the messages (below) would be most effective. The three PMT-inspired notifications were designed to trigger or nudge more secure behaviour:

- A coping message told users it was easy to minimize the chances of a cyber-attack and also indicated what steps to take.
- A fear appeal warned individuals that their behaviour could leave them vulnerable to a cyber-attack.
- A threat and coping message contained both elements described above.

The table below illustrates in detail the study that took place.



Control condition

Navigate safely.

Coping message

Navigate safely.

You can easily minimise the possibility of suffering a cyber-attack if you choose safe connections, remember to log out and use secure passwords (e.g. combining lower and upper cases, numbers and symbols).

Threat appeal

Navigate safely.

If you don’t, your personal data could be compromised or you could introduce a virus onto your computer.

Coping + threat combination

Navigate safely.

You can easily minimise the possibility of suffering a cyber-attack if you choose safe connections, remember to log out and use secure passwords (e.g. combining lower and upper cases, numbers and symbols).

If you don’t, your personal data could be compromised or you could introduce a virus onto your computer.

There conclusions were that ‘treatments including a coping message worked better than a threat appeal; it was more effective to tell subjects how to effectively manage the probability of suffering a cyberattack than to threaten them with the consequences of not behaving safely. Viewed differently, a coping message was effective and the addition of a threat appeal did not significantly increase its effectiveness. On the other hand, although the threat appeal on its own was effective, the addition of a coping message significantly increased its effectiveness.'

They report that 'the most successful interventions simply involved telling our participants what effective actions to take to protect themselves online.' They report the growing recognition (mainly from health settings) that fear appeals in isolation have limited value in securing behaviour change. They can also be counter-productive, producing defensive responses, especially amongst the most vulnerable groups. If you have no coping mechanism you may feel uncomfortable and deny that there is any risk. People targeted need to know what response is recommended for an appeal to be successful.

They summarised, 'messages that contain 'coping' information that support the user in taking action against cybersecurity threat are most effective in improving secure behaviours. Threat messages, presented in isolation, are more likely to lead to a defensive or avoidant response (dropout in our study).'

They report that the research has implications for communications and policy, moving beyond just reporting of the threats, and improving 'coping messages' and the way that they are promoted.

Like others they highlight that 'people are rarely given simple, consistent information about how to deal with a cyber-threat and often don't know which source to trust (Shillair and Meng, 2017).' They emphasise that these coping interventions are particularly useful when people have little prior knowledge of how to stay safe online.

References & other background reading

UK Safer Internet Centre, Supporting vulnerable groups online, August 2017

Ipsos Mori Scotland for Carnegie UK, Online privacy from attitudes to action

The behavioural science of online harm and manipulation and what to do about it, April 2019

Government Office for Science, Using behavioural insights to improve the publics use of cyber security best practices, 2014

Bavel et al, Using protection motivation theory in the design of nudges to improve online security behavior, March 2019

Ofcom Adults media use and attitudes, 2019

Behaviour Insights Team

The behavioural science of online harm and manipulation and what to do about it, April 2019

Improving consumer understanding of contractual terms and privacy policies evidence based actions for business, July 2019