Internet-connected products are everywhere these days, in our homes, in our offices and pervasive throughout our lives. They allow us to monitor the temperature in our apartments, to put the kettle on before we even get out of our beds and to reduce our carbon footprint through reduced energy wastage, for example.

However, the Internet of Things (IoT) poses many threats to consumers. Products that are ‘Secure by Design’ are the ideal, however currently many ‘things’ in the IoT are far from secure and users need to take action to help protect their internet connected products.

This issue can be seen in the numerous incursions and hacks reported regularly in the press. With attacks on driverless cars turning off the engine on a moving vehicle, strangers being able to talk to children through connected toys or attacks on cameras we may have in our homes to keep us secure, the exciting and rapidly changing world in which we live can also potentially allow unwanted intrusion into our lives through cyber security breaches and the introduction of more technology into our homes.

To help counter cyber threats, consumers will need to adopt protective behaviours when using internet-connected products. Such behaviours are wide ranging from using strong and unique passwords to taking unsafe products off the home Wi-Fi. However, to encourage protective behaviours when using internet connected products, we first need to understand what consumers need to do to protect their products.

This report has been prepared by UCL researchers as part of PETRAS, a large research programme examining cyber security in the context of the IoT. The cyberhygiene project focused on designing ways to effect behavioural change in consumers in order to improve their cyber security practices. Cyberhygiene is the practices that people use to stay secure and safe when using connected devices.

In this report, we detail the studies that identify key protective behaviours across product lifecycles (purchasing, set-up and maintenance, and disposal) that users could engage in to protect themselves based on experts’ and users’ perceptions.

By empowering consumers with practical advice that they will actually use, as well as persuading manufacturers to follow ‘Secure by Design’ principles, the IoT can be made more secure for consumers.

Summary
There is a lot of work underway to make sure that IoT products are ‘Secure by Design’ to prevent cybersecurity threats. But that is only part of the equation - alongside this, encouraging consumers to adopt safer behaviours when they use internet connected products is a key element in defending against cybersecurity risks. Knowledgeable users can not only help prevent successful attacks but also drive manufacturers to build robust security into their products.

Current research shows that 66% of people are worried about unauthorised access (hacking) to their internet connected products, but that 72% are not aware of the protective behaviours they should be using to shield themselves from these risks. Some examples of these protective behaviour include regularly updating products and using strong passwords (such as three random words).

Behaviour change campaigns can encourage better protective behaviours amongst users, helping to safeguard products from threats and protect users from risks. The first stage in designing behaviour change interventions is to identify the target behaviour. Who needs to do what differently, when, where, and how?

The “who” question is particularly important to address in the cybersecurity context, often behaviour change campaigns jump to a “fix the user” approach instead of focussing on different parties or participants that contribute to behavioural cybersecurity issues. For example, in the workplace, the practice of frequent password changes leads users to create less secure passwords rendering the practice less useful. Recent efforts have therefore focussed on changing the behaviour of security officers or system owners who dictate these policies. This shift can be seen through the National Cyber Security Centre which has published guidance on passwords for system owners in workplaces, detailing advice for password policies that are human centred (https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach).

In the context of cybersecurity, there is often little consensus on what constitutes good advice. Many people already have a good sense of how to protect our computers and smart phones, with current government advice encouraging people to “Download software updates” and “Use strong passwords comprising of three random words” (HM Government, 2017). However, the same cannot be said for emerging technology like the Internet of Things, where there is a lack of evidence base and understanding of good security advice for users. There is also inconsistency in the advice given by different sources of advice which can cause confusion in consumers. A key aspect of identifying advice for consumers is that it aligns with users’ goals and motivations. Often, advice can be cumbersome and too technical for consumers to follow which reduces the likelihood that consumers will follow it.

The work detailed in this report aimed to first identify what behaviours are currently expected of users to protect their products through a survey with IoT security experts, and secondly identify which of these behaviours are perceived as usable through a survey with prospective users. The report ends with practical, important and usable advice for consumers that are currently adopting, or seeking to adopt, IoT products based on the current status quo around securing consumer internet connected products.

---


2 https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry

The researchers used an “expert consensus” approach where a panel of 34 cybersecurity experts first independently gave estimates on the importance of 43 different possible security-focused behaviours across product lifecycles (pre-purchase, set-up and maintenance, to disposal of product). The research team then reviewed the data and issued a summary report back to the expert panel, which discussed the report, and then if necessary updated their initial estimates of importance. The process continued until experts reached a consensus around important behaviours to protect IoT products.

The following behaviours were seen by experts as most important actions for each product life cycle.

**Product purchasing**

1. Buy products that allow passwords and for the default password to be changed
2. Research the security of the IoT product before purchasing
3. Decide whether the considered IoT product is acceptable for its intended purpose (e.g. decide whether smart features are required or if a non-IoT product would suffice)

**Product set-up and maintenance**

1. Change the default password on products, networks and services
2. Use strong passwords on products, networks & services
3. Ensure that your Wi-Fi is secured (to at least WPA2 level)

**Product disposal**

1. Securely wipe products before disposal, where possible
2. Remove unsafe products from the network
3. Perform a factory reset on products before disposal, where possible

However, expert views are only one part of the equation. Security advice can be ineffective if users don’t understand or can’t carry out the behaviour suggested. For example, when asked to ‘use a strong password’, some users may find this advice vague and unhelpful. What is a strong password? Is it a phrase, does it need numbers, capital letters, symbols?

Research has shown that if security advice is based solely on the views of information security experts with little consideration of users’ goals, motivations and capabilities, users may prioritise convenience of use, over security. There has also recently been a move towards more usable security advice for users through attempts to align security with users’ goals. For example, the UK government recently changed their password guidance to “three random words” as research has shown they are easier to remember for users and the developer of initial password guidance which argued that they had to be long and complicated has since admitted that the guidance was wrong.

Furthermore, users have to make up for poor product design, such as changing default passwords that are shipped with the product. These could be rectified through better security by design. It is important to focus on behaviours that users will continue to be responsible for (such as using strong passwords and updating products).

In order to identify advice that is usable for users, in study two the researchers asked prospective users to indicate how easy each of the suggested security behaviours was to adopt and how time consuming it was.

---

5 https://www.cyberaware.gov.uk/blog/three-random-words
6 http://www.telegraph.co.uk/technology/2017/08/08/man-wrote-password-bible-admits-advice-completely-wrong/
The second study asked 479 IoT consumers to rate the 43 protective behaviours from study 1 on importance, usability (in terms of how time consuming the behaviour is and how easy it is to perform) and likelihood of following the advice.

In terms of importance, users viewed password behaviours as vital to securing products. They also rated not sharing passwords and securely wiping products before disposal highly. For usability, “not sharing passwords” and “using auto-update” were considered to be the most implementable of the behaviours in terms of relative ease of action and time consumption. Reading terms and conditions and isolating products in the network were seen as least usable, probably due to the time consuming and technical nature of these actions. Table 1 shows the top three and bottom three behaviours per lifecycle stage as rated by participants.

Table 1. Top three and bottom three ratings of importance and usability for each lifecycle stage

<table>
<thead>
<tr>
<th>Importance (out of 7)</th>
<th>Purchasing</th>
<th>Set-up and maintenance</th>
<th>Disposal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 3</td>
<td>Bottom 3</td>
<td>Top 3</td>
<td>Bottom 3</td>
</tr>
<tr>
<td>1. Buy devices with password protection (6.35)</td>
<td>1. Minimise device providers (3.82)</td>
<td>1. Don't share passwords (6.64)</td>
<td>1. Securely wipe before disposal (6.29)</td>
</tr>
<tr>
<td>2. Buy reputable products (6.16)</td>
<td>2. Buy devices without cloud services (5.20)</td>
<td>2. Use strong passwords (6.58)</td>
<td>2. Perform a factory reset (6.27)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usability (out of 7)</th>
<th>Purchasing</th>
<th>Set-up and maintenance</th>
<th>Disposal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 3</td>
<td>Bottom 3</td>
<td>Top 3</td>
<td>Bottom 3</td>
</tr>
<tr>
<td>1. Buy reputable products (5.44)</td>
<td>1. Research product before buying (3.82)</td>
<td>1. Don't share passwords (6.3)</td>
<td>1. Remove unsafe products from network (4.78)</td>
</tr>
<tr>
<td>2. Buy devices with password protection (5.02)</td>
<td>2. Buy updatable products (4.19)</td>
<td>2. Use auto-update (5.63)</td>
<td>2. Perform a factory reset (7.73)</td>
</tr>
<tr>
<td>3. Decide whether you need a smart device is necessary (4.84)</td>
<td>3. Buy devices without cloud services (4.35)</td>
<td>3. Write down passwords (5.43)</td>
<td>3. Discard devices with security weaknesses (4.6)</td>
</tr>
</tbody>
</table>

Get in touch: IoTUK.org.uk info@IoTUK.org.uk IoTUKNews Cyberhygiene Insight Report 5
Study Two: User Views on Usability of TargetBehaviours

The researchers also investigated users’ willingness to follow the advice. They found that users are most willing to perform password behaviours e.g. “Not sharing passwords”; “Use strong passwords” and less willing to perform network behaviours e.g. “isolate devices onto their own network”; “disabling UPnP”. These findings demonstrate that behaviours that require high technical capability are less likely to be adopted by consumers.

The findings also allowed the comparison between users’ and experts’ perceptions of relative importance of security advice. Experts place greater importance on using a password manager, whereas users place greater importance on writing passwords down. These findings suggest that users either lack knowledge of the importance of passwords managers or that they prefer more physical methods of managing with passwords.

The next stage of the cyberhygiene project was to combine the findings from studies one and two to create effective advice for consumers of internet connected products. To achieve this, the researchers combined the experts’ ratings of importance for consensus-agreed behaviours with the users’ ratings of what behaviours were most usable. Therefore, the final set of behaviours to be recommended to users comprises of important but usable behaviours (see appendix for infographic on page 8).

The findings described here provide practical advice for consumers based on what the current status quo is regarding what is expected of consumers to protect their internet connected products. Presently, the burden for protecting IoT devices often falls to consumers and future government policy will encourage manufacturers to follow principles of Secure by Design to reduce this burden. Furthermore, we need the security of IoT devices to be aligned further with user goals and motivations for using IoT devices. Improving the security of IoT devices will require a holistic approach, requiring behaviour change on many levels from manufacturers to retailers to consumers.
Next steps: Using a systematic method for behaviour change

This report has identified the generation of advice for consumers to protect their IoT products. To encourage consumer uptake of security advice, the next step is to explore the reasons behind why consumers do not follow advice through behavioural analysis and then explore the full range of potential interventions to be considered. Currently, behaviour change interventions are often conducted without using a systematic method that draws on behavioural science, instead jumping straight to an “awareness” campaign. However, interventions that are designed following an in-depth behavioural analysis and with the aid of evidence based intervention frameworks are likely to have a higher probability of success. The remaining studies in cyberhygiene were focussed on behaviour change interventions for a subset of the identified behaviours.

Conclusion

There is still much work required to securing the IoT that requires radical shifts in the manufacturing of the devices. However, this report, based on the research conducted at UCL provides advice for consumers that are currently or seeking to adopt IoT products.

In early 2018, the Department for Digital, Culture, Media, and Sport will be releasing additional guidelines to help manufacturers with creating products which are “Secure by Design”. This is expected to include recommendations around the enablement of consumers to make more informed choices regarding the security features of products currently on the market.

This report was created for PETRAS and IoTUK by Dr John Blythe and Dr Carmen Lefevre.

Dr John Blythe is Research Associate for the PETRAS Internet of Things Research Hub (see http://www.petrashub.org/). John is currently employed at the UCL Dawes Centre for Future Crime and has previously held positions at the UCL Centre for Behaviour Change, Department for Digital, Culture, Media and Sport, and PaCT Lab at Northumbria University. He has worked on a number of different projects exploring behaviour change and cyber security.

Dr Carmen Lefevre is an Honorary Senior Research Associate and Associate Consultant of UCL’s Centre for Behaviour Change. She is currently involved in the Horizon 2020 City4Age project aiming to utilise digital technology to prolong independent living in older adults as well as a PETRAS funded project on Cyberhygiene aiming to improve user’s cybersecurity in the context of the Internet of Things. Prior to joining the CBC in 2015, Carmen held posts at the Universities of Leeds and York, as well as Northumbria University. Carmen completed her PhD in Psychology (2013) at the University of St Andrews. She is currently a UX Researcher at DrEd.

Get in touch: IoTUK.org.uk info@IoTUK.org.uk @IoTUKNews

7 https://dcmsblog.uk/2017/10/securing-connected-world/
Purchasing

1. Decide whether an internet-connected product is necessary or if a normal product would suffice.

2. Buy products that allow for password protection and for the default password to be changed.

3. Buy products with security-focused platforms (e.g., Apple HomeKit, Samsung SmartThings)
**SET-UP**

4. **Change** the default **password** on products, networks and services

   "Alexa... turn on automatic updates"

   "I will now update automatically"

5. Select "**automatically update**" when possible

6. **Use strong passwords** on products, networks and services

7. **Ensure** that your **Wi-Fi** is secured to at least WPA2 level

   "Do you want to share your location with us?"

   **Password strength**
   
   **Default Password**

   **Change Default Password**

   **Password**
   
   **Change**

   **Reset**

   **Factory**

   **Discard products** that have security weaknesses that can’t be fixed

   **APP STORE**

   **Authorised smart companion apps**
MAINTENANCE

8

Don’t share your passwords

9

Only use authorised software/services with your IoT products

10

Keep your IoT products updated

11

Limit sharing of your personal information with products
DISPOSAL

12
Remove unsafe products from the Wi-Fi network

13
Perform a factory reset on products before disposal, where possible

14
Discard products that have security weaknesses that can’t be fixed