Australian Government
Department of the Prime Minister and Cabinet

BETA

Stay Smart

Helping consumers choose cyber secure smart devices

March 2022

Other uses

Enquiries regarding this license and any other use of this document are welcome at:

Managing Director
Behavioural Economics Team of the Australian Government
Department of the Prime Minister and Cabinet
1 National Circuit
Barton ACT 2600
Ngunnawal Country
Email: beta@pmc.gov.au

The views expressed in this paper are those of the authors and do not necessarily reflect those of the Department of the Prime Minister and Cabinet or the Australian Government.

Research team

Current and former staff who contributed to the report were: Ashley Breckenridge, Vathany McCormick, Hanne M Watkins, Nicholas Hilderson, Andrea Willis, Scott Copley and Su Mon Kyaw-Myint.

Acknowledgments

Thank you to the Department of Home Affairs for their support and valuable contribution in making this project happen. In particular, special thanks to D'Arcy Ertel, Nishant Rao, Grace Zhang, and Jeremy Burnett for their work on this project.

The trial was pre-registered on the BETA website and the American Economic Association registry:

https://behaviouraleconomics.pmc.gov.au/projects/stay-smart-helping-consumers-choose-cyber-secure-smart-devices

https://www.socialscienceregistry.org/trials/8044

Who?

Who are we?

We are the Behavioural Economics Team of the Australian Government, or BETA. We are the Australian Government's first central unit applying behavioural economics to improve public policy, programs and processes.

We use behavioural economics, science and psychology to improve policy outcomes. Our mission is to advance the wellbeing of Australians through the application and rigorous evaluation of behavioural insights to public policy and administration.

What is behavioural economics?

Economics has traditionally assumed people always make decisions in their best interests. Behavioural economics challenges this view by providing a more realistic model of human behaviour. It recognises we are systematically biased (for example, we tend to satisfy our present self rather than planning for the future) and can make decisions that conflict with our own interests.

What are behavioural insights and how are they useful for policy design?

Behavioural insights apply behavioural economics concepts to the real world by drawing on empirically-tested results. These new tools can inform the design of government interventions to improve the welfare of citizens.

Rather than expect citizens to be optimal decision makers, drawing on behavioural insights ensures policy makers will design policies that go with the grain of human behaviour. For example, citizens may struggle to make choices in their own best interests, such as saving more money. Policy makers can apply behavioural insights that preserve freedom, but encourage a different choice – by helping citizens to set a plan to save regularly.

Contents

Executive summary

‘Smart’ devices are products with extra functionality to connect to the internet. **Many smart devices lack basic cyber security features,** and their rising popularity increases the risk of cyber security incidents and cybercrime. Consumers may not be aware of the risk of insecure smart devices, as it is currently difficult to find and use cyber security information when shopping for smart devices. As a result, manufacturers are not sufficiently incentivised to invest in cyber security.

A cyber security labelling scheme may help consumers make better purchasing decisions. A label could communicate to consumers the overall level of cyber security of the device, or specific details such as for how long it will continue to receive security updates. This would allow consumers to compare products and make more cyber secure purchases.

In partnership with the Department of Home Affairs, BETA explored how cyber security labels could perform in an Australian setting. **We designed three different cyber security labels: a ‘graded’ label,** using shield and tick icons to indicate four levels of cyber security; and **two ‘expiry’ labels,** indicating how long the device would receive guaranteed security updates (e.g. “guaranteed until August 2023”). One expiry label included an icon, the other simply included the same information in plain text.

We tested the labels in an online ‘shopping scenario’ with a nationally representative sample of 6,000 Australians. Participants were asked to choose which smart devices they would like to ‘buy’. We found:

- Participants were more likely to choose a device with a cyber security label than one without a label, by 13-19 percentage points.
- The graded shield had the largest impact, but the expiry labels were still effective.
- A high security level or long expiry date increased the likelihood of choosing a device.

Follow-up questions and analysis allowed us to examine the different advantages and disadvantages of each label:

- Participants preferred both the graded shield label and the icon expiry label over the plain text expiry label.
- Participants generally had a better understanding of what the two expiry labels were communicating compared to the graded shield label.

We expect in the real world people’s understanding of the labels would increase over time as they become familiar with them, and especially if supported by a consumer education campaign.

These results demonstrate the potential for a labelling scheme to improve consumer decision-making in the Australian smart device market. Further research in the field – such as partnering with a retailer and evaluating the impact of cyber security labels on real choices made by actual consumers – could be considered to test how the current findings translate to a real-world context.

Why?

Many smart devices lack basic cyber security features, increasing the risk of cyber security incidents and cybercrime

'Smart' devices – also known as consumer Internet of Things (IoT) devices – are products with extra functionality to connect to the internet. Examples include smart lights that can be controlled via an app and smart doorbells that let you monitor your deliveries remotely.[1] Smart devices are becoming increasingly popular among consumers in Australia and internationally, with estimates suggesting there are already 21 billion smart devices worldwide today (Malan, Eager, Lale-Demoz, Ranghieri & Brady, 2020).

While helpful to our everyday lives, research shows many of these devices have security vulnerabilities that can be exploited, leading to negative impacts on cyber security, privacy, and online safety (Marrapese, 2020; Sivaraman, Gharakheili & Fernandes, 2017). For example, in 2018 the *Washington Post* reported hackers used a 'smart' baby monitor to access a family's Wi-Fi system and broadcast threats to the parents (Wang, 2018).

Smart devices are insecure in part due to a lack of cyber security information for consumers, leading to a lack of awareness and understanding and a lack of incentives for manufacturers

One reason many smart devices are vulnerable may be that it is currently difficult for consumers to find and use cyber security information about smart devices currently on the market (Data61, 2020; Blythe, Sombatruang, & Johnson, 2019). Many consumers incorrectly assume that cyber security is already 'built in' to smart devices (Data61, 2020; Harris Interactive, 2019). As a result, manufacturers do not currently feel a significant push from consumers to raise their standards and are not sufficiently incentivised to invest in cyber security (Department of Home Affairs, 2021b). When a business fails to invest in cyber security, the direct cost of any cyber security incident is often felt by others – for example, their customers and suppliers – rather than by the business itself, and there may be a lack of feedback about these consequences.

Cyber security labels may address both these issues and help consumers make better decisions

Consumers say they care about cyber security and would take it into account when shopping – if they had access to the right information (Data61, 2020; Harris Interactive, 2019). A label could communicate the overall level of cyber security of the device, or more specific details about the device to consumers – for example for how long it will continue to receive security updates. As consumers begin to make purchasing decisions which take into account the

[1] For the purposes of this report, 'smart devices' does not include mobile phones and laptops.

cyber security of a device, businesses will be increasingly incentivised to invest in cyber security. Maintaining their reputation as a trusted brand is a strong driver for manufacturers to invest in cyber security (Department of Home Affairs, 2021b). Labels are one way businesses could signal their commitment to cyber security.

Evidence from existing labelling schemes and academic research shows labels can help consumers make better purchasing choices

Based on previous research, we expect a label would be effective in helping consumers take cyber security information into account when purchasing smart devices. In an online study with U.K. residents, Johnson and colleagues (2020) found consumers (in a hypothetical shopping scenario) were significantly more likely to select a smart device with a cyber security label than one without. This is consistent with the conclusions of a research study commissioned by the U.K.'s Department for Digital, Culture, Media and Sport (DCMS, Harris Interactive, 2019), which estimated that even if a device with a label was 5% more expensive, 59% of consumers would choose it over a cheaper device *without* a label. In both studies, participants indicated cyber security labels would assist their purchasing decisions in the real world (Emami-Naeini, Agarwal, Cranor & Hibshi, 2020). In the Australian context, a survey by Data61 (2020) found 75% of people agreed they would be "more likely to purchase a [smart device] if it had a cyber security rating system, similar to the Energy Star Rating".

In partnership with the Department of Home Affairs, BETA explored how Australian consumers would respond to cyber security labels

As part of *Australia's Cyber Security Strategy 2020* (Cyber Security Strategy, 2020) the Australian Government is considering a range of regulatory reforms and voluntary incentives to strengthen cyber security across the economy. This includes considering the introduction of a cyber security labelling scheme for consumer smart devices. Between 13 July and 27 August 2021, Home Affairs consulted the community and industry on a voluntary 'graded' label, and a mandatory 'expiry date' label (Department of Home Affairs, 2021a). In this project, we aimed to build on existing international evidence and explore which type of cyber security labels have the biggest impact on Australians' purchasing decisions when purchasing smart devices. We also explored whether people differentiate between different levels of cyber security communicated by the labels, and how much people are willing to pay for a device with a cyber security label.

What we did

In collaboration with Home Affairs, we designed cyber security labels to help consumers make informed choices about their smart devices

Buying a smart device requires assessing and weighing up a wide range of information, including product features, price, and your personal circumstances. While consumers say they would take cyber security into account if this information was available (Data61, 2020; Harris Interactive, 2019), we also know people have difficulty making a decision when considering a great deal of information, especially if some of it is technical and unfamiliar (Bossaerts & Murawski, 2017). In these situations, consumers often rely on heuristics – or 'rules of thumb' – and cognitive shortcuts to make the choice easier (Gigerenzer & Gaissmaier, 2011). Simple, visually appealing labels can make it easier to take a 'shortcut' to choose a device with high cyber security rating. In collaboration with Home Affairs, we designed three different cyber security labels (see Figure 1).

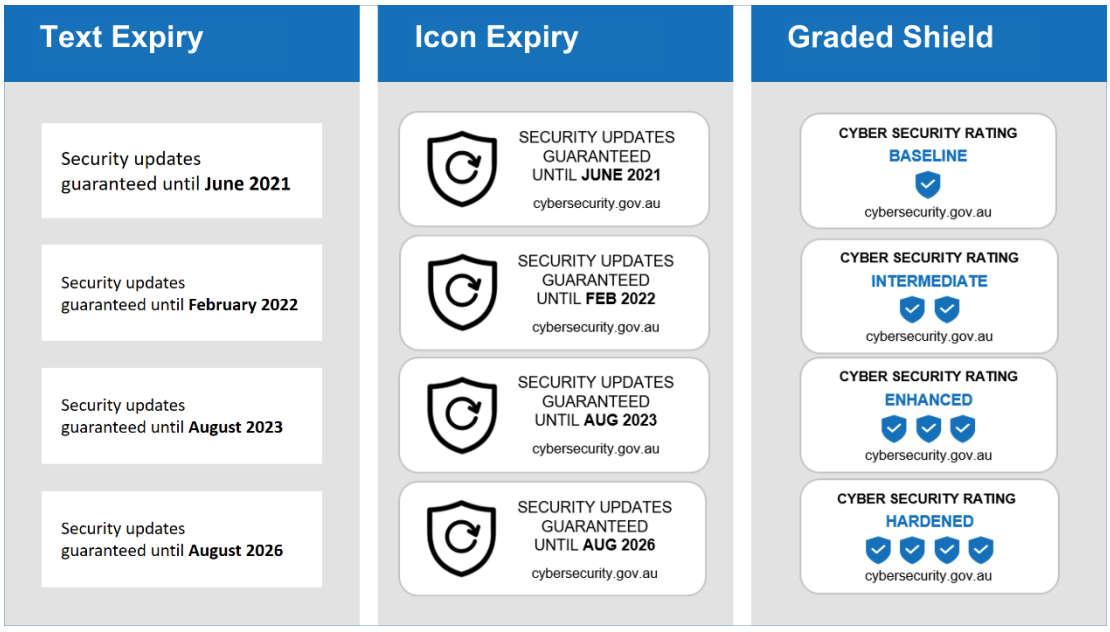


Figure 1. The three types of cyber security labels designed and tested for this project. Each label type had four levels. For the expiry labels, the levels indicated increasing amounts of time the device would receive security updates. For the graded shield label, the four levels indicate increasingly strong categories of cyber security, modelled on the Singapore framework (Cyber Security Agency of Singapore, 2021).

We drew on behavioural science principles to design labels that would be informative, salient, recognisable, novel, and trustworthy

Two of the labels were ‘expiry date’ labels, which indicated how long the device would continue to receive security updates. The expiry date label was simply ‘informative’ in that it included a clear statement about cyber security updates (e.g. “Security updates guaranteed until February 2022”, see Figures 1 and 2). On the second label, the icon expiry label, this statement was supported by an update icon (circular arrow) inside a shield. Each label had four levels, indicating increasing lengths of time during which security updates would be guaranteed. The Level 1 expiry label indicated security updates were guaranteed until June 2021. As we conducted this study in July 2021, we included this (past) date to test what consumers would do when faced with an device that no longer had guaranteed security updates (see further details in the ‘What we found’ section).

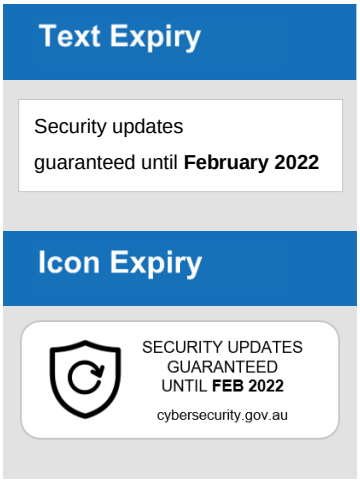


Figure 2. The expiry labels.

For the graded shield label we drew on four behavioural science principles – salience, familiarity, novelty, and trusted messenger (see Box 1) – to enhance the effectiveness of the label. We chose to use tick-marks combined with a shield icon to visually communicate ‘positive’ levels of security. Tick marks also differentiate the design from the ‘star ratings’ that are used in Australia for energy and water efficiency, noting that cyber security cannot be measured on a continuous scale – compared to kilowatts and litres (see Figures 1 and 3). This design was tested in a study by Harris Interactive (2019) and was preferred by participants compared to other labels. We also drew on international examples to inform the design: Singapore’s Cybersecurity Labelling Scheme also consists of a graded label with four levels (Cyber Security Agency of Singapore, 2021). We added descriptor words (e.g. ‘baseline’ and ‘enhanced’) to each level. This was important, as a single shield (Level 1) indicates a ‘baseline’ level of cyber security has been achieved (an appropriate level for some devices), rather than signalling weak cyber security.

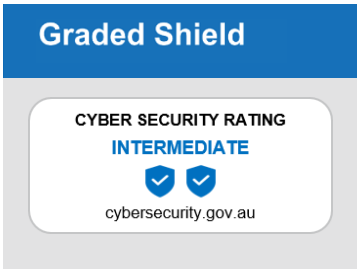


Figure 3. The graded shield label.

Box 1: The behavioural science behind the labels

Salience

In order to be effective, a label has to be noticed by consumers: making a label colourful, rather than just black and white, makes it stand out against device packaging. We adopted blue on a white background for the graded shield label so that the level (e.g., 'baseline') and shields were most salient.

Familiarity

Ideally, consumers would understand the message of the label almost instantly, without needing to read the text. Adopting styles that are commonly used to indicate approval means the message is communicated quickly and unambiguously (Argo & Main, 2004). We therefore adopted 'tick marks' for the graded shield label as these are frequently used in Australia[2] and are easily recognisable as indicating a positive rating. 'Expiry' dates are also familiar to consumers from perishable food and drink items.

Novelty

Academic literature has shown that in addition to familiarity, novelty helps make a label more attention-grabbing and memorable (Pieters, Warlop, & Wedel, 2002). Ensuring some element of the design is unique could help it cut through other information on device packaging (Boelhouwer, et al, 2013). For both the icon expiry label and graded shield label we used a shield icon to add novelty and connect the label to the idea of security.

Trusted messenger

Including a Government URL makes it clear the message is coming from an official and trusted source. The icon expiry and graded shield labels both included a '.gov.au' website link. In addition to signalling trustworthiness (e.g. Wilson & Sherrell, 1993), such a link could be useful for providing consumers with further information about the labelling scheme and assurance of its legitimacy.

[2] For example, a 'tick mark' has been used by the Heart Foundation in campaigns for healthy eating (Heart Foundation, 2021), to indicate that a device conforms with the *Radiocommunications Act 1992* (the 'C-tick', IP Australia, n.d.), and to indicate that a product is certified organic (Australian Certified Organic, 2018).

We tested the labels to evaluate whether they influenced participants' purchasing decisions

Our online study combined two research methods for evaluating the effectiveness of the labels: a randomised control trial (RCT) and a discrete choice experiment (DCE). The DCE provided an estimate of *how much* each label influenced participants' purchasing decisions in a hypothetical shopping scenario. The RCT allowed us to compare the labels and test which one had the *biggest* influence on participants' decisions. We combined both methods by randomly assigning each participant to see one of the three label types (the RCT), and then asking them to complete a shopping scenario (the DCE) in which they used the label to make purchasing decisions about smart devices.

We recruited 6,000 Australian adults[3] to complete the online 'shopping scenario'

Participants were randomly assigned to shop for one of four smart products: a TV, watch, home hub, or a light bulb. Participants were asked to weigh up three different product attributes: price, features, and cyber security, and choose the device they would prefer to 'buy' (Figure 4 shows those in the smart light category). Participants faced this choice ten times. Each time, the attributes of the three devices varied, which meant participants faced repeated trade-offs between price, standard or premium functionality, and four different cyber security levels (labels could also be absent). By analysing which devices participants chose, we could estimate how much the cyber security labels influenced their choices, and how they weighed up cyber security against the other product features and price.

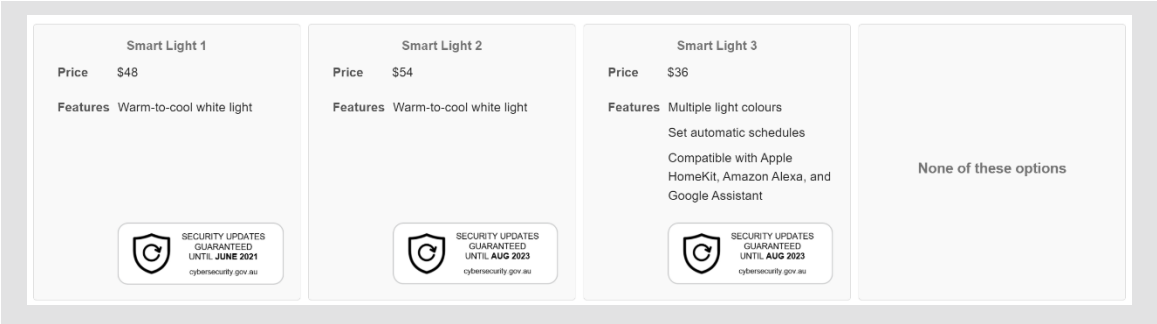


Figure 4. An example of the purchasing choice participants faced. This screenshot displays the 'smart light' product type. Lights 1 and 2 have standard features, while Light 3 has premium features. The price for the lights ranged from $30 to $54. All devices have a cyber security label in this screenshot, but devices could also be displayed with no label (blank).

In the final part of the study (once the shopping scenario was completed), we asked participants a range of true-false, multiple-choice and open-ended questions to gather more in-depth information about people's impressions and understanding of the labels.[4] This helped us explore whether people liked the labels and understood them correctly.

[3] Full demographic details of the sample are included in the Technical Appendix.
[4] A full copy of the study materials is provided in the Technical Appendix.

What we found

People were more likely to choose a device with a cyber security label than one without, and the graded shield label had the largest impact

In the online shopping scenario, a device with a cyber security label was 13-19 percentage points more likely to be chosen than a device with no label (Figure 5). Consistent with previous research, participants were also, on average, more likely to choose a device with premium product features rather than standard features, and they were more likely to choose a cheaper device than a more expensive one (Johnson et al., 2020).

The graded shield label had the largest impact on participants' choices, with a 19 percentage point increase in purchasing compared to no label.[5] The two expiry labels did not differ from each other in terms of their impact on participants' choices. The graded shield label may have been most effective as consumers are more familiar with a rating label on consumer products (while expiry labels are currently most common on food and drinks), and the design elements may have made it more eye-catching and easier to interpret.

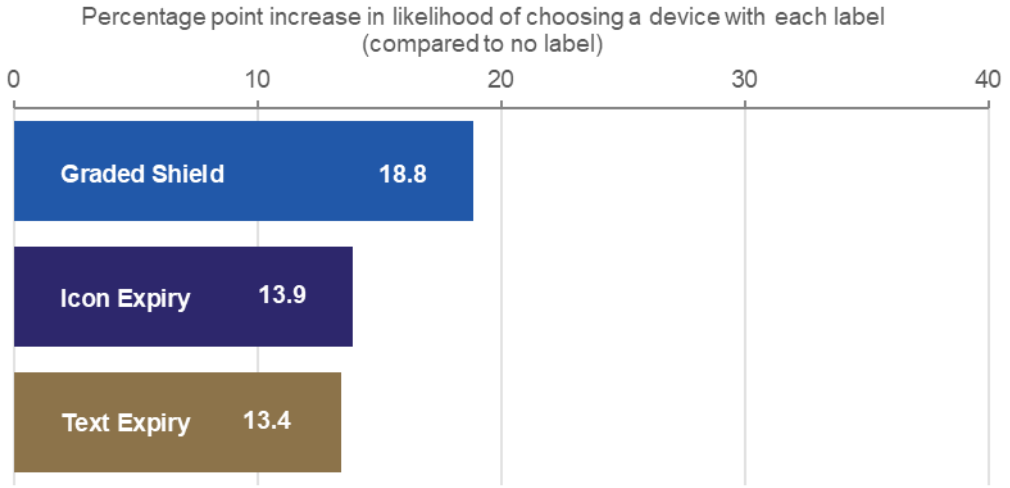


Figure 5. Increase in purchasing associated with each label, compared to a device with no label. Each horizontal bar indicates the impact of a cyber security label (vs. no label), when product features and price are held constant. All results were significant compared to the no label group, $p < 0.001$. The sample sizes were: Graded Shield = 1,985, Icon Expiry = 1,971, Text Expiry = 1,987.

[5] This difference between the graded shield label and the icon expiry label was statistically significant in our pre-registered analysis ($p = .04$, one-sided) with a sample size of 3,956. See the Technical Appendix for further details.

People were more likely to choose devices with higher cyber security levels

We designed each label to have four different levels to indicate increasing degrees of cyber security (Figure 1 in 'What we did'). This meant we could also evaluate the impact of each level of the labels, and test whether people were sensitive to different levels of cyber security. We found the higher the level of cyber security, the more likely participants were to choose a device with that label (see Figure 6).

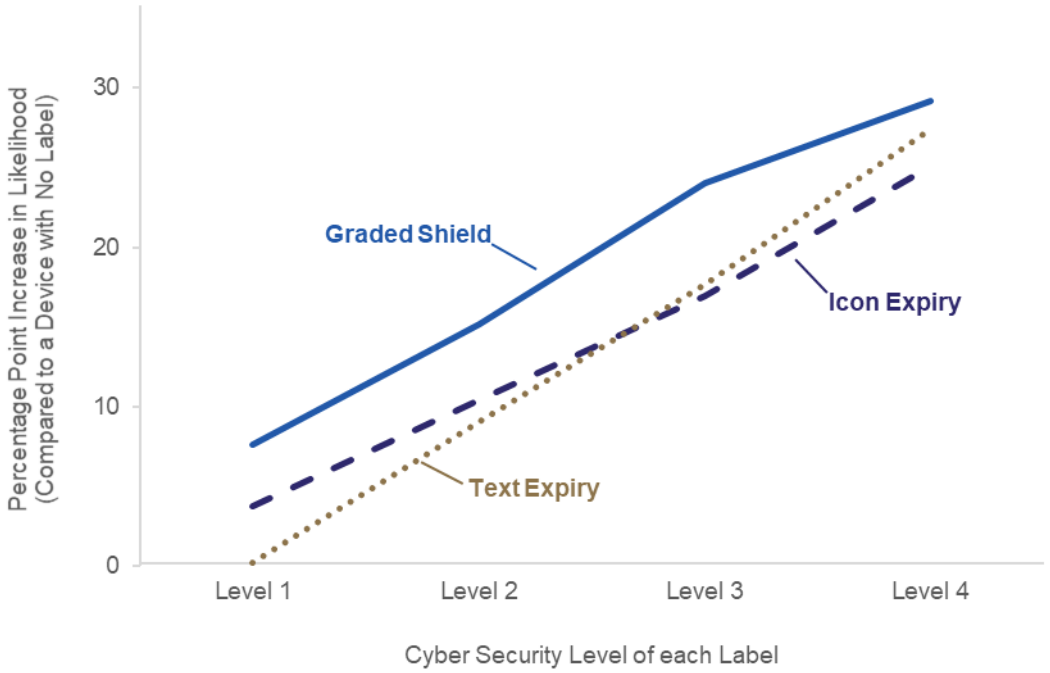


Figure 6. Devices with any label of any level were significantly more likely to be chosen than a device with no label ($p < 0.001$), except for the Level 1 text expiry label which was not more likely to be chosen than a device with no label ($p = 0.782$).[6] The sample sizes were: Graded Shield = 1,985, Icon Expiry = 1,971, Text Expiry = 1,987.

The Level 1 expiry labels stated "Security updates guaranteed until June 2021" (see Figure 1). This date had already passed at the time of the experiment (July 2021), indicating the device may no longer be receiving updates, and consumers should consider seeking out a device with a higher level of cyber security. In the shopping scenario, a device with a Level 1 *plain text* expiry date was *not* more likely to be chosen than a device with no label (indicated by the dotted 'text expiry' line in Figure 6 being at 0 for Level 1). This suggests participants correctly identified the device with this label was no longer guaranteed to receive updates. However, when choosing between a device with no label and a Level 1 *icon expiry* label, participants were 4 percentage points more likely to choose the labelled device (see Figure 6 dashed line Level 1). Taken together, these findings suggest that participants were influenced

[6] These analyses – comparing each level of each label to baseline separately – were pre-registered as secondary analyses.

by the update icon on the label, not just by the actual information communicated by the label. We discuss the implications of this finding further in the discussion section (see pp. 17-18).

People were willing to 'pay' more for a device with a cyber security label

In the discrete choice experiment ('shopping scenario'), participants faced a trade-off between price, product features, and cyber security. This meant we could estimate how much people would be willing to pay for a device with a cyber security label (versus one without a label) for each of the four products in the study. The estimates are summarised in Table 1. Although participants were asked to weigh up the different attributes of the devices as they would in 'real life', they did not actually spend their own money in this study and their willingness to pay may therefore be overestimated. We consider this further in the 'Limitations' section (p. 16).

Table 1. 'Willingness to pay' estimates for cyber security labels

Product	Price range of smart device[a]	Additional amount willing to pay for a device with a cyber security label (vs one without a label)[b]
Smart TV	$1000 - $1800	$322 - $377
Smart watch	$420 - $720	$104 - $123
Home hub	$125 - $225	$53 - $60
Smart light	$30 - $53	$8 - $10

Note: [a]We selected these devices to capture the variability in the 'Internet of Things' market. The price ranges for each smart device is based off research on well-known retailers' webpages. [b]The range given for willingness to pay estimates represents a 95% confidence interval.

Follow-up analyses[7]

The survey component of this study allowed us to examine in more detail how participants engaged with the labels, what they liked about them, and what they potentially misunderstood. Consistent with previous research, our results suggest people intend to take cyber security into account when shopping for smart devices. We asked participants how much they were influenced by the cyber security labels when they completed the shopping scenario, and 35% said they were influenced 'a lot' by cyber security.[8] In response to a separate question, 55% agreed or strongly agreed they would use a cyber security label when shopping for smart devices. However, in both this online study and the real world, cyber security information competes with product features and price – and people have to trade off different attributes to make the choice that suits them. Further follow-up analyses revealed specific advantages and disadvantages of each label and elements of the labels. These are summarised below.

When asked which label they preferred, most participants chose the one they had become familiar with during the shopping scenario

At the end of the study, we showed participants all three label types and asked which one they preferred. Overall, 50% of participants preferred the graded shield label, and 47% preferred the icon expiry label. But, in the group that had seen the graded shield label in the shopping scenario, 70% preferred this label, and among those who had seen the icon expiry label in the shopping scenario, 61% preferred this label, a difference which was statistically significant.[9] This demonstrates the power of repeated exposure (i.e. familiarity) in shaping people's preference (Montoya et al., 2017).

People liked the graded shield, but some participants misunderstood certain aspects

We asked participants a number of true-false questions to test their understanding of the graded shield label. Eighty per cent of participants correctly understood a label with more shield/ticks indicated a device had higher cyber security levels. However, given the shopping scenario was the first time they had seen the label, it is not surprising that participants were also uncertain about the specific meaning of the graded shield and some of its features: Roughly half (49%) thought a device with a single shield 'baseline' label (Level 1) had poor cyber security. As we discussed earlier in this report, Level 1 indicates that a baseline level of cyber security has been achieved (and this may be appropriate for some devices).

Further, almost a quarter of participants thought the graded shield label indicated the device had won a cyber security award (24%), and more than half (56%) mistakenly believed a label with four shield/ticks (Level 4) was four times as secure as a label with a single shield/tick. As explained earlier, it is difficult to measure cyber security on a continuous scale and the label therefore indicates discrete categories of cyber security. Of note, a small proportion (14%) of

[7] See Technical Appendix 2: Survey Instrument and accompanying Statistical Tables for full results.
[8] We asked participants how much they were influenced by cyber security, price, and product features when making their decisions in the shopping scenario. Response options for each attribute were 'a lot', 'a little', and 'not at all'. Consistent with previous research using similar scenarios, participants also said they were influenced by price (57% 'a lot' responses) and product features (46%).
[9] The statistical tests in this section were not included in our pre-analysis plan. All follow-up analyses should be considered exploratory.

participants mistakenly thought ‘a device with this label can never be hacked’. This proportion was slightly higher for higher levels of the label (12% for Level 1, 16% for Level 4), although this difference was not statistically significant. While greater cyber security means it is less likely the device will be hacked, it is *not* true that the device can *never* be hacked.

Both expiry labels were generally well understood, but some participants were uncertain about what the updates covered

Participants also responded to a set of true-false question about both the icon and plain text expiry labels. The vast majority (85%) understood these labels indicated a device would receive security updates until a specific date, and 63% correctly answered that it is false that ‘a device with this label can never be hacked’ – a significantly higher proportion than the 50% who answered this question correctly for the graded shield label.

However, a minority of participants (33%) falsely believed that a device with an expiry label came with an extended warranty until the date on the label, and 20% believed it was ‘true’ that a device would only work until the date indicated by the label.

If either the expiry labels or the graded shield label are implemented, the issues discussed above are likely to dissipate over time as people become familiar with the label and its meaning, particularly if supported by a consumer education campaign.

Limitations

In this project, we aimed to estimate the impact of cyber security labels on people's purchasing decisions when shopping for smart devices. Participants completed a hypothetical shopping scenario (i.e. they compared smart devices with different attributes), and were asked to consider which device they *would prefer*, if faced with such a choice in the real world. However, in an actual shopping situation, people may be faced with additional pressures, or they may not follow through on their stated intentions.

For example, in the present study the smart products were described and displayed in generic terms, and were not branded. We also provided participants with relatively little information about each device, which meant the cyber security information stood out, and the labels were able to grab participants' attention. When purchasing a real smart device in a physical shop or online, other product details, including branding and the colour or design of the device packaging, may also influence a consumer's decision. The plain text expiry label, in particular, seems likely to be overwhelmed by other information on packaging or in a shop. The results in this report may therefore overestimate the impact of cyber security labels when intentions are translated into actual behavior in the real world.

In particular, in the shopping scenario participants were not required to spend their own money. While the results provide a reasonable estimate of how the labels compare to each other (and to no label), we are less confident in how much people would be willing to pay for a given cyber security level (displayed on a given label) once they are facing a real purchase and weighing up their personal circumstances. However, research suggests that discrete choice experiments correctly predict individuals' actions roughly 80 per cent of the time (Fifer et al., 2014; Lambooij et al., 2015; Mohammadi et al. 2017). A recent meta-analysis of differences between real and hypothetical 'willingness to pay' calculations suggests the overestimate may be around 21% (Schmidt & Bijmolt, 2020), given the methods used in this study (see also Murphy et al., 2005).

Finally, participants were not provided any explanation of what the labels meant before they saw and used them in the shopping scenario. If cyber security labels are implemented in Australia, it may be useful to accompany them with explanatory materials (targeted at retailers or the public), providing an opportunity to teach people how to interpret and use the labels.

Discussion

Cyber security labels helped consumers make better purchasing decisions

Compared to a device without a cyber security label, a device with a label was 13 to 19 percentage points more likely to be chosen by participants. Of the three labels we tested, the 'graded shield' label performed the best and participants thought this label was more visually appealing than the two 'expiry' labels. The expiry labels, which displayed the date the device would receive security updates until, also influenced people's purchasing decisions in the shopping scenario. All label types had four levels of cyber security. As expected, people were more likely to choose a device with a higher cyber security rating than a lower one, for all three label types. These results suggest cyber security labels are likely to achieve their aim of helping Australian consumers make more informed decisions about cyber security when purchasing smart devices.

Each label type had different advantages and disadvantages

In addition to having the largest impact in the shopping scenario, the graded shield label was preferred overall, and people generally understood that more shields indicate greater cyber security. However, people were also more likely to misunderstand aspects of this label than the expiry labels. In the shopping scenario the expiry date labels also had a positive impact on people's choices. People generally understood the expiry labels, and the icon expiry label was also well liked. However, almost no one preferred the plain text expiry option. While this label also influenced participants' choices in the shopping scenario, in the real world its influence will depend on consumers noticing the text – and the plain text option may easily be overwhelmed by other details on device packaging.

Consumer education, especially about devices that no longer have guaranteed security updates, could improve real-world outcomes

Participants were not given any explanation of the labels and their meaning before or during the study. If a labelling scheme was introduced in Australia, consumers may benefit from an education campaign to address some of the limitations identified in this study. For example, an education campaign could explain to consumers that a device with a label does not mean it cannot be hacked, that other cyber security measures may still be required (e.g. accepting security updates), and, for the graded shield label, that the four levels indicate discrete categories of cyber security (rather than being a continuous measure).

As outlined in the 'What we found' section, in the shopping scenario participants preferred a device with an icon expiry label (over a device with no label) even when the 'guaranteed updates' date had passed (see Figure 6). This suggests participants were influenced by the icon label itself, not just by the actual information communicated by the label. In their

consultation, Home Affairs sought feedback on a mandatory expiry label. If implemented, consumers in the real world would therefore be unlikely to face a choice between a device with an expiry label versus one with no label. However, consumers may encounter products that have reached or are close to the end of their guaranteed update period, in which case they should be encouraged to seek further information (e.g. from the device manufacturer on whether the device will continue to be updated) to help inform their purchasing decision.

Labels can influence consumers at the point of purchase; influencing decision-making beyond this would require alternative approaches

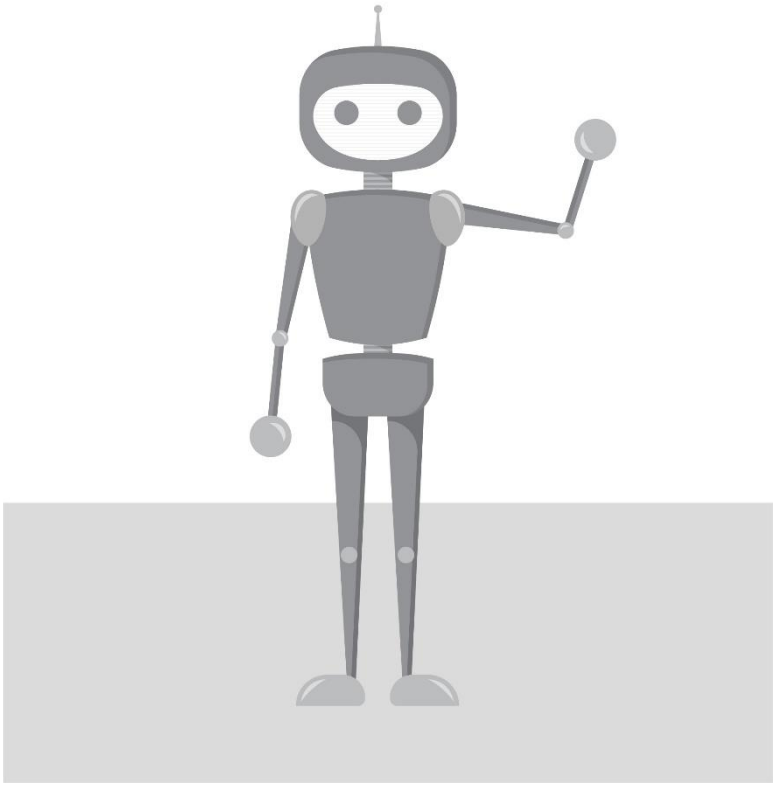
Cyber security labels are intended to influence consumers at the point of purchase (Parkin et al. 2014) and are unlikely to be salient to consumers after this point. Other approaches (e.g. education) may be required to help people decide what to do when the devices they already own no longer receive security updates (e.g. whether they continue to use the device, replace it or dispose of it). In this project, we did not evaluate any additional education materials beyond the labels themselves. While education and informational approaches may be helpful in some settings, more information may not be sufficient to change behaviour (e.g. Allara et al. 2013). Labels are intended to cut through complex information environments and provide quick heuristics for consumers to help guide their decision-making at the point of purchase. The findings in this report suggest labels will help consumers in this situation, and further research – including for example in-depth interviews and exploration of people's decision-making processes – would be required to help understand consumer decisions about devices they already own, that have reached the end of their guaranteed update period.

Australian consumers would benefit from a cyber security labelling scheme, but further research could answer some remaining questions

The results of this project demonstrate the potential for a labelling scheme to improve consumer decision-making in the Australian smart device market. Further research and consumer testing of cyber security labels could enable greater understanding of how people are likely to interpret and make use of labels on their actual smart devices. As international labelling schemes are rolled out and tested (e.g. in Singapore, Cyber Security Agency of Singapore, 2021), their progress and experiences are likely to provide useful lessons which could be drawn on if a labelling scheme was implemented in Australia. Looking further ahead, evaluating the labels in the field – for example through partnering with a retailer and evaluating the impact of cyber security labels on real choices made by actual consumers – could also be considered to test how the current findings translate to a real-world context.

Australian Government
Department of the Prime Minister and Cabinet

BETA



Technical Appendix

Stay Smart

December 2021

Contents

Appendix 1: Technical Details

Pre-registration, pre-analysis plan, and ethics

This trial was publically pre-registered on the AEA registry, record number AEARCTR-008044. The pre-registration plan was also documented on the BETA website. Registration took place before we launched the trial or analysed the data. Our analyses were consistent with our pre-analysis plan. The pre-analysis plan is published on the BETA website as a supplement to the report.

The project was approved through BETA's ethics approval process, with risk assessed by Macquarie University in accordance with the guidelines outlined in the National Statement on Ethical Conduct in Human Research.

Population and sampling

Our population of interest was all Australian adults, as anyone is a potential consumer of smart devices. We recruited participants who were 18 years old and over. We did not have any exclusion criteria, but we requested that participants complete the study on laptop or desktop devices (i.e. not mobile devices), as the experimental task looked better and was easier to complete on a larger screen. Our sample was recruited by Dynata, who incentivised participants. Dynata describe their incentivisation process as follows: 'Panellists are rewarded for taking part in surveys according to a structured incentive scheme, with the incentive amount offered for a survey determined by the length and content of the survey, the type of data being collected, the nature of the task and sample characteristics. (…) All incentives are awarded only once the survey has been completed. The incentive options allow panellists to redeem from a large range of gift cards, points programs, charitable contributions, and partner products or services.'

We recruited with interlocking quotas on age (three bands: 18-34, 35-54, and 55+) and gender, in order to have a broadly nationally representative sample on these dimensions. We also aimed to match national proportions for location (state). We administered the quotas in-house using the online Qualtrics survey platform.

Our target was a sample of 6,000 participants, and after filtering out people who did not complete the study our final sample size was 5,943. The sample was close to nationally representative on our quota variables. Demographics of the sample are included in Table 2.

Table 2. Sample characteristics

Category		Number (%)
Gender	Women	2,962 (50)
	Men	2,934 (49)
Age	Younger (18-34 years)	1,893 (32)
	Middle (35-54 years)	1,882 (32)
	Older (55+ years)	2,121 (36)
Location	Victoria	1,501 (25)
	New South Wales	2,101 (35)
	Queensland	1,082 (18)
	Other	1,255 (21)
Income	Under $26,000	1,599 (27)
	$26,000 - $65,000	1,953 (33)
	$65,000 - $91,000	878 (15)
	Above $91,000	1,004 (17)
Education	Less than secondary education	122 (2)
	Secondary education	1,349 (23)
	Certificate level I, II, III, IV; Diploma or advanced diploma	1,730 (29)
	Bachelor degree	1,475 (25)
	Graduate diploma or graduate certificate	287 (5)
	Postgraduate degree	849 (14)
Language other than	No	5,055 (85)
English at home	Yes	719 (12)

Note: Proportions do not all sum to 100% as not all individuals responded to all questions, and a number of "other" and "prefer not to say" responses are excluded from this table. N = 5,943

Randomisation

Using the Qualtrics survey platform we randomly allocated participants to one of the three label conditions (plain text expiry, icon expiry label, graded shield rating label). Participants initially had equal probability of being assigned to each cell, but Qualtrics increased the probability of assignment to the cell with the lowest sample size to ensure even cell sizes. We also randomly allocated participants to 'shop' for one of four smart products (smart TVs,

smart lights, home hubs, or smart watches), which meant that the study had a total of 12 cells. However, we focus on the three experimental conditions here.

The final sample size of each cell ranged from 1,971 to 1,987 participants. The characteristics of the sample in each cell are summarised in Table 3 on the next page.

Sample size and power calculations

These power calculations were originally reported in our pre-analysis plan. We conducted power calculations for the RCT component of the research project only (see Method of Analysis for further details).

Due to resource and timing constraints, our sample was fixed at around 6,000 individuals, which provided 2,000 individuals per experimental condition (label type). Each individual responded to 10 choice sets. To account for repeated measures, we clustered our standard errors by individual. Individual preference for selecting a labelled device over a non-labelled device is likely to be highly correlated across an individual's 10 choice sets. For the sake of these power calculations, we therefore assumed an ICC of 1. This is very conservative with any reduction in this correlation reducing the minimum detectable effect at a given power level/sample size. For this study, alpha was set to 0.05, and beta to 0.2, and hypothesis tests were one-sided.

With these assumptions in place, for H1a and H1b, which both relate to the RCT component (see below), we estimated that our design could detect a standardised effect of 0.08 (Cohen's *h*) with 80% power, this corresponds to approximately a 4 percentage point increase from a conservative 50% baseline.

Outcome measures

RCT component

The primary outcome measure for the RCT component was whether, for each choice set**, an individual chose to 'buy' a device with a cyber security label (coded as '1')** or one without a label (coded as '0'). We calculated sample proportions from this binary measure.

The secondary outcome measure for the RCT component was, for each choice set, the level of cyber security of the device the individual chose to 'buy'. The level was treated as a continuous variable from 0 (no label) to 4 (Level 4 label). That is, if an individual chose a device with no label, they got a 'score' of 0 for that choice set. If they chose a device with a Level 1 label, they got a 'score' of 1, and so on.

Discrete Choice Experiment (DCE) component

The primary outcome measure for the DCE component was the device each individual chose to 'buy', in each of ten choice sets (each choice set contained three variations on a single device – e.g., watch or TV). Each device was coded as '1' if it was purchased, and as '0' if it was not purchased. For the DCE component we also calculated 'willingness to pay' for cyber security labels.

See pre-analysis plan for further details on outcome construction.

Table 3. Sample characteristics by treatment condition

Grouping Variable	Condition	Plain text expiry N (%)	Icon expiry label N (%)	Graded shield label N (%)
Gender	Men	983 (50)	966 (49)	985 (50)
	Women	987 (50)	994 (50)	981 (49)
Age	Younger	655 (33)	642 (33)	628 (32)
	Middle	634 (32)	626 (32)	633 (32)
	Older	698 (35)	703 (36)	724 (37)
Location	VIC	518 (26)	480 (24)	503 (25)
	NSW	708 (36)	693 (35)	700 (35)
	QLD	328 (17)	391 (20)	363 (18)
	Other	432 (22)	405 (21)	418 (21)
Personal income	Under $26,000	530 (27)	527 (27)	542 (27)
	$26,000 - $65,000	653 (33)	668 (34)	632 (32)
	$65,000 - $91,000	303 (15)	276 (14)	299 (15)
	Above $91,000	330 (17)	334 (17)	340 (17)
Education	Less than secondary education	41 (2)	36 (2)	45 (2)
	Secondary education	445 (22)	456 (23)	448 (23)
	Certificate level I, II, III, IV; Diploma or advanced diploma	573 (29)	567 (29)	590 (30)
	Bachelor degree	519 (26)	464 (24)	492 (25)
	Graduate diploma or graduate certificate	92 (5)	94 (5)	101 (5)
	Postgraduate degree	266 (13)	306 (16)	277 (14)
Language other than English at home	No	1680 (85)	1693 (86)	1682 (85)
	Yes	248 (13)	227 (12)	244 (12)
Total Population		**1987 (100)**	**1971 (100)**	**1985 (100)**

Hypotheses

In our pre-analysis plan, we specified two hypotheses in relation to our primary outcome. We report the results relevant to all these hypotheses in the main report, and the full regression outputs in excel documents available at https://behaviouraleconomics.pmc.gov.au/projects/stay-smart-helping-consumers-choose-cyber-secure-smart-devices.

Randomised controlled trial

H1a: People in the icon expiry label group will choose a greater proportion of devices with labels than people in the expiry plain text group (B > A, one-tailed test).

H1b: People in the graded shield label group will choose a greater proportion of devices with labels than will people in the icon expiry label group (C > B, one-tailed test).

For H1 we will pool the data from the four product categories.

Discrete choice experiment

H2: The presence of a cyber security label (versus no cyber security label) will increase people's likelihood of purchasing a given device (one-tailed test). We will conduct this (conjoint) analysis separately for the three label types (A, B, C), pooling the four product categories.

Method of analysis

All data processing and analysis was performed using R (version 4.1.1, R Core Team, 2020) with the dplyr package (version 1.0.3; Wickham, François, Henry & Müller n.d.), lme4 (version 1.1.27.1, Bates, Maechler, Bolker & Walker, 2021), lmerTest (version 3.1.3, Kuznetsova, Brockhoff, Christensen & Jensen, 2020), in R Studio (RStudio Team, 2020).

As stated in our pre-analysis plan, there were two components to this research: an RCT component, and a discrete choice experiment (DCE) component.

For H1, which stemmed from the RCT component of this research, we fitted an OLS regression with cluster-robust standard errors. Choice of a device with vs without a label (1 vs 0) was regressed on a binary treatment indicator (type of label coded depending on which comparison we are making). There were no covariates. We fitted this model only to the subset of the data that was relevant to the comparison we were making (graded shield and icon expiry labels for H1a, icon expiry label and plain text expiry for H1b). We pooled product categories. For Secondary Hypothesis 3, we fitted the same models but used the continuous secondary outcome measure.

For H2, which stemmed from the DCE component of this research, we fitted a mixed-effects linear regression. Choice of device (0 vs 1) was regressed on a binary treatment indicator (0 = no label, 1 = any label), a binary indicator for feature level (0 = standard, 1 = premium), and a continuous variable for price, mean-centred. We specified random slopes for treatment (label) and feature level, by individual. The random slopes were modelled as uncorrelated. We fitted this model separately for each label type, but pooled product categories. For Secondary Hypothesis 4, we fitted the same models but used dummy codes for each level of the labels. Although we had implied in our pre-registration (by not specifying otherwise) that we would include a random slope for treatment and feature level also for these secondary analyses, we included only a random slope for feature level.

Including random slopes for each level of the labels (treatments) was too computationally intensive. This as the only departure from our pre-analysis plan.

We also conducted a number of robustness check by fitting alternative models. A summary of these models is available on request.

Use of p-values

We have made use of *p*-values to aid the interpretation of our results. However, we also consider the *p*-value together with effect size, robustness checks and design limitations to assess the strength of a finding.

Statistical tables underpinning the findings

The full set of statistical tables and analyses underpinning the findings presented in this report are provided in separate excel documents available at https://behaviouraleconomics.pmc.gov.au/projects/ stay-smart-helping-consumers-choose-cyber-secure-smart-devices. The only exception is participants' responses to an open-ended question about the labels, which are summarised below.

Free text responses

We also asked a subset of participants (20% of the total sample) a single open-ended question about what they thought the cyber security label they saw in the shopping scenario meant ("In your own words, please tell us what you think this label tells you.") We undertook an **informal analysis** of responses to this question, summarised below.

Roughly 1,100 participants gave interpretable responses to this question. A majority of these participants correctly thought the label indicated how long a device would receive updates, or the 'level' of cyber security as mandated by the government – responses differed by whether they saw the expiry or graded shield label.

There were also a portion of the free text responses that said they found the label confusing, or 'don't know' what it told them. Given the small number of responses overall, this may be a biased sample. Of note was a subset of participants who thought the labels indicated a warranty period for the device. There were also a proportion of participants who expressed that a label could only indicate cyber security, and that a device was still vulnerable to cyber security threats. These responses were given before the true-false section of the report, so participants were not primed.

Appendix 2: Survey Instrument

The survey instrument consisted of three parts:

- **Part 1:** the screener, containing background information for participants (including the consent form), a few demographic question, and randomisation
- **Part 2:** the ‘shopping scenario’ (discrete choice experiment, DCE), in which participants chose one of three devices, ten times
- **Part 3:** additional survey questions, and a few extra demographic questions

Parts 1 and 3 are reproduced verbatim below. We’ve also provided screenshots of the shopping scenario (for Part 2), to give an impression of how the DCE worked.

Part 1: Screener

The full text of the screener is included below. Where response options were quite verbose, we have summarised the options in square brackets.

First, we have a few questions about you to make sure you're eligible for this study.

[*age*] How old are you?

[Response options were Up to 17 years, 18-24, then five-year spans until 65-69, then 70 years or older.]

[*gender*] What is your gender?

- Man or male (1)
- Woman or female (2)
- Non-binary (3)
- I use a different term (please specify) [open text box] (4)
- Prefer not to say (5)

[*location*] Where do you live?

- Australian Capital Territory
- New South Wales
- Northern Territory
- Queensland
- South Australia
- Tasmania
- Victoria
- Western Australia

Part 2: Shopping Scenario

Participants were randomly assigned to ‘shop’ for one of four smart product types (smart TV, smart lights, home hubs, or smart watches). They were also assigned to one of three experimental conditions (i.e. three label types). All participants received the same initial introductory text, formatted with background colour and bolding to make it more visually engaging (formatting not shown here).

Page 1

On the next few screens, we’ll ask you to imagine you're shopping for a new smart device. You’ll be provided with information about the features and prices of range of smart devices.

We’ll show you three smart devices at a time. Assuming the devices were available for purchase, please compare the options and choose which one you'd prefer to buy.

You'll also be able to opt not to ‘buy’ any of the devices shown if you don’t find any suitable. Please try to choose from one of the three options and only choose not to 'buy' if you really can't decide.

We’ll ask you to do this 10 times. We’ll then finish by asking you a few questions about the information you saw. The whole task should take you around 10-15 minutes.

When you’re ready to start, please click >> below.

Page 2

Before you 'shop' for smart devices, we want to ask you to help us with a problem we have in studies like this one. Because people don't actually have to pay for the products in this study, they often don't pay much attention to the actual cost shown. Instead, they might just notice that one cost is larger than another.

For example, if the cost of the products in the questions are $100, $120, $150 and $200, people often think of them as just 'very low', 'low', 'medium', and 'high'.

They don't really think about what they would have to give up out of their monthly budget - such as a take-away meal or some new clothes - if they actually bought the product. If people don't pay attention to the actual costs, our analysis will be wrong, and we won't get a true measure of the value of smart devices.

Please help us measure your preferences correctly by paying attention to the actual costs of the products before deciding which one of the three options you prefer.

Thank you!

Page 3: On the third page, participants were given a brief description of the type of product they would be shopping for. Each description was accompanied by a photo (not included here). Each participant saw only one *of the following descriptions.*

Smart lights

Imagine you're shopping for SMART LIGHTS.

Smart lights create instant ambience for any occasion. You can control your lights and dim or change their colour via an app, even if you're not in the same room.

Some smart lights can even be programmed with automatic schedules so you can coordinate your lights with your daily routine.

When connected to a compatible home hub, your smart lights can also be voice-controlled and you won't have to lift a finger.

Smart lights range from about $20 to more than $100 in price.

On the next pages, we'll ask you to choose from a range of smart lights.

Remember to try to choose one of the three smart lights and only opt not to 'buy' if you really can't decide.

Please click >> when you're ready to continue.

Smart TV

Imagine you're shopping for a SMART TELEVISION.

Smart televisions connect to the internet and can support your favourite apps, streaming services, games, and social media.

Many smart TVs also have the latest audio and display features, offering a richer sound experience and vibrant images in ultra-high resolution.

If connected to a smart speaker or home hub, smart TVs can also be voice-controlled.

Smart TVs range from about $200 to more than $5,000 in price.

On the next pages, we'll ask you to choose from a range of smart TVs.

Remember to try to choose one of the three smart TVs and only opt not to 'buy' if you really can't decide.

Please click >> when you're ready to continue.

Home hubs

Imagine you're shopping for a HOME HUB.

Home hubs connect to and control other smart devices in your home. Your smart devices interact with each other via a single app – so you have everything collected in one convenient location.

You can ask your home hub to play music or check your mail via voice control.

Some home hubs let you set up automatic schedules to control your other devices, like lights or thermostats.

Home hubs range from about $70 to more than $300 in price.

On the next pages, we'll ask you to choose from a range of home hubs.

Remember to try to choose one of the three home hubs and only opt not to 'buy' if you really can't decide.

Please click >> when you're ready to continue.

Smart watches

Imagine you're shopping for a SMART WATCH.

Smart watches give you instant access to a range of apps and features all on your wrist. You can receive notifications or tap to pay for purchases without getting your phone out of your pocket or bag.

Like to keep track of your fitness? Smart watches are great for activity tracking, logging your steps, calories, workouts, and heart rate.

Smart watches range from about $200 to more than $1,000 in price.

On the next pages, we'll ask you to choose from a range of smart watches.

Remember to try to choose one of the three smart watches and only opt not to 'buy' if you really can't decide.

Please click >> when you're ready to continue.

Discrete choice experiment task

In the discrete choice experiment, participants were presented with 10 choice sets. Each choice set included three devices (e.g. three smart watches; three smart TVs), as illustrated in Figure 7.

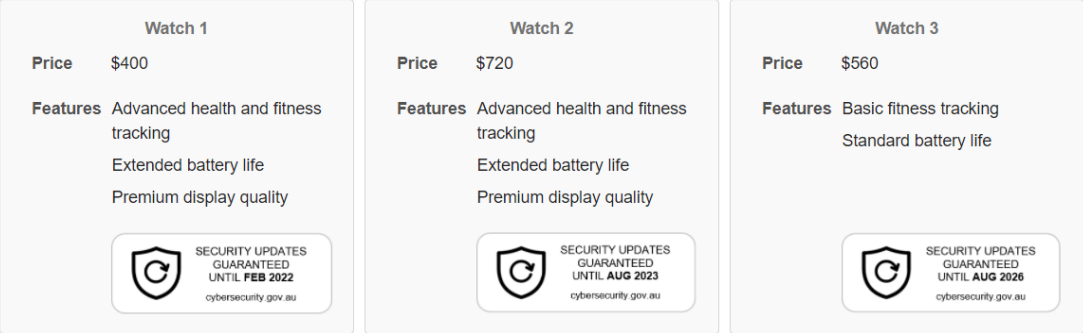


Figure 7. Screenshot of a choice set for the smart watches, in the icon expiry label condition, illustrating a range of prices, product features, and three different levels of cyber security. There was also an option to select "none of these".

The devices randomly varied on three attributes: price, product features (standard vs premium), and cyber security label (Levels 1-4, or absent). The specific price ranges and features of each product type is displayed in Table 3.

Table 4. Summary of the attributes of the four different product types.

Product type	Lightbulb	Home hub	Watch	Television
Price levels	$30, $36, $42, $48, $54	$125, $150, $175, $200, $225	$400, $480, $560, $640, $720	$1000, $1200, $1400, $1600, $1800
Standard features	Warm-to-cool white light	Connect up to five devices Standard speaker quality	Basic fitness tracking Good battery life	HD screen
Premium features	Multiple light colours Automatic scheduling Compatible with Apple HomeKit, Amazon Alexa, and Google Assistant	Connect up to ten devices Automatic scheduling Premium speaker quality	Advanced health and fitness tracking Extended battery life Premium display quality	Ultra HD (4K) screen Fast processor for lag-free viewing Integration with Google Assistant, Amazon Alexa, and Apple HomeKit

Note: Each participant 'shopped' for only one of the four product types. In each of 10 choice set, they were shown three devices of the same type, which varied in price (five levels), features (standard or premium) and cyber security level (not shown in this table). We used Qualtrics survey software to set up the discrete choice experiment. We specified the attributes, how many levels of each attribute, how many choice sets, and how many options in each choice set. On the basis of these specifications, Qualtrics then generated a D-efficient experimental design, which determined exactly which combination of attributes each participant saw in each choice set.

Participants were asked to choose one of the three options, but could select "none of these" if they were unable to choose.

Each choice set was displayed on a separate page, and numbered 1-10. After completing 5 choice sets, participants were shown a screen saying “You’re halfway through – just five more to go!”

After completing the 10 choices, participants were told: “Thank you for your attention - you have just completed Part 1 of this study. We now have some questions about the information you saw earlier.”

Part 3: Additional survey questions

Part 3 contained the additional survey questions. Part 3 is reproduced verbatim below, with commentary in square brackets.

Page 1

Question 1

The smart devices you looked at earlier varied in features, cyber security, and price.

Thinking about your choices overall, to what extent did each of these attributes influence your decisions?

Product features/Cyber security features/Price

[Attributes were displayed in a random order, and each attribute was rated as “did not influence me at all,” “influenced me a little,” or “influenced me a lot”.]

Page 2

Question 2

Here is a review of the four different [statements/labels] you saw on the smart devices earlier in this study: [depending on the experimental conditions, participants saw all four levels of the graded shield label or the icon expiry label, or all four levels of the plain text expiry (statements)]

Please tell us how much you agree or disagree with the following [6-point scale from strongly disagree to strongly agree]:

- The [statements/labels] are appealing
- The [statements/labels] are easy to understand
- The [statements/labels] have too much information
- The [statements/labels] would make it easy to compare products
- I would use this type of [statement/label] to help me when buying a product

[The first four statements were listed in a random order; the fifth was always listed last]

Page 3: This page was displayed only to 20% of the sample, because free text is more time consuming to analyse. The page again displayed all four of the cyber security labels/statements participants had seen earlier in the study.

Question 3
In your own words, please tell us what you think the [labels/statements] above tell you. [free text]

Page 4

Question 4

Different smart devices – like the ones you've seen in this study – can differ in how cyber secure they are. Some devices might have minimal or no security, other devices have very strong security.

If the following words were used to describe a device's level of cyber security, how strong do you think the security would be for that device?

There's no right or wrong answer, we're just interested in how 'strong' you think each word is.

[Words were listed in a random order, and each word was rated from 0 = no security to 5 = very strong security. The bolded words below are ones that appeared on the graded shield cyber security labels – they were not bolded for participants in the study.]

- **Baseline**
- Basic
- Above Baseline
- **Intermediate**
- **Enhanced**
- Strong
- Advanced
- **Hardened**

Page 5: on this page participants were asked a range of true-false questions about a label. At the top of the page they were shown the label type they saw in the DCE, but only one (randomly selected) level (from 1 to 4). The specific question they are asked depended on whether they saw the graded shield label or one of the two expiry labels.

Question 5

Graded shield label [response options: True/False/I don't know]:

Please tell us whether you think the following sentences about the label above are **true** or **false.**

A device with…
… this label can never be hacked
… more shields has more product features than one with fewer shields
… more shields means the device has stronger cyber security than one with fewer shields
… a 'baseline' label and one shield has poor cyber security
… this label has won a cyber security award
… a label with four shields is four times as secure as one with a label with one shield

Expiry labels/statements [response options: True/False/I don't know]. The [date] in the question below corresponded to the date displayed on the label.

Please tell us whether you think the following sentences about the [labels/statements] above are **true** or **false.**

A device with this [label/statement]…

… can never be hacked
… will receive security updates until [date]
… comes with an extended warranty until [date]
… is unsupported after [date]
… will only work until [date]

Page 6: This question, about people's preference for one of the three labels, was accidentally left out when we launched the study. We realised when we were about 2/3 of the way through data collection, and added it then. For this reason, only 1456 people responded to this question.

Cyber security might be presented in different ways in a label on new smart devices. Of the following, which one do you prefer?

[*One level of all three label types were displayed. The level was randomly assigned to each participant, but was the same for all three labels*.]

Page 7: Outro

Thank you for your time so far! This is the last page - just three more quick questions about you.

What is your total personal income before tax, per week (per year)? [Brackets taken from ABS census, starting at "Nil income" and increasing to "$4,000 or more per week ($208,000 or more per year)". We also included a "prefer not to answer" response option.]

What is the highest level of education you have completed?

- Less than secondary education
- Secondary education
- Certificate level I, II, III, IV
- Diploma or advanced diploma
- Bachelor degree
- Graduate diploma or graduate certificate
- Postgraduate degree
- Prefer not to say

Do you speak a language other than English at home? No, English only / Yes, other (please specify) [open text box] / Prefer not to say

Thank you for completing this study! If you have any last comments for us, including if you had any technical problems with the study, please tell us below. When you click >> you will be redirected back to the panel provider. [open text box]

References

Allara E, Ferri N, Bo A, Gasparrini A, and Faggiano F (2015). 'Are mass-media campaigns effective in preventing drug use? A Cochrane systematic review and meta-analysis', *BMJ Open, 5,* 1-10.

Argo JJ and Main KJ (2004). 'Meta-Analyses of the Effectiveness of Warning Labels', *Journal of Public Policy & Marketing, 23*(2): 193-208.

Australian Certified Organic (2018) Labelling and Logo Style Guide, accessed 18 October 2021.

Bates D, Mächler M, Bolker B, Walker S (2015). "Fitting Linear Mixed-Effects Models Using lme4." *Journal of Statistical Software*, **67**(1), 1–48. doi: 10.18637/jss.v067.i01.

Blythe J M, Sombatruang N, and Johnson SD (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? *Journal of Cybersecurity, 5*(1), 1-10.

Boelhouwer E, Davis J, Franco-Watkins A, Dorris N, and Lungu C (2013). 'Comprehension of hazard communication: Effects of pictograms on safety data sheets and labels', *Journal of Safety Research,* 46: 145-155.

Bossaerts, P., & Murawski, C. (2017). Computational complexity and human decision-making. *Trends in Cognitive Sciences, 21*(12), 917-929.

Cyber Security Agency of Singapore (CAS) (2021) Cybersecurity Labelling Scheme - For Consumers, accessed 18 October 2021.

Data61 (2020). *Results of the IoT Consumer Focused Survey: Internet of Things (IoT) Consumer Research*. [unpublished report] Prepared for the Cyber Security Cooperative Research Centre.

Department of Home Affairs (2021a) '*Strengthening Australia's cyber security regulations and incentives: Discussion Paper',* [online document], Home Affairs, accessed 29 September 2021.

Department of Home Affairs (2021b) '*Strengthening Australia's cyber security regulations and incentives: Annex A',* [online document], Home Affairs, accessed 29 September 2021.

Emami-Naeini P, Agarwal Y, Cranor LF and Hibshi H (2020.) Ask the Experts: What Should Be on an IoT Privacy and Security Label? In *2020 IEEE Symposium on Security and Privacy (SP)* 447-464, IEEE.

Fifer S, Rose J, and Greaves S (2014). 'Hypothetical bias in Stated Choice Experiments: Is it a problem? And if so, how do we deal with it?' *Transportation Research Part A: Policy and Practice, 61*, 165-177.

Gigerenzer, G., & Gaissmaier, W. (2011). Heuristic decision making. *Annual Review of Psychology, 62*, 451-482.

Harris Interactive (2019*).* '*Consumer Internet of Things Security Labelling Survey Research Findings*,' report prepared for the UK Government Department of Digital, Culture, Media & Sport.

Heart Foundation (2021). The Heart Foundation Tick, accessed 18 October 2021.

Johnson SD, Blythe JM, Manning M, and Wong GT (2020). 'The impact of IoT security labelling on consumer product choice and willingness to pay', *PloS one*, *15*(1), e0227800.

IP Australia (n.d.) C-Tick Mark, accessed 18 October 2021.

Kuznetsova A, Brockhoff PB, Christensen RHB (2017). "lmerTest Package: Tests in Linear Mixed Effects Models." *Journal of Statistical Software*, **82**(13), 1–26. doi: 10.18637/jss.v082.i13.

Lambooij MS, Harmsen IA, Veldwijk J, de Melker J, Mollema L, van Weert YWM, and de Wit GA (2015). 'Consistency between stated and revealed preferences: a discrete choice experiment and a behavioural experiment on vaccination behaviour compared'. *BMC Medical Research Methodology, 15*(1), 1471-2288.

Malan J, Eager J, Lale-Demoz E, Cacciaguerra Ranghieri G and Brady M (2020). '*Framing the nature and scale of cyber security vulnerabilities within the current consumer Internet of Things (IoT) landscape',* Centre for Strategy & Evaluation Services, Kent, UK.

Marrapese P (2020). 'Security cameras vulnerable to hijacking', available at https://hacked.camera/, accessed 27 September 2021.

Mohammadi T, Bansback N, Marra F, Khakban A, Campbell JR, FitzGerald JM, Lynd LD, and Marra CA (2017). 'Testing the External Validity of a Discrete Choice Experiment Method: An Application to Latent Tuberculosis Infection Treatment'. *Value in Health, 20*(7), 969-975.

Montoya, R. M., Horton, R. S., Vevea, J. L., Citkowicz, M., & Lauber, E. A. (2017). 'A re-examination of the mere exposure effect: The influence of repeated exposure on recognition, familiarity, and liking.' *Psychological Bulletin, 143*(5), 459-498.

Murphy, J. J., Allen, P. G., Stevens, T. H., & Weatherhead, D. (2005). A meta-analysis of hypothetical bias in stated preference valuation. *Environmental and Resource Economics, 30*(3), 313-325.

Parkin, S, Redmiles, EM, Coventry, L, and Sasse, MA. (2019). 'Security when it is welcome: Exploring device purchase as an opportune moment for security behavior change.' In *Proceedings of the Workshop on Usable Security and Privacy (USEC'19)*. Internet Society: San Diego, CA, USA.

Pieters R, Warlop L, and Wedel M (2002) 'Breaking through the clutter: Benefits of advertisement originality and familiarity for brand attention and memory', *Management Science, 48*(6), 765-781.

R Core Team (2021). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. URL https://www.R-project.org/.

RStudio Team (2020). RStudio: Integrated Development for R. RStudio, PBC, Boston, MA URL http://www.rstudio.com/.

Schmidt, J., & Bijmolt, T. H. (2020). Accurately measuring willingness to pay for consumer goods: a meta-analysis of the hypothetical bias. *Journal of the Academy of Marketing Science*, *48*(3), 499-518.

Wang A (2018). '"I'm in your baby's room": A hacker took over a baby monitor and broadcast threats, parents say', *The Washington Post,* accessed 28 September 2021.

Wickham H, François R, Henry L and Müller K (2018). dplyr: A Grammar of Data Manipulation. R package version 1.0.3. https://CRAN.R-project.org/package=dplyr

Wilson, EJ and Sherrell, DL. (1993). 'Source effects in communication and persuasion research: A meta-analysis of effect size.' *Journal of the academy of marketing science*, *21*(2), 101-112.

ISBN 978-1-925364-90-3
Stay Smart: Helping consumers choose cyber secure smart devices (online)

Australian Government

BETA

Behavioural Economics Team of the Australian Government

General enquiries beta@pmc.gov.au

Media enquiries media@pmc.gov.au

Find out more https://behaviouraleconomics.pmc.gov.au/