IAAC People-Centric Information Assurance research

Paper 7 - People's role in fending for themselves online

Results from IAAC's PCIA workshop of 12 October 2010

The aim of the current PCIA research is to understand how to help people fend for themselves online. By "fend for themselves online" we mean people doing whatever it is they need to do so that they can feel safe doing the things they want to do online. It includes behaving sensibly and taking appropriate precautions.

The objective of this workshop was to broaden and deepen our understanding of people's attitudes to digital safety and security, to explore what role and responsibilities people have for their own safety online, and to suggest ways people can be helped to take these on.

Disclaimer: This report is not a record of the workshop discussion. It is, as with previous workshop reports, a digest of the many insightful points made in, and arising from, the discussion. The ideas expressed in this report should not be taken to represent the views of any individual IAAC member or sponsor.

Key messages

1. There is no fixed set of behaviours that people need to follow to stay safe online. Objectively what people need to do will vary from situation to situation. On top of that, what each person thinks they need to do will vary from person to person, as it does for any other type of personal risk. Despite having been around for a long time, the idea that there should or could be a fixed set of behaviours that people need to follow to stay safe online does not stand up to scrutiny.
2. It follows from this that people need to learn to make their own decisions regarding the way they behave and the things they do. Decisions like these are not made by people based on any objective measure of the actual or general level of risk they face. They are made based on the individual's personal perceptions of, and attitudes towards, the risks they are taking. These decisions can be informed by specific safety rules and guidelines but cannot be prescribed by them. Therefore, if people are to behave safely online it is their perceptions and attitudes that are the keys and that need to be addressed. It is not sufficient just to try to improve the public's knowledge of safety rules and best practice behaviours.
3. Perceptions include the understanding people have of the digital threats around them and the harm those threats can cause. People seem well aware of the existence of digital threats such as malware, cybercrime and poor data handling practices, and typically believe that these are widespread. However, their behaviours suggest that they do not tend to believe the risks from these are particularly significant. They tend to believe that any harm they might be caused by any of these threats is likely to be minor.
4. People's behaviours suggest that most people do not consider digital security and safety to be particularly important issues. Many people seem more concerned about convenience than safety, and often seem prepared to trade in some of their safety or security for no more than a relatively low value reward.
5. Many people see digital safety and security as a complicated technical matter. Perhaps for that reason it is common for people to see the job of making the digital world safe the responsibility of others, e.g. manufacturers, providers and the Government, not something they personally have a role to play in. Changing this attitude is essential if people are to learn to fend for themselves online. One way in which this attitude could be changed is discussed in the body of this report.
6. People have a role to play in keeping themselves safe online and they have responsibilities that go with that role. That role (which is described in the body of this report) is not to become a master of digital

safety and security, and the responsibilities that go with that role do not require them to have any specific technical understanding of the digital devices they use. Most people should be able to fulfil this role and their responsibilities without any difficulty. A lack of technical knowledge or shortage of digital expertise is no barrier to people being able to discharge their responsibilities in full.

7. People need help to build up a realistic general understanding of how safe or unsafe the digital world can be. This can be achieved using analogies drawn from the physical world. They then need to be made familiar with the types of situation they might face online and the problems and consequences that could arise. The media would be well placed to help in this regard.

8. Next comes helping people develop situational awareness. Situational awareness is the ability to recognise the key threats, risks and dangers one is exposing oneself to in each situation that arises. In the physical world, people develop situational awareness through the warning cues they receive from the world around them. In the digital world, many of these warning cues are missing. New thinking is required, from product and service providers primarily, so people can be provided with the warning cues they need. A number of suggestions are given within this report.

9. The main skill people need to develop is one that could be called 'digital common sense': the ability to make sensible choices regarding how to act and how to protect themselves for each situation they find themselves in. To help people make the right choices they need to be given a mix of both general guidelines and specific instructions. Importantly, they need this advice to be sensible, appropriate and consistent regardless of its source. Often, the advice people are given today does not live up to these requirements. As a result, people get confused and do not know which approaches are safest. Clearer thinking and better cooperation between advice providers would help people learn what is safe and to make better choices.

Discussion

What it takes to keep oneself safe online

1. The findings from earlier PCIA workshops[1] indicate that, on the whole, the digital world is reasonably safe. This is not to say that the digital world is completely safe, or ever will be completely safe. It is saying that, provided people pay attention behave sensibly and take appropriate precautions, the digital world can be safe enough to allow them to do all the things they want to do online.

2. What people need to do to keep themselves safe online will vary from situation to situation. Just as some city streets are less safe to walk down at night than others, some places on the Internet are less safe to visit than others. Just as some physical activities attract a higher physical risk for the participant than others, some online activities (e.g. peer-to-peer file sharing) attract a higher digital risk than others. Hence, behaviours that might seem sensible in some digital spaces might not be so sensible in others. Precautions that might seem unnecessary in some digital spaces might be essential in others.

3. Significantly, what people need to do to keep themselves safe online will also vary from person to person.

   If people were all of a similar mind and accepted a common view of the risks, then maybe it would be possible for everyone to stay safe simply by adhering to a digital equivalent to the Highway Code. This Digital Highway Code could contain a set of general behavioural principles for all people to follow so most problems could be avoided (e.g., defining who has right of way at information junctions where different parties' interests could collide). It could tell people what warning signs to look out for so they could take extra care when negotiating their way through the more dangerous places on the Internet.

[1] Primarily PCIA workshops 5 (29 April 2010) and 6 (14 July 2010), but see also the reports from the earlier workshops

And it could describe the steps people should go through should they become involved in a digital accident or become a victim of cybercrime.

However, people are not all of a similar mind. Different people will have different views of the risks they face online and make different decisions about how to behave and which precautions to follow. This is the same as they would do for any other type of personal risk. Some people are comfortable taking more risk in their daily physical lives than others who are, by their nature, more cautious. Similarly, some people will be comfortable taking more risk in their daily digital lives.

4. Unlike driving on the roads, there is no need to require people's digital behaviours to conform to a fixed set of standard patterns. People can be allowed to make their own decisions on how they behave and on what precautions they need to take to stay safe. Despite having been around for a long time, the idea that there should or could be a fixed set of behaviours that people need to follow to stay safe online does not stand up to scrutiny.

The role of perceptions and attitudes

5. It follows from this that if people are to keep themselves safe online they need to learn to make good decisions regarding the way they behave and the things they do. Decisions such as these are not based on any objective measure of the actual or general level of risk the person faces. They are based on the person's personal perceptions of, and attitudes towards, the risks they are taking. Therefore, if people are to make good decisions, they need to have appropriate perceptions and attitudes.

6. We are living through the early period of the digital age. Many people do not yet have well grounded perceptions of digital risks. Neither have they developed attitudes that are conducive to staying safe and secure online. People will need a lot of help as well as a substantial amount of time if they are to develop these.

7. In the meantime, specific safety rules (e.g. on how to look after one's PINs and passwords, or about not clicking on suspect links in e-mails or messages, the digital equivalents to "don't play with matches" or "look both ways before crossing the road") have an important role to play. They stand in for a more considered decision-making process while people do not yet feel ready, able or willing to make case-by-case decisions for themselves. Specific safety rules also guide people when they do make their own decisions by embodying good practices: accepted good behaviours appropriate to all normal situations that people should generally try to adhere to.

8. However, specific safety rules, no matter how often they are repeated, are unlikely to be adopted unless people accept them as being valid. They will not be accepted as valid unless they are appropriate to the situation at hand and accord with the person's views of the risks. Telling people not to give out personal information online falls on deaf ears if the person is going online to visit a social networking site. In that situation, sharing personal information is central to the underlying purpose. Telling people to choose different complex passwords for different accounts but then not to write those passwords down would, in most people's minds, be dealing with the wrong risk. It is telling people to protect themselves from what most perceive to be a relatively remote risk, the physical theft of their passwords. At the same time, it is creating what they perceive to be a much more significant problem, that of having to remember what all one's passwords are.

9. This shows that people's perceptions and attitudes are the keys to them fending for themselves online. Perceptions and attitudes determine the decisions people make for themselves. They also influence the degree to which people are likely to accept and follow any specific digital safety guidelines and rules they might be given.

10. The conclusion of this is that, if people are to improve their online behaviours, in the short-term as well as in the long-term, then it is their perceptions and attitudes that need to be improved, not just their knowledge of safety rules and best practice behaviours. The idea that it is sufficient to provide people

with tutorials or instructions on how to behave or what to do does not stand up. It is essential that the effort must go first into helping people develop more realistic perceptions and better attitudes.

The perceptions people have

People's perceptions are based on the knowledge and beliefs they hold about the way the world works, and include the understanding people have of digital threats and the harm those threats can cause them.

11. Perceptions, as reported in surveys, are typically that levels of safety and security in the digital world are poor and threats are commonplace. For example (from the Norton Cybercrime Report 2010):

    - 65% of people say they have been exposed to some form of cybercrime;
    - 7% say they have been touched by social network profile hacking;
    - 97% say they expect to become the victim of some form of cybercrime at some stage;
    - 79% do not expect cyber criminals to be brought to justice, i.e. their belief is that cyber criminals typically do not get arrested or punished appropriately.

12. Children say they have had negative experiences online too. For example (from the same report):

    - 1 in 3 say they have been exposed to viruses;
    - 1 in 4 say they have been exposed to violence or porn online;
    - 1 in 10 say they have been approached online.

13. The definition of cybercrime used in the above survey was very broad and included malware, scams, phishing and harassment as well as fraud and theft. Hence, it did not discriminate between anti-social digital behaviour and criminal digital behaviour. What is reported as perceptions of cybercrime is in practice an amalgam of perceptions of a wide range of different types of malicious cyber behaviour. Not only does this make it hard to know what people's perceptions might be regarding each of these different types of behaviour, it makes it difficult to use this report to improve people's perceptions of the dangers of the digital world. It would be helpful if surveys and reports such as this could, in future, be more discriminating.

14. The perception that malicious behaviour is rife across the Internet agrees with the findings from IAAC's earlier workshops[2]. People are well aware of the existence of digital threats such as malware and cybercrime and typically believe that these are widespread. However, people's behaviours suggest that they do not typically believe the risks from these types of attack to be particularly significant. Whatever people might believe about their chances of falling prey to malware or cybercrime, they seem to believe that in most cases any harm they might be caused by any of these is likely to be minor. Most people rank the harms that can arise from digital risks well below the harms that can arise from routine physical activities such as driving (broken bones, loss of limbs, loss of life).

15. Looking next at perceptions relating to data handling practices, it was reported that people do not like organisations gathering personal information (PI) about them that they do not believe is relevant. People typically think organisations ask for too much of their PI, and that once they have it, those organisations cannot be trusted to look after it well or not to use it in ways that they shouldn't. The perception is that if one challenges an organisation that one believes is asking for too much PI, one is as likely as not to get an unhelpful response such as "it's our standard procedure" rather than a clear explanation of why that PI is needed. Also, that if one does not concede to the excessive PI request, one will not be able to complete the task that brought them to that point in the first place.

16. However, again, people's behaviours suggest that they do not believe the risks from poor data handling practices are significant. People tend to provide whatever PI is requested even if they feel it to be

[2] See the reports from PCIA workshops 5 (29 April 2010) and 6 (14 July 2010).

excessive. They feel inconvenienced by having to concede to an excessive request more than they feel they are made vulnerable by it. Poor data handling practices constitute an annoyance to them rather than a threat. They feel that, in the large majority of cases, whatever use is made of any excess PI gathered causes them no harm, and any harm that is caused is likely to be minor.

The attitudes people hold

Given that these represent many people's perceptions of digital risks and dangers, what are people's attitudes to digital safety and security?

17. Reports that appear in the media from time to time indicate that most people do not consider digital safety and security to be particularly important issues. Many people's attitudes seem to be driven more by convenience. And, as more safety and security can often lead to more complication and less convenience, people are often in the position of having to trade the two sides against each other. Reports tend to indicate that people are often willing to trade in a degree of safety or security for no more than a relatively low value reward.

18. One attitude that appears to be common to many people is that they do not feel able to take ownership of the safety and security issues that affect them. For them, safety and security is a complicated technical matter and it would not be fair for them to be made responsible for sorting such matters out for themselves. Possibly for that reason, they tend to see the job of making the digital world safe a responsibility for others, e.g. manufacturers, providers and the Government. They do not see it as something they have a role to play in themselves. Changing this attitude is essential if people are to learn to fend for themselves online.

Sensitising people to digital safety and security

19. For people to engage with digital safety and security matters, they need to feel that safety and security problems are problems that affect them personally. If people do not feel these problems have a bearing on their lives, they are not likely to accept that they have a role to play in dealing with them.

20. People are affected personally by cybercrime though maybe not in the way they might at first expect. The way people are affected was covered in a preceding workshop report[3]. There it was recognised that the direct consequences of cybercrime befall only a small minority of people. However, it was also noted that cybercrime has an indirect impact on nearly all consumers. Consumers pay for cybercrime each time they pay a service provider for the use of an online service. A proportion of the service or transaction charge they pay goes towards covering the costs the service provider faces from cybercrime attacks on their systems. As long as consumers continue to pay these costs, service providers are not being forced by market pressures to do more to reduce them. As a result, not only do people pay for cybercrime each time they use online services, the price of the convenience they desire so much is the level of cybercrime that is allowed to take place.

21. As a result, though they might not realise it, people are being affected by the harmful aspects of malicious digital activities. Digital safety and security matters do have relevance to their lives. If people were to be made more aware of this, that could help to change people's perceptions of digital dangers. This is a necessary prerequisite to changing their attitudes. That, as discussed above, is essential if people are to learn to fend for themselves online.

The role of the individual

Getting people to understand that they are more affected by a problem than they had realised can help make their perceptions more realistic. This is a start towards improving people's attitudes. To build on this, the next step is to help people deal with that problem.

---

3 The report from PCIA workshop 6 (14 July 2010)

22. Many people do not feel able to deal with digital safety and security problems because they do not feel they have either the technical knowledge or the skills that would require. Getting them to overcome this obstacle is not just a matter of giving them ample advice and instructions on what to do. People need to be given an understanding of the role they have to play and the responsibilities that go with that role.

23. The role of the ordinary person is not to become a master of digital safety and security. It is much simpler – it is to make sure that, as a user of digital devices, they take whatever steps are necessary to maintain their safety online. Helping people to understand what this role entails can be achieved by drawing on physical world parallels.

    Most people are not master car mechanics and readily admit they do not understand much about the technical details of the cars they drive. However, they do understand that, in their role as car owner, it is their responsibility to ensure that their car remains roadworthy and that when they drive they always drive safely. Most people manage to do this without difficulty. There are a few maintenance tasks that car owners typically undertake for themselves (such as keeping tyres inflated, keeping windscreens clean). For everything else it is the car owner's responsibility to get the job done by someone who does have the requisite knowledge and skills. The balance between those things that are usually done by the car owner and those that are usually done by a trained mechanic has changed over the years as cars have become more complex. Today people tend to be reliant on trained mechanics for everything but the simplest routine car maintenance tasks. However, an owner's lack of knowledge and skill as a car mechanic does not absolve them of their responsibility to ensure the car's roadworthiness and to drive safely. And it does not, for a moment, stand in the way of them discharging that responsibility in full.

    In a very similar sense, a person's lack of technical understanding of the digital devices they use is no reason for them not to be able to fulfil their responsibility to look after the security of those devices and to keep themselves safe when online. Their role as a user of digital devices entails ensuring that their digital devices remain 'roadworthy', i.e. able to withstand the daily security threats they are under, and that when they go online they 'drive', i.e. behave and act, safely and within their capabilities. Those maintenance tasks that the device owner feels they understand they can take on for themselves. For everything else, if the task cannot be automated by product providers then the owner should expect to get the job done by someone else who does have suitable knowledge and skill. That might be a family friend, a knowledgeable neighbour, or the service staff at the local PC shop.

24. Whatever the limitations of the individual's technical understanding, they have a role to play in keeping themselves safe online. The responsibility that goes with that role is to maintain the security of their digital devices and the safety of the way they behave. Most people should be able to do this without difficulty. Any lack of knowledge or shortage of expertise is no reason for them not to be able to discharge this responsibility in full.

Building a realistic general understanding

Once people have understood and accepted this role, they will be in a position where they can take on the task of dealing with the safety and security of the situations they face. The goal is to get people to make sensible safety and security decisions that match the situations they are in and the level of risk they are willing to take.

25. The first requirement is for people to develop a realistic general understanding of the threats, outcomes and harms that are possible in the digital world. People need their knowledge and beliefs about the digital world to be realistic so they do not take risks they would otherwise be unwilling to take.

26. In the physical world, people's knowledge and beliefs relating to their physical safety evolve and adjust continually as they face and deal with a wide variety of different physical situations some of which are more unsafe than others. In today's digital world, most people do not have an equivalent level of experience dealing with unsafe digital situations. They need to be helped to develop their understanding. The first step towards this is to provide people with a general sense of how safe or unsafe the digital world can be. As before, this can be achieved through the use of familiar physical world analogies.

For example, most people have a realistic and well grounded sense of how safe / unsafe driving is. To paraphrase:

- On the whole, cars are safe, and a lot safer today than they have been in the past.
- People understand that this does not mean that cars are absolutely safe and it does not mean that they can afford to drive carelessly and irresponsibly.
- People understand the sorts of personal harm and physical damage they can cause, to themselves and to others, if they do not drive carefully enough.

This is exactly the type of general understanding that people need to acquire about the digital world. They need to recognise that the digital products and systems they use are, on the whole, safe but this does not mean that the digital world is absolutely safe and it does not mean that people can afford to be careless and unthinking when they go online.

There are other analogies that could be used to convey this general message to non-drivers. For example, children will recognise that playgrounds are generally safe but that they can still get hurt if they are careless. The elderly and infirm will recognise that walking in a crowded pedestrian area is generally safe but that they still need to take care walking over uneven paving. Different analogies will work for different people, each serving to convey the same general understanding.

27. Once this general understanding has been established, it can then be populated with greater detail. This will give people familiarity with the types of situation they might face online, the problems that could arise from these situations and the consequences these problems could have for them. The media, for example, would be well placed to help in this regard. TV channels could weave digital dangers into the storylines of the soaps and dramas they show. Local newspapers could report on digital burglaries and accidents alongside their reports of house burglaries and car accidents.

Developing situational awareness

The next skill that people need to develop is situational awareness. Situational awareness is the ability to recognise the key threats, risks and dangers the person is exposing themselves to in each situation they face.

28. Situational awareness, as with trust, is largely experiential. As people gain more experience with a range of digital situations, they learn to recognise the different risks and become familiar with what not to do and whom not to trust. However, many of the warning cues people receive in the physical world are not present in the digital world.

29. In the physical world, people pick up on a wide range of cues that allow them to calibrate how dangerous a given situation is. For example, people learn from an early age how great a physical impact their body is capable of taking. They learn (e.g. by jumping down from a height, crashing into a wall, falling off a bike) how much impact or stress is needed to give them minor injuries (e.g. bruising, soreness) and at what point they might start to sustain more serious injury. These experiences help people judge when a physical situation might be a bit too dangerous for them even if they haven't experienced that exact situation before in their lives. Similarly, people can see when they have had a near miss, when a possible accident was just avoided, and can adjust their behaviour next time to increase their margin of safety.

30. In the digital world, smart devices don't give off these cues. They do not show signs that allow their owners to calibrate how much security stress their smart devices are put under by the digital threats that are rebuffed or what dangers are being averted. They do not give warning cues showing when a possible security failure has just been avoided. For example, if after some delay a PC owner eventually applied a software patch, they will not know if that was just in time to block a particularly nasty attack that was about to hit them. This makes it difficult for people to develop an equivalent sense of when a digital situation is becoming too dangerous for them or to learn when they need to adjust their behaviours to increase their margin of safety.

31. As a result, today people cannot easily know how safe or unsafe a digital situation is. The only thing people can tell is when a digital situation becomes sufficiently unsafe that things turn out bad and a security problem hits them. To help people avoid having to run into each type of problem before they know it is there, it would be helpful if people could be given the warning cues and signals they need.

    Some of these sources could be informal and others more formal. As suggested above, TV shows or dramas could weave digital dangers into their storylines. This would let people see how digital dangers manifest themselves, what sorts of things people do that make them vulnerable, what harms get caused and how much time and effort is needed for people to recover. Alternatively, just as insurance companies collate burglary statistics and produce a crime rating for each locality, it would be helpful to have some equivalent measurements that could lead to the development of a security rating for the main types of activity people can perform on the Internet.

32. People need generic warning signals such as these. They also need specific warning signals, signals specific to them and their situation. For this they need greater transparency into what is going on beyond their device's screen. For example, it would be helpful if their consumer security products were able to recognise and inform them when a 'near miss' had just occurred. It would also be helpful if the organisations that hold people's personal data were to provide a periodic (or on demand) 'statement' to the data subject showing what personal data of theirs is being held and the uses that have been made of it since the preceding statement.

33. These are just a few examples. New approaches need to be thought up that would strengthen people's situational awareness and their appreciation of the dangers, generic and specific, they face as they participate in the digital world.

Making good choices

Ultimately, the main skill people need to develop is one that could be called 'digital common sense'.

34. Digital common sense is about knowing how to behave in ways that are safe in each of a wide variety of common situations. It is also about being able to make sensible informed case-by-case safety decisions in less common situations. It includes knowing when it is best to stay close to one's normal 'best behaviours' and when it is safe to deviate. And in those situations where it is safe to deviate, knowing how far to go is far enough.

35. To help people make good choices they need both general guidelines and specific instructions. General guidelines help people develop safe behaviours. Specific instructions help them to do the right thing in situations where the danger, if they were to deviate, might be higher than normal.

36. Importantly, these guidelines and instructions need to be sensible and appropriate. They also need to be consistent regardless of their source.

    There is an abundance of guidance and instruction available to people today. However, as mentioned earlier, it is not all as sensible as it should be or always appropriate to the situations in which it is provided. There is also inconsistency between the advice that different sources provide. For example, some organisations allow their users to keep the same password indefinitely, others force their users to change their passwords on a regular basis. People get confused and do not know which approach is safest. Clearer thinking and greater cooperation between advice providers would help people learn what practices are generally safest and to make better choices.

37. Providing good guidelines and instructions is one part of helping people make better choices. Another is to design information systems in a way that makes it easier for people to make good choices and harder for them to make bad ones. For example:

    - Making systems more user-centric so it is easier for people to exercise control;
    - Making the safe option the default option so people have to make an explicit choice if they wish to deviate and do something that might be unsafe;

- Designing systems in ways that reduce their reliance on users having made good choices – for example reducing the need for a system to rely on the consumer's device being uninfected;
- Having systems that use personal data provide their users with different levels of service for different levels of personal data provided. This would allow users to choose how much data to provide and give them options if they do not wish to provide the full amount of data requested.

38. Finally, it might help people make better choices if there were a direct correlation between the way they behave and the consequences they face. As discussed in a previous report[4], the burden of cybercrime is shared across the entire user community rather than being borne by the individuals who fall for cybercrime scams and phishing. This does not drive home to people the need for them to develop safer habits. By way of contrast, if someone drives while under the influence of alcohol or drugs, they are the ones who get the points on their licence and whose insurance premiums go up. This gives drivers an incentive to improve their driving habits. Where reasonable and fair, this approach should be adopted for digital behaviours too.

Concluding remark

39. Reducing the dangers for people when they go online is a shared responsibility. It is shared across all parties within the digital ecosystem. It is not the sole responsibility of government and suppliers, and neither is it the sole responsibility of individual people themselves. Each party has to take on its share of that responsibility if it is to expect others to take on theirs. People will not be inclined to take more care to prevent cybercrime if they continue to feel (as has been reported) that cybercriminals do not get brought to justice. However, law enforcement bodies will be reluctant to give combating cybercrime a higher priority for their attention if the public does not take more care and show more concern. People will not bother to maintain a secure posture if they feel that the organisations handling their personal data cannot be trusted to protect that data. However, system developers and vendors will not put in the effort to improve their offerings unless consumers show they are interested and are prepared to pay for the benefits they would get. As the saying goes, the bridge needs to be repaired from both ends. Each party has to take on its role and its share of the responsibility otherwise none will.

4 The report from PCIA workshop 6 (14 July 2010)