Online security won't improve until companies stop passing the buck to the customer

4 May 2017, by Steven J. Murdoch

‘No, I absolutely do not wish to change my password, thanks.’ Credit: Shutterstock/Rawpixel.com

It's normally in the final seconds of a TV or radio interview that security experts get asked for advice for the general public – something simple, unambiguous, and universally applicable. It's a fair question, and what the public want. But simple answers are usually wrong, and can do more harm than good.

For example, take the UK government's Cyber Aware scheme to educate the public in cybersecurity. It recommends individuals choose long and complex passwords made out of three words. The problem with this advice is that the resulting passwords are hard to remember, especially as people have many passwords and use some infrequently. Consequently, they will be tempted to use the same password on multiple websites.

Password re-use is far more of a security problem than insufficiently complex passwords, so advice that doesn't help people manage multiple passwords does more harm than good. Instead, I would recommend remembering your most important passwords (like banking and email), and store the rest in a password manager. This approach isn't perfect or suitable for everyone, but for most people, it will improve their security.

Advice unfit for the real world

Cyber Aware also tells people not to write down their passwords, or let anyone else know them – banks require the same thing. But we know that people commonly share their banking credentials with family, for legitimate reasons. People also realise that writing down passwords is a pretty good approach if you're only worried about internet hackers, rather than people who can get close to you to see the written notes. Security advice that doesn't stand up to scrutiny or doesn't fit with people's lives will be ignored – and will discredit the organisation offering it.

Because everyone's situation is different, good security advice should include helping people to understand what risks they should be worried about, and to take steps that mitigate these risks. This advice doesn't have to be complicated. Teen Vogue published a tutorial on how to select and configure a secure messaging tool, which very sensibly explains that if you are more worried about invasions of privacy from people who can get their hands on your phone, you should make different choices than if you are just concerned about, for example, companies spying on you.

The Teen Vogue article was widely praised by security experts, in stark contrast to an article in The Guardian that made the eye-catching claim that encrypted messaging service WhatsApp is

insecure, without making clear that this only applies in an obscure and extremely unlikely set of circumstances.

Zeynep Tufekci, a researcher studying the effects of technology on society, reported that the article was exploited to legitimise misleading advice given by the Turkish government that WhatsApp is unsafe, resulting in human rights activists using SMS instead – which is far easier for the government to censor and monitor.

The Turkish government's "security advice" to move from WhatsApp to less secure SMS was clearly aimed more at assisting its surveillance efforts than helping the activists to whom the advice was directed. Another case where the advice is more for the benefit of the organisation giving it is that of banks, where the terms and conditions small print gives incomprehensible security advice that isn't true security advice, instead merely a legal technique to allow the banks wiggle room to refuse to refund victims of fraud.

It's for this reason that prominent bank marketing is aimed at making customers feel safe, while security advice is buried in places banks know customers don't read. Despite complaints from consumer groups like Which? to the Payment Systems Regulator, so far banks have got away with this.

Out of your hands

Giving good security advice is hard because very often individuals have little or no effective control over their security. For example, the extent to which a customer is at risk of being defrauded largely depends on how good their bank's security is, something customers cannot know.

Similarly, identity fraud is the result of companies doing a poor job at verifying identity. If a criminal can fraudulently take out a loan using another's name, address, and date of birth from the public record, that's the fault of the lender – not, as Cifas, a trade organisation for lenders, claims, because customers "don't take the same care to protect our most important asset – our identities".

Keeping your computer or smartphone software up-to-date is good advice, but is only any use if the device's manufacturer provides security updates and ensures that they're tested and don't cause more problems than they solve.

It is precisely because security is so often out of the hands of individuals that the new UK National Cyber Security Centre (NCSC) has focused its advice on helping companies improve security, without placing an undue burden on the customer (or even requiring them to read the advice). Its passwords guidance shows how companies can remain secure even when most of their customers choose fairly simple passwords. This advice was developed in collaboration with the Research Institute in Science of Cyber Security (RISCS) which promotes evidence-based research.

NCSC chief executive Ciaran Martin promoted this guidance at an event in February, and at the CyberUK event in Liverpool last month. And in March, NCSC launched a video explaining that "If security does not work for people, it doesn't work". This workable security advice, based on RISCS research, is having an effect: the government no longer recommends regularly changing passwords, because doing so has been shown to have a harmful effect on security. However, Cyber Aware, another government website, still offers advice to consumers that is out-of-date and counterproductive.

Customers do want to protect themselves, and there is a clear demand for good security advice. But this advice needs to be realistic, needs to consider that different individuals have different circumstances that require different approaches, and put the interests of the customer first. Companies that develop security systems are in the best position to improve security, and they must take responsibility for doing so by learning from the research that reveals how individuals really use, understand, and misunderstand security technology.

This article was originally published on The

Provided by The Conversation