THE CONVERSATION

Academic rigour, journalistic flair

Password education should be age-appropriate: here’s how

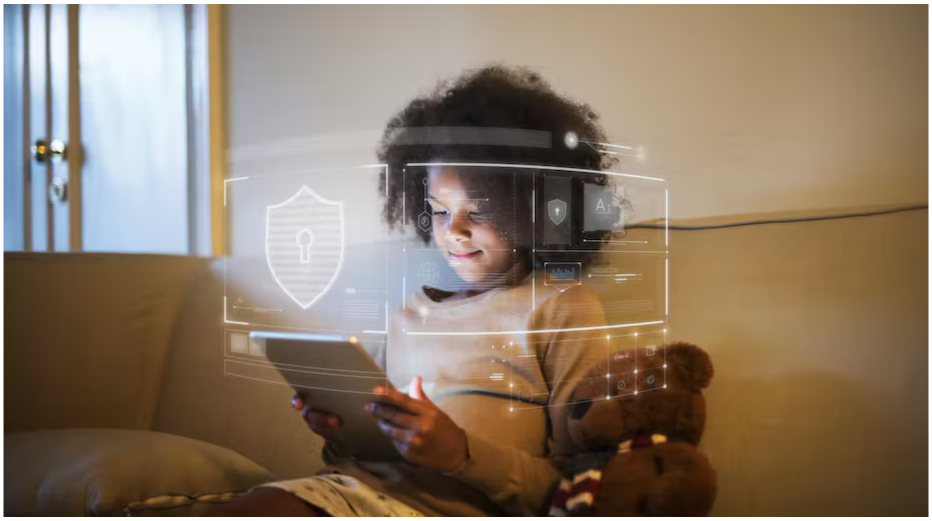
Published: September 21, 2020 3.35pm BST

Karen Renaud

Visiting Professor of Cybersecurity, Rhodes University

Suzanne Prior

Lecturer in Computing, Abertay University



Our set of best practice principles should help adults to teach the principles to children in an age-appropriate way. Shutterstock

Children are increasingly being exposed to, and using, technology from a very young age. This has never been more true than in 2020 when the vast majority of children worldwide have used online resources to access educational resources and communicate with family and friends during the COVID-19 pandemic.

Many of the resources and websites used, along with the devices they are accessed on, require the use of a password to authenticate the user. However, young children don’t necessarily have the skills and knowledge required to use and maintain these passwords appropriately. They are likely to use weak, predictable passwords and tell other children their passwords.

Children come from a variety of different backgrounds and their parents will have a wide range of cyber-related skills. They might pick up some password related knowledge but there is no guarantee that they will learn the correct principles.

This situation led us to wonder what principles children should learn, and when they should learn them. To answer this question, we carried out research to:

1. Determine what current best practice is with respect to password management, gathering the information from international standards bodies. We wanted to gather a set of password “best practice” principles.

2. Gauge the best age at which to introduce each “best practice” principle by consulting the child development literature.

3. Develop three sets of age-appropriate password “best practice” principles, to ensure that children learn the correct principles as and when they are ready for them.

Preparing our Children for a Cyber Secure Future

Karen Renaud

Teaching children about cyber security.

Organisations have tended to advise that passwords should be at least eight alphanumeric characters long, contain digits or punctuation characters as well as letters, and both upper and lower case characters.

This essentially imposes *complexity* requirements on passwords. But in 2017, the National Institute for Standards and Technology, the UK’s National Cyber Security Centre and the Centre for Protection of National Infrastructure published revised password guidelines. One important change is that length, not complexity, characterises strong passwords. Other widespread practices have also been replaced. For example, they advise against automatically replacing passwords at regular intervals.

Read more: A computer can guess more than 100,000,000,000 passwords per second. Still think yours is secure?

So, we worked through these reports and derived a set of password "best practice" principles.

The next step was to investigate the child development literature, to provide a baseline for creating three sets of appropriate "best practice" principles. A number of relevant developmental aspects emerged: emerging literacy, ability to focus, and the ability to discriminate between people they can tell secrets to, and those they shouldn't.

There are also issues for children with dyslexia. These children experience difficulties in learning to read and to parse words into individual characters. This makes password usage challenging.

Best practice

Based on these insights, we allocated the principles to three different sets, for children aged 4-5, 6-7 and 8-9. These ensure that the principles will be taught when children are ready to learn and apply them.

We then ran focus groups with parents of children of these ages, to ensure that we had assigned appropriate principles to each age group. We also rephrased the principles to make them child friendly. For example instead of naming "impersonation" as being a consequence of password leakage, we rephrased that to: "someone telling the computer that they are you".

Our next project aims to test these initial sets of principles by giving them to teachers and parents to help them to educate the children in their care. We hope to refine them based on their feedback.

Below are the principles we can teach to children when they are starting to use passwords.

Password best practice for 4-5 year olds.

This small set of principles is augmented as the children develop and mature, with the full set, as shown below, being taught by the time they get to 9 years of age.

The full set of principles for 8-9 year olds.

We also carried out a review of children's books that teach password principles. We discovered that the majority of the books didn't teach the correct principles. Many advised children to choose complex passwords instead of correctly advising them to use passphrases (three or more words). Nor was coverage of the principles particularly comprehensive.

Hence, children's books are probably not the best tool for parents to use to teach the latest password "best practice" principles. The sets of "best practice" principles we have derived should help adults to teach the principles to the children in their care in an age-appropriate way.

To make it easier for teachers and parents, we have developed some videos, together with accompanying child-friendly materials to reinforce lessons learned. Our Cyber Squad will teach password "best practice principles" in a fun and engaging way.

A final titbit for bilingual adults and children – use multiple languages in your passwords. Recent research by Pardon Maoneke and Stephen Flowerday has discovered that this makes passwords much stronger. Here’s an example using English and isiXhosa, two of South Africa’s 11 official languages: instead of the password “I love pink elephants”, you could use “Mna love pinki elephants”.