How to Teach Kids to Use Passwords

Good password practices can start even before a child knows how to read. Here's an age-by-age guide.

The trick is to explain things in a way appropriate for children at different developmental stages.

By Karen Renaud

June 20, 2020 9:15 am ET

It's crucial to teach children good password hygiene and computer security from an early age.

The only question is: How?

Think about how hard it is to teach adults good password and cybersecurity best practice. Then try to come up with an age-appropriate practice for a 4-year-old. Or a 7-year-old. Or a 9-year-old. It isn't easy.

The problem is that password "good practice" requires skills that very young children might not yet have developed, even as many of them are using online devices from a very young age.

For example, consider a 4-year-old who is just learning how to read. She would likely be hard pressed to memorize an alphanumeric password, because she doesn't yet know her alphabet. Instead, she may have to remember a shape on the keyboard. As children learn their alphabet, they start being able to reproduce simple passwords. But because they type

very slowly, they will have a hard time remembering the moving position within the password while they search for the right key.

Other challenges for our 4-year-old: She uses a keyboard displaying uppercase letters, but when typed, it actually enters a lowercase letter. Even worse, the entered password is hidden during entry so that she gets no feedback. She also isn't able to keep her passwords secret, nor can she perceive or anticipate deception, the whole reason for secrecy.

The trick is to have a strategy that allows parents and teachers to explain things in a way that a child at different developmental stages would understand—and be able to implement.

Here's a look at what those best practices might look like for children of various ages, based on research I've conducted with my colleague Suzy Prior.

Ages 4-5

Ideally, we wouldn't ask children to use a password at all, but instead find another way to authenticate them when they go online.

> To this end, one of my students developed a password alternative for preliterate children that relies on the child's ability to recognize faces. Under this alternative—which is still just a concept and not a product—the child's caregiver would provide the system with a photo of an adult the child knows well. To log in, children would identify themselves by picking the animal that they chose when they enrolled. They then would authenticate by choosing their familiar face from a set of faces displayed on the screen. (One is theirs and the others aren't real people, but are computer-generated).

Unfortunately, it isn't going to be possible to avoid passwords altogether. So, caregivers and educators for children this young should start by explaining the consequences of lost passwords, using examples such as, "You might not be able to play a game if you lose your password." This will help the child understand the rationale behind password use. Giving them a concrete example makes it personal.

For children of this age, their trusted adults have a prominent role to play. They generally wouldn't have the required creativity and problem-solving skills to create passwords, so their caregiver should do this for them.

Still, children at this age *can* be made aware of the need to check for someone observing their password as they enter it. ("Before you enter your password, make sure no one is peeking.") In this way, they can start taking ownership of "their" password—implicitly teaching them the cardinal rule of passwords: keep them secret.

Ages 6-7

Having made children aware of the consequences of a lost password, at this age they can understand the specific reason for passwords: "This will stop others from using your computer" and "People will tell the computer that they are you."

> This is possible because children of this age are able to anticipate and imagine other people's actions.
>
> What's more, children at this age are capable of creating and memorizing their own passwords, and they have developed problem-solving skills, so it is possible to give them more autonomy.

They are ready to create their own passwords, with advice like:
"Make up a silly sentence" ("silly" makes it easier to remember) and "Make sure you can remember your password." Then, because they have also developed metacognition skills, we can tell them to think about creating a password that will be easy for them to remember and won't confuse them when they are typing.

Many password guidelines tell people *not* to write down their passwords, but that approach doesn't necessarily work with children, where it is better to phrase the advice in positive terms. If you tell a child not to write down his password, he has to first think about writing it down, and then remember that he should not do this. He might easily forget the "not" part of the instruction.

So it's better to simply tell a child to "remember your password." You can get at the written concerns more indirectly, by noting separately that one issue with passwords is that
"somebody could find your written-down password."

It is also important for this age group to understand that they should change a password only if someone else knows it. This advice runs counter to more old-fashioned advice about changing passwords regularly. But we now know that forcing people to come up with new passwords at regular intervals makes them use weaker passwords, so the practice is counterproductive.

We can also update the password entry advice to: “Before *and while* you enter your password, make sure no one is peeking.”

We retain the advice about consulting a trusted adult. Yet the parents have a lesser role: less active participant and more mentor who can be relied upon for advice and help.

Ages 8-9

This group is likely to be reading fluently, and to have a range of skills that mean they can cope with a lot more advice. We can now address the issues related to password reuse (“Doors have different keys, you should also use different passwords”), and also suggest that they match the strength of the password to the value of what is being protected (“If someone could use your password to change something you care about, choose a longer password”).

> We would still advise this age group to come up with a silly sentence as their password. Because they can be expected to be fluent readers, they can be encouraged to use longer and perhaps more words in their silly sentence to make it stronger.
>
> Finally, they are ready to be taught to check for the little padlock in the address bar of the browser before they enter their password (to check for a secure connection). At this age they are likely to have the attention skills to be able to focus on this level of fine-grained detail.

If they do all these things, they are on their way to being security-savvy consumers. And probably showing more-secure behavior than most of the adults around them.

Dr. Renaud is professor of cybersecurity at Abertay University in Dundee, Scotland. She can be reached at reports@wsj.com.