KAREN STEPHENS

Karen Stephens is the co-founder and CEO of BCyber. After more than 25 years in financial services, Karen moved into SME cybersecurity risk management. She works with SMEs to protect and grow their businesses by demystifying the technical aspects of cybersecurity and helping them to identify and address cybersecurity and governance risk gaps. She was recently named inaugural Female Cyber Leader of the Year at the 2023 CyberSecurity Connect Awards in Canberra.

COLUMN

Are you ever too young to start your cyber safety journey?

So, what age is too young to start someone on their cyber safety journey? I have been puzzled over this question for weeks as I prepared to write a few words on the topic. Should we be saying to parents: “you be you” and let everyone make their own decision? Or should we rely on the government to play big brother, step in and say: “this platform is not suitable for your children” (hello TikTok). I landed somewhere between the two. I know every parent wants to keep their children safe from harm, but sometimes their own actions do the exact opposite. As parents we need to educate ourselves and learn what is age-appropriate for our children.

Let me explain. It is wonderful to share exciting news and experiences such as a birth, adoption, starting a new school, graduation and the like, and wanting to share the news far and wide is understandable. However, putting everything out and about on social media is not such a good thing. The practice of sharing your family news on social media platforms does not take into consideration your role as your child’s privacy custodian. Some good pointers to be mindful of include:

1. **Be careful what you share.** What you share may be used by people you don’t know for activities you don’t condone. This article highlights some of the dangers.
2. **Think beyond the here and now.** Social media has been around for a while and we are starting to see children get to an age where they start to question what has been shared about them by their parents. Reddit posts like this one have started to appear and be picked up by mainstream media.

3. **Protect your child’s privacy - play the long game.** When you go to share something about your child, ask yourself “how will it impact my child’s future adult self?” This was brought home rather starkly by Deutsche Telekom. It joined forces with the creative agency adam&eveBerlin to produce “Don’t share your kids personal information without consent Deutsch Telekom Deepfake AI Ad” (Viewer discretion is advised).

In my world there is nothing like a real life example to bring it all home. So grab a hot beverage of your choice and get comfortable.

Picture this. Your child has been invited to a playdate by someone who pretty much shares their entire life on social media. Now you’re a bit old fashioned when it comes to data privacy and have a strict no-social media rule. This means no photos of the family are to be placed on any platform. The usual “please don’t share any pics of my kid on any platform” request is made, and to get the point across you ask to have a quick look at a few pics the couple has placed on its social media platforms.

Now you're not a 'professional bad guy' but after a quick browse you can work out their home address, cars, children's names, school, ages, year groups, sports, interests, etc. Get the idea? While no social media postings of your family may have occurred on that day, you may never get another invite. This is called putting your family's data privacy first. It is neither a popular nor an easy path.

After reading the above you may think I am a social media luddite who lives off the grid in the middle of nowhere. I am not. But I am hypersensitive and aware of the pitfalls of oversharing. Coming back to the original question, my answer is that you can never be too young to start your cyber safety journey. While the internet can be scary, it can also be a magical place of wonder. So, remember:

- Start the cyber safety discussion early.
- Respect the age minimums of social media platforms.
- Provide practical advice to kids. For example, on good password hygiene and on adding friends to social platforms. (If you don't know them in real life you don't know them at all!)
- Parental controls are their friend NOT something they need to "work around".
- Model good behaviour. Your children are watching you and copying you. For example: no devices in bedrooms, no working around parental controls.

And my story? That may or may not have happened in real life.

www.linkedin.com/in/karen-stephens-bcyber

www.bcyber.com.au *twitter.com/bcyber2*

karen@bcyber.com.au *youtube.bcyber.com.au/2mux*