

Cyber savvy parents keep kids safer online

By  Dan Thornton

22 Aug 2022

While there may be a good dose of fearmongering around child online safety, the risks are still real, and parents need to understand them so that they are empowered to take action to protect their families. Cyberbullying, exposure to harmful and inappropriate content, and grooming by online predators are the stuff of parents' nightmares. However, on the plus side, there's also a robust cybersecurity ecosystem offering significant tools that help parents to protect their families.



Image supplied

The digital realm is rich with opportunities for our kids to explore, learn and connect. As parents, we don't want to stand in the way of that. But, it's also a Wild West when it comes to cybercrime. [The 2022 Parent Guide for child online safety](#) reports that 68% of child internet activity is not monitored by parents and 85% of parents are putting devices into their kids' hands just to keep them busy.

One of the biggest hurdles to keeping kids safe online is a parent's lack of knowledge of the cyberspaces where their kids are active. Many parents sanction their kids having social media accounts without much clue about how those platforms actually work. Some parents aren't aware that the games their kids play have online chatrooms where they are engaging freely with strangers.



South African data breach costs reach an all-time high, report finds

28 Jul 2022



There are parents who are unaware that recreational drugs are sold online to minors, or who think it's impossible that their kid may engage with pornographic or suicide ideation content. This raises the risks that their child could become a victim or even a perpetrator of cybercrime. It also flies in the face of data - Ofcom, the UK communications regulator, reported in 2019 that [79% of internet users aged 12 to 15](#) experienced at least one potentially harmful interaction online over a 12-

month period.

As parents we instruct, guide and model behaviours for our children so that they can succeed and make a positive contribution to the world. We teach them all sorts of things to keep themselves safe and ensure they don't cause harm to others. Today, this vital parental role has to include the fast and ever-changing digital environment. Our kids are not just citizens in the physical world, they are digital citizens too. This demands that parents take a keen interest in ensuring that they are cyber-savvy and that they make good use of the latest cybersecurity tools that help to keep families safer.

There are three steps parents need to take to become cyber savvy:

1. **Be informed** - when it comes to your child's safety, ignorance is not bliss. Know exactly where they are engaging online through games, websites and apps on their phones. Understand those platforms, how they operate and the risks to minors. Make sure your kids are only playing age-appropriate games and don't let them sign up for social media accounts when they are underage.
2. **Talk to your kids about online safety** - open, trusted communications are your best route to keeping your child safe online. Just as you are in the physical world, be their first-line of protection in online spaces. Educate them about the risks and the warning signs. Let them know that they can and should come to you with their concerns. Educate them about privacy and the importance of not publishing or sharing their personal data, which includes your credit card details! Keep abreast of evolving cyber safety risks and talk through these as a family.
3. **Deploy the latest cybersecurity tools** - a parental control app is just one layer of security, and it can't possibly mitigate all the online risks. The cybersecurity ecosystem for families is constantly evolving and latest tools include AI-driven apps that can alert parents to potentially risky child engagements with people and content online across multiple devices. This empowers the parent to step in at the moment of risk and ignite conversations and take actions that can keep their child safer online.

ABOUT DAN THORNTON

Dan Thornton, CEO and co-founder of GoldPhish Cyber Security Training, is a former Royal Marine Commandos Officer. During his seven years of service, he was deployed all over the world including multiple operational deployments leading teams in both Iraq and Afghanistan. He then transitioned from the military into a career in Corporate Security Risk Management helping international oil and gas companies operate safely and securely in some of the most high-risk locations around the world, including West Africa, North Africa, and the Middle East.

- SA shoppers warned of online scams ahead of shopping season - 20 Oct 2022
- Building cyber-savvy workplaces in SA - 3 Oct 2022
- Cyber savvy parents keep kids safer online - 22 Aug 2022
- Cyber fraud has steep collective costs - 27 Jul 2022
- Why cybersecurity needs to tighten up as cryptocurrencies plummet - 22 Jun 2022

[View my profile and articles...](#)

For more, visit: <https://www.bizcommunity.com>