



Mitigating Risks of Allowing Children to Use Personal Mobile Devices - Tips For Parents

Safe on Social, our cyber safety partner, is providing tips to help Australian parents become more aware of the risks associated with mobile device use. It's essential to be cautious when giving your child your mobile device to watch videos or play games in public places, as there are potential risks you need to be aware of. With the constant media attention on cyber security, Safe on Social is here to provide guidance and help keep your child safe online.

Many organisations allow employees to use personal devices to access work email and networks. However, when children use these same devices for social media and free games, it can lead to significant risks.

It's essential to be aware of some of the top risks to ensure the safety of both your personal and work-related data:

1. **Malware and Virus Infection:** social media and free games may contain malware and viruses that can spread to your corporate network through your device, causing damage to the entire corporate infrastructure.
2. **Data Theft:** Children using a parent's device which can access a parent's work email or network may unknowingly download and install malicious apps that steal data and record keystrokes that may lead to a data breach that can result in severe financial and legal consequences for the organisation and the parent!
3. **Phishing Attacks:** Children may fall victim to phishing emails, texts, or ads that appear legitimate. They may lead to a compromise of sensitive business information stored on your phone.

To protect yourself and your organisation, consider these tips:

- Use company-owned devices for all work-related matters when possible, and only your devices for games and social media if you do not access anything work-related from that device.
- Regularly update your devices' antivirus and firewall software to protect against malware and virus infections.
- Be cautious of emails or texts that ask for personal information or download links.

- Talk to your children about cyber security risks and safe use of social media and educate them about safe online practices.
- Make sure your children know never to use a school email address to sign up for social media accounts. This will help protect us from potential Ransomware attacks.

By being aware of these risks and taking necessary precautions, you can help protect Australia against potential cyber-attacks.

Conversations around online safety are not always easy, but they are essential. This year we'll be providing you ongoing support and tips on social media apps, trends, and more to ensure open communication is happening in the classroom - and at home.