What South Africans need to know about smart devices - from cars to cots

Issued by ESET

12 Sep 2023

We live in a world surrounded by smart devices - from our pockets to our driveways and living rooms. These advancements offer convenience, and in many cases, extra security. But when gadgets are fitted with computing power and internet connectivity, they also become a target for remote hackers, says Carey van Vlaanderen, CEO of Eset South Africa.

Carey van Vlaanderen, CEO at Eset Southern Africa

Smart cars meet smart hackers

Earlier this year, a TikTok trend helped thieves hack certain models of Kia, Hyundai cars. According to Bloomberg, videos about the so-called Kia Challenge showed mostly teenagers giving instructions on how to unlock certain models of Kia and Hyundai cars. By inserting a USB cable into a broken steering column, TikTok videos show, thieves can hotwire an engine – much like the way that screwdrivers typically come in handy for the same reason. While in the past, obscure skills and knowledge were needed to break into and start a car, today, thieves and anyone else can easily find all that info online and sometimes even on social media.

Van Vlaanderen says several ethical hackers, who use their skills to identify security vulnerabilities to publicly raise awareness, have found vulnerabilities in various smart car models that allowed them to start them, sound their horns, or flash their lights – all done remotely or from close vicinity. “Unfortunately, there is not much car owners can do about cybersecurity of their vehicles aside from having a general awareness about the vulnerabilities inherent to any device connected to the internet and to take steps as advised by manufacturers as and when needed.”

Get savvy about smart home technology

She adds that one of the biggest attractions of smart home technology, particularly in South Africa, is using internet-connected devices to secure personal dwellings remotely. “Despite the ease smart home security devices provide for protecting homes against theft, damage, or accidents, smart home devices also create the risk of lowering personal data security. Two major flaws in connected homes make them susceptible to attacks; vulnerable local networks and weak IoT devices.”

Wi-Fi connections can be at risk if they have simple default names or easy-to-guess passwords. Even though some smart devices come with built-in security features, Van Vlaanderen says it’s essential for owners to take extra precautions. This includes setting up strong passwords and using two-factor authentication. This means when you try to log in, you'll need an extra code or approval from your phone or a special app to access the device.

ICT

ChatGPT and cybersecurity: what AI means for digital security

ESET 13 Mar 2023

Monitoring your baby securely

“The same principles hold true for internet-connected baby monitors. There are examples of distressed parents discovering that their baby monitors have been breached by strangers, and while these cases are relatively rare – they do happen from time to time,” she says.

The motives for hackers trying to access a baby monitor may vary, from playing an elaborate prank to gathering information for more nefarious purposes, such as stealing personal information overheard on the monitor, or confirming that no one is home so that the house can be burgled.

“Wi-Fi baby monitors are more exposed to hacking because they connect to the home router and, often, out to the public internet. The latter supports functionality which allows parents to view the video feed via a mobile app, wherever they are. While this could provide peace-of-mind when out and about, it also opens the door to remote hackers, who might be scouring the web looking for unsecured cameras to hijack,” notes Van Vlaanderen.

How to protect your smart devices and online privacy

Securing smart devices is crucial in today’s interconnected digital world. Here are Van Vlaanderen’s top tips to help ensure the safety of your devices:

- Change default passwords and always use **strong passwords**.
- **Update your device’s firmware and software regularly**. Manufacturers often release updates to fix known security vulnerabilities.
- Whenever possible, **enable two-factor authentication**.
- **Turn off any unnecessary features on the device**. If you don't need your smart device to listen for voice commands disable the microphone.
- **Use a trusted home security solution** like Eset to ensure your online protection and privacy.
- **Educate yourself** about the security features of any smart device before purchasing.

- **Eset launches solution to address SOHO security concerns** 15 Apr 2024
- **Don’t gamble with your cybersecurity** 29 Feb 2024
- **Avoiding job scams, and finding a job you love** 9 Feb 2024
- **Sharenting and security concerns: Will you be posting that back-to-school photo?** 10 Jan 2024
- **Fighting the digital grinch: Cybersecurity tips for kids and parents for a safe festive season** 8 Dec 2023

ESET

ESET has been helping people protect their digital worlds for more than three decades. From a small, dynamic company we've grown into a global brand with over 110 million users in 202 countries.
Profile | News | Contact | Twitter | Facebook | RSS Feed