Turn your phone off every night for five minutes, Australian PM tells residents

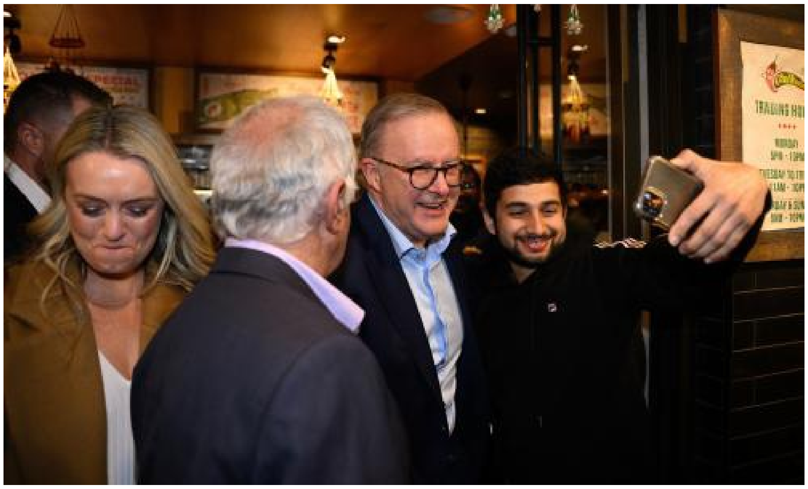
Publication Date: 2023-06-23

Author: Elias Visontay

Section: Technology

Tags: Cybercrime, Anthony Albanese, Australian politics, news

Article URL: https://www.theguardian.com/technology/2023/jun/23/turn-your-phone-off-every-night-for-five-minutes-australian-pm-tells-residents



Australia’s prime minister, Anthony Albanese, has told residents they should turn their smartphones off and on again once a day as a cybersecurity measure – and tech experts agree. Albanese said the country needed to be proactive to thwart cyber risks, as he announced the appointment of Australia’s inaugural national cybersecurity coordinator. “We need to mobilise the private sector, we need to mobilise, as well, consumers,” the prime minister said on Friday. Sign up for a weekly email featuring our best reads “We all have a responsibility. Simple things, turn your phone off every night for five minutes. For people watching this, do that every 24 hours, do it while you’re brushing your teeth or whatever you’re doing.” The Australian government’s advice is not new. In 2020, the United State’s National Security Agency issued best-practice guidelines for mobile device security, which included rebooting smartphones once a week to prevent hacking. While a reboot every day may seem a basic measure, experts believe it can help, in some instances. Dr Priyadarsi Nanda is a senior lecturer at the University of Technology Sydney who specialises in cybersecurity development. He said rebooting a phone regularly could minimise risk because it forcibly closes any applications and processes running in the background that could maliciously be monitoring users or collecting data. Nanda said many users don’t realise their apps are often running in the background. “Given how much we use smartphones in our lives, we know of cases where people haven’t turned their phones off in an entire year,” Nanda said, noting people who rely on their phone’s alarm clock, for example, may need it on 24 hours a day. Nanda said some of the benefits of rebooting a phone could be achieved by regularly closing apps that might be running in the background. But there could be other malicious processes running on a compromised device that will only be stopped by turning the phone off. “If there’s a process running from the adversarial side, turning off the phone breaks the chain, even if it’s only for the time the phone is off, it certainly frustrates the potential hacker. “It may not fully protect you, but [rebooting] can make things more difficult” for hackers, Nanda said. Experts, while backing the advice of a regular reboot, have previously flagged the strategy is unlikely to stop determined hackers targeting a specific individual – especially in light of the proliferation of sophisticated technologies used to hack world leaders revealed in recent years. Dr Arash Shaghaghi, a senior lecturer in cybersecurity at the University of New South Wales, said daily rebooting was a good first step to “encourage users to adopt good cyberhygiene” because disconnecting can minimise certain risks. However, Shaghaghi warned against a false sense of security. “If your password is stolen and you disconnect your phone, you are not protected, and your account is still at risk. If attackers target a device, a temporary disconnect may be only an inconvenience for attackers,” he said. Some components of phones can remain active even if turned off. Shaghaghi said that with so-called zero click exploits – sophisticated attacks that don’t require an action from a user to give an adversary access – rebooting a smartphone “may challenge the attackers as they may need to find alternative means to exploit the device once powered back on”. “Rebooting your device regularly helps when your device is not compromised with persistent malware, as can turning on airplane mode.” Shaghaghi said smartphones can compromise privacy via apps that maliciously track location and listen to conversations. Being cautious of the applications users install and the permissions they grant is another important cybersafety step, he said.