Stop digital criminals with basic cyber hygiene practices, says expert

October 5 2023

Credit: Pixabay/CC0 Public Domain

Amid an escalating global cybercrime bill—now estimated at US$8 trillion a year—cybersecurity experts are calling for a new, more transparent, and collective approach to address cyberattacks.

While 99% of attempted cyberattacks are thwarted, the 1% that manage to slip through the net are wreaking not only economic damage, but significant reputational, legal, and personal harms.

Optus Chair of Cybersecurity and Data Science at the University of South Australia, Associate Professor Mamello Thinyane, says that individuals, companies, and governments must all share the responsibility.

"In the past, organizations have been unwilling to disclose their cyberattack experiences for fear of reputational damage and legal implications. However, it's important we strengthen our collective intelligence and reduce the barriers for companies that have been victims of cyberattacks. By sharing their experiences and lessons learned, we can build trusted networks and become smarter together," Assoc Prof Thinyane says.

"At an individual level, we can do so much more to lower the risks of cybercrime. Basic 'cyber hygiene' should be instilled in everyone. This includes protecting our accounts with multi-factor authentication, strong passwords, password managers, and being super vigilant around potential phishing attacks and scams."

As cyber threats become more sophisticated and lucrative, and artificial intelligence (AI) exposes the world to more security risks, the challenges are mounting.

AI is proving a double edged sword—helping bad actors to disrupt systems but also allowing authorities to strengthen digital security.

"The genie is out of the bottle. All of us are increasingly using digital technologies and devices with sensors and processing ability, such as wearable computers and smart home systems. While this benefits our

lives, it also makes us far more vulnerable to being hacked."

Ensuring that we only purchase safe and secure Internet of Things (IoT) devices, protecting them with strong passwords and multi-factor authentication, and keeping them regularly updated is part of basic cyber hygiene, Assoc Prof Thinyane says, but consumers are often lax about digital security.

"Think twice before clicking on that suspicious link or forwarding fake social media posts. Cyber criminals are very clever at exploiting human vulnerabilities and 82% of data breaches are linked to human factors, so we need to be very, very cautious.

"Digital technologies are here to stay, but for societies to thrive, we need to make our systems and data more secure, and we need to collectively become cyber resilient."

October 2023 is Cybersecurity Awareness Month, carrying the theme "Be cyber wise—don't compromise."

Provided by University of South Australia

Citation: Stop digital criminals with basic cyber hygiene practices, says expert (2023, October 5) retrieved 27 April 2024 from https://techxplore.com/news/2023-10-digital-criminals-basic-cyber-hygiene.html