tuanz
TECH USERS ASSOCIATION

Position Paper:

Improving our security and safety online

Problem

Cyber and online security is an issue that is never going to go away; it just keeps getting bigger every year. An increased reliance on digital devices post-pandemic and the growing number of open platforms and interconnected systems has created more opportunities for cyber criminals.

Valuable lessons can be learned from publicly disclosed cyber incidents and data breaches to help prevent other organisations from becoming victims in similar instances. However, cyber event disclosures tend to be generalised and not happening in a timely enough manner. More detailed insights into the key lessons learned are needed to help organisations effectively focus their investments and efforts against the current attack types.

In recent years, online scams have emerged as a rapidly growing problem, posing significant threats especially to individual users. The increasing prevalence of technology and the widespread use of the internet have provided scammers with a vast playground to exploit unsuspecting victims. Scammers are employing ever more sophisticated techniques to deceive and manipulate users, making it difficult to distinguish between legitimate and fraudulent activities. It is crucial for individuals to learn to remain vigilant, educated, and cautious while navigating the digital landscape to protect themselves from falling victim to these increasingly prevalent online scams.

Position

Develop a national strategy that leads to enforceable legislation and regulations. The strategy should ensure the enhancement of the capabilities of Government agencies in investigating and combating cyber security threats. This includes developing a coordinated approach within agencies that have cybercrime in their mandate.

Implementing guidelines encouraging more detailed cyber security disclosures including what information and key lessons learnt which need to be shared with the industry in a timely manner. Foster collaboration between government agencies, law enforcement, and private sector entities to share information and intelligence about emerging scams and cyber threats.

Prioritise the development of a digital identity system in Government that is enhanced and more sophisticated than that which is currently in use.

Prioritise the development of comprehensive privacy and data protection regulations that keep pace with technology, ensuring they address clear guidelines for the collection, use, and sharing of personal data, with a focus on obtaining informed consent, ensuring data security, and empowering individuals with control over their data.

Continue to invest in awareness campaigns through agencies like CERT to educate citizens about the various types of online scams, their modus operandi, and the precautionary measures they can take. This includes promoting digital literacy and responsible online behaviour from an early age. Further encourage public-private partnerships, especially in relevant industries such as the financial sector to combat online scams.

Recommendations

- → Develop a new national cyber security strategy.
- → Implement guidelines on cyber security disclosures.
- → Implement an improved Government digital identity system.
- → Develop comprehensive privacy and data protection regulations.
- → Instruct relevant Government agencies to develop public-private partnerships in specific industries.