FPP

BizNewz

Jan - May 2023

MANAGEMENT • INVESTMENT • ECONOMICS • ENTREPRENEURSHIP • TECHNOLOGY

BUKIT MERAH "THE RED FOREST"

PERMATA TERSEMBUNYI DI JERANTUT

TOXIC FRIENDSHIP

WHEN IT'S TIME TO LET GO

GRADUATES

WHO ARE THE URBAN POOR

ARROWS OF THE FAITHFUL

THE IMPORTANCE OF ARCHERY IN ISLAM

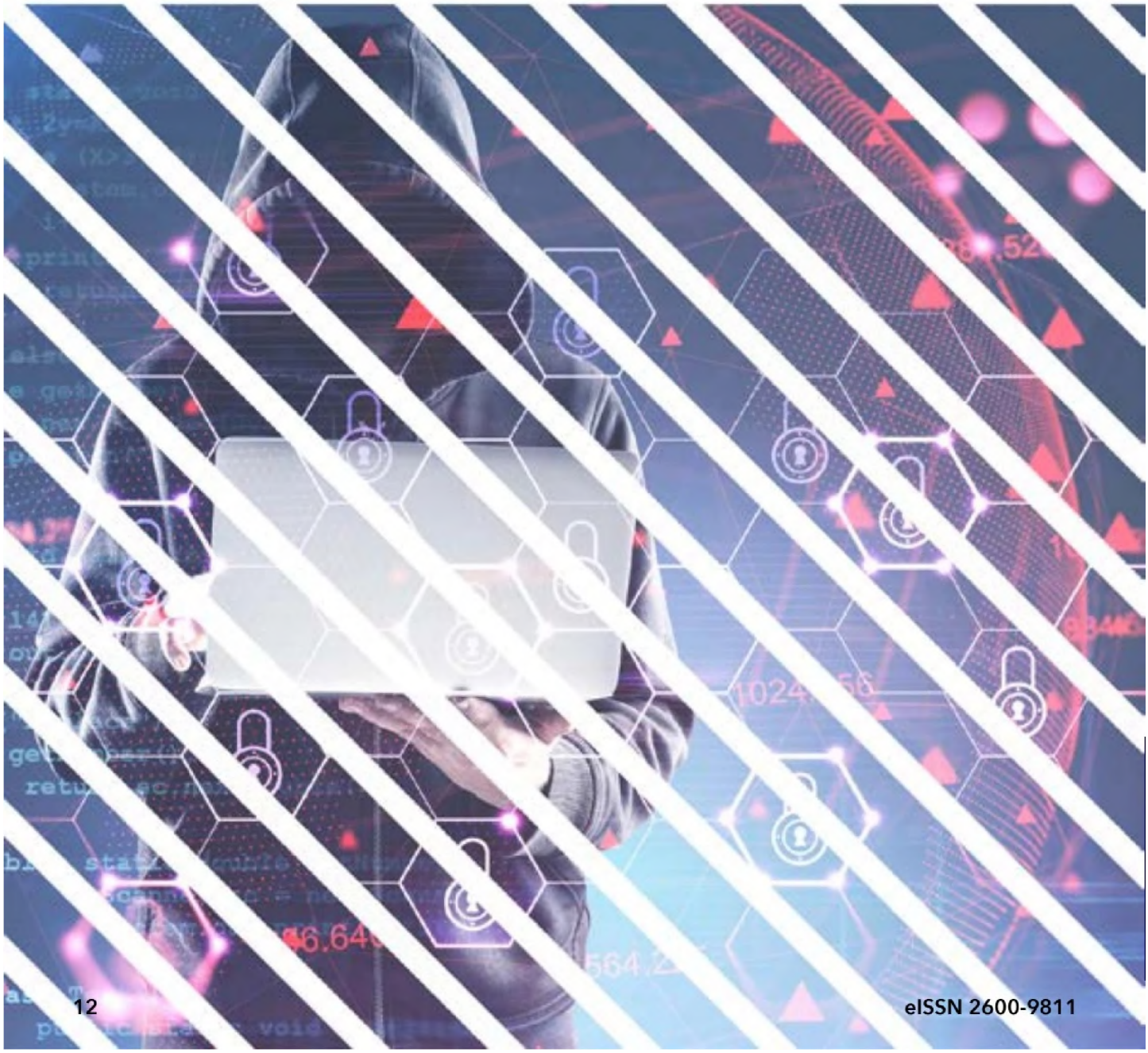
TWIN-TO-TWIN TRANSFUSION SYNDROME (TTTS)

eISSN 2600-9811

Publication Date
1 June 2023

CYBER SECURITY

HOW VULNERABLE ARE WE?



12 eISSN 2600-9811

By:
Marha Abdol Ghapar*, Azlina Shamsudin, Nazlin Emieza Ngah, and Nur Dalila Adenan
Faculty of Business and Management, Universiti Teknologi MARA Cawangan Terengganu, Terengganu
*Corresponding email: marha@uitm.edu.my

Whenever the term 'cyber security' arises, many ordinary people would think of passwords and biometric scanners. Well, it goes way beyond that. In the current digital era, cyber security is a major concern because it is undeniably true that we are susceptible to cyber-attacks. When technology and the Internet are used increasingly often, more and more data are kept digitally, which attract crooks. Cyber-attacks come in a wide variety and can be dangerous to people, companies, and even governments. Phishing frauds, malware infections, ransomware assaults, and data breaches are a few typical occurrences.

Any devices with an Internet connection have a potential to be hacked or be the target of a cyber-attack. This is due to the fact that Internet-connected devices are potential entrance points for cybercriminals. Hackers can use holes in software or hardware to access networks and devices without authorisation, steal confidential data, and engage in other malicious actions.

Today, this vulnerability is not only limited to devices, such as smart phones or computers, but also includes Internet of Things (IoT) gadgets. "What is IoT?", you asked. In a layman's term,

IoT refers to billions of physical objects that are connected to the Internet and are actively collecting and exchanging data (Ranger, 2020). IoT devices

include smart-home appliances, such as refrigerators, rice cookers, washing machines, microwaves, oven; and smart wears, such as smart watches; and also smart transportations, such as electric automobiles (Thomas, 2023).

There have been some memorable episodes from our favourite television shows called 'CSI: Cyber'. The first episode has portrayed the greatest fear among parents; Wi-Fi-enabled nanny cams have been hacked by criminals, who have studied the routine of a family, and at the right moment when everyone was being sound asleep, they kidnapped babies. To add salt to the wound, they have conducted online auctions to sell off the babies they have kidnapped to international buyers. Horrifying, isn't it? Another episode has shown that IoT home appliances have been hacked and have been remotely turned on without owners noticing, and they have been run excessively until the temperature has risen and finally caught on fire, which was spreading all over the residence, killing the residents who were sleeping at the time.

Meanwhile, smart watches also make users prone to danger since they unveil their real-time locations. People tend to have routines, for instance, one may go jogging on the same route daily at 5.00 p.m. in the evening. Thus, criminals may wait mid route to rob or kidnap the person, or maybe break and enter the person's home to steal valuable things since no one is at home at the moment.

In movies, you could see smart cars being remotely driven by hackers to cause harm, accidents, and grand theft auto intents. There are numerous ways for criminals to hack into your vehicle. The brake pedal and engine are prone to first-level attacks since they rely on an onboard computer's microprocessors (Garakh, 2022). Hackers who gain access to the

onboard computer can disable the brake or even halt the engine. Not only that but wipers, heaters, air conditioners, and the radio may have all been used by the hackers to impede the movement of the vehicle by being remotely operated and utilised to divert motorists. Besides, unreliable repair companies are capable of hacking by conning a diagnostics system into indicating that cars require repair when they do not actually need it, easily making money from the false unneeded repairs. Thus, it is crucial to choose only trustworthy mechanics and service centres.

Hence, it is wise to keep in mind that not all gadgets or systems are equally susceptible to online threats. Depending on elements like the robustness of their security features, the complexity of their software and hardware, and the regularity of security updates and patches, certain devices are safer than others. Even though the most secure systems can be compromised if attackers are determined enough, it is vital to remember that no system is totally error-proof.
There are precautions that can be taken to lessen the risk of cyberattacks, which are by using strong passwords that are both unique and complex, updating software with the most recent security patches, using antivirus software, and maintaining good online hygiene by avoiding dubious links, emails, or attachments from untrusted sources. These are all the examples of basic cyber-security hygiene that you should follow to secure all of your Internet-connected devices, and thus, ensure worry-free online experiences.

References:
Garakh, I. (2022). How easy is it to hack your car? Passwork. https://blog.passwork.pro/car-hacking/
Ranger, S. (2020). What is the IoT? Everything you need to know about the Internet of Things right now. ZDNet. https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/
Thomas, M. (2023). 29 Internet of Things Examples You Should Know. Built In. https://builtin.com/internet-things/iot-examples

BizNewz 2023
Faculty of Business and Management
Universiti Teknologi MARA Cawangan Terengganu, Kampus Dungun
Sura Hujung, 23000 Dungun, Terengganu, MALAYSIA
Tel: +609-8400400
Fax: +609-8403777
Email: biznewzuitm@gmail.com