WILFRIDUS BAMBANG TRIADI *Handaya, Founder,*
Website: https://tuwuhwutuh.com
LinkedIn: https://www.linkedin.com/in/wilfridus-handaya-46717153/

With 15 years experience in cybersecurity, Linux system administration, digital forensics, and higher education. Joined with various information security projects with government, private sector in Indonesia and overseas.

TIP 1. REGULAR OPERATING SYSTEM (OS) AND APPLICATION UPDATES

A few people don't care about the latest version of the OS or the applications used on their computers. Various reactions result, such as the process of using old updates until the computer's performance decreases. Using the latest version of the OS (and applications) is one way to keep your computer safe. In addition to security, the update process will significantly improve computer performance.

TIP 2. USE A STRONG PASSWORD

A password is essential to secure your digital account to the device you are using. To prevent hacking, you need to use a secure and strong password. All-access to critical data and information must be given a password with a unique combination of letters, characters, and numbers and enable double authentication so that hackers will have difficulty when attempting hacking. The more sensitive your information is, the more often you have to change your password. Once changed, don't use that password again for a very long time.

TIP 3. USE OFFICIAL SOFTWARE

Most people are no stranger to widely circulated pirated software. Some inherent dangers threaten your security from this software. Similarly, on mobile devices, make sure users only install apps from the default store as a safe and trusted place for the whole world to find apps that meet high standards of privacy, security, and content. If you are still using pirated software, immediately replace it with the original software because you will get benefits such as avoiding potential viruses and malware and qualify for regular updates from the provider.

TIP 4. DESIGN A SECURE SYSTEM AND IMPLEMENT AN ACCESS RIGHTS

In creating an IT system, you must distinguish the access rights of each user according to their needs. Eliminate unnecessary access to hardware, software, or storage space and monitor every user who logs in. If possible, you can create a unique username and password to monitor each user directly.

TIP 5. REGULARLY BACKUP DATA

Data backup is one of the best guarantees for users in overcoming virtual interference. Some of the incidents that occur are by deleting data (data loss) from the computer. In some situations, data loss occurs when data is accidentally deleted, or something causes data to become corrupted. This activity must be done regularly, scheduled, and placed on devices that vary on location and storage media. The benefits are that you can briefly duplicate the data, restore data if data is lost, provide data protection, ease accessing data, and anticipate when the operating system is accidentally problematic.

TIP 6. PROVIDE BASIC IT SECURITY TRAINING REGULARLY

People who are still public in the field of IT become the easiest targets, especially by hackers. Consistent and continuous distribution of information and training to all elements in the company is one part of building cyber resiliency. Evaluate potential cyber-attacks constantly mitigates the risks of maintaining data and information security. Increasing awareness and improving information security knowledge and skills become mandatory needs and shared responsibility for all system users.

TIP 7. BE CAREFUL WHEN OPENING UNKNOWN OR SPAM EMAILS

It is advisable to consider all your email data as important - ranging from your name, address, place of birth, passwords, phone number, and other related data. It would be best always to be vigilant lest emails fall into the hands of irresponsible people. Users are advised not to download the attachments directly or click the links sent to emails from unclear addresses. Especially emails with interesting titles usually related to finance or advertising such as gifts, vouchers, discounts, and related advertisements. It would be best to confirm that the sender is correct before opening any message. One example of a commonly used attack utilizing a user's inattention in opening any unknown email is email phishing. It became a popular choice among hackers because it is cheap, and its ease and effectiveness are quite high.

TIP 8. USE ANTIVIRUS AND ANTISPAM

Antivirus works to maintain all your systems' security. With an effective antivirus, you will avoid malicious programs that damage (or steal) your personal information. Various vendors have provided antivirus and antispam with multiple advantages and disadvantages, respectively. Users need to be smart to choose the right tool with the needs of the company. Consider buying the paid version of antivirus software which offers more advantages over the free version for more protection, such as support, updates, and obstacles faced during the tool's operation.

TIP 9. DO NOT GIVE PERSONAL INFORMATION TO A LESS CREDIBLE SYSTEM

Be careful not to share personal information when using public connections because it is prone to hacking. Also, make sure that personal data is used in interacting with the system is given to a secure and reliable system. That personal data could be taken by hackers - who can then claim to be you to commit fraud to your relatives and friends. In addition, personal data becomes an asset that can be sold on the Internet. Try to limit personal information to avoid cybercrime.

TIP 10. USE SSL (SECURE SOCKETS LAYER) PROTECTED WEBSITE

SSL establishes a secure connection on the website to transmit essential data from the server to the client and vice versa. This technology allows sensitive information such as credit card numbers, social security numbers, and login credentials to be securely sent. The data sent has been encrypted and scrambled to make it difficult for hackers to access. SSL also serves as authentication, which means SSL will ensure the data is secure when you send the information to the right server.