**WILLY SUSILO,** *Distinguished Professor, IEEE Fellow, Head of School of Computing and Information Technology, University of Wollongong (Cybersecurity Expert, IEEE Fellow, IET Fellow, ACS Fellow)*
LinkedIn/Website: www.linkedin.com/in/willy-susilo-295591b/
https://sites.google.com/view/willy-susilo/about-me

Willy has over 22 years of experience in cybersecurity and cryptography domain. He has published more than 600 articles in prestigious journals and conferences. He was appointed as an IEEE Fellow due to his contributions in the area of cloud computing security

## TIP 1. BACKUP YOUR DATA

The most valuable resource these days are data. Unfortunately, hackers tend to steal or corrupt your data via several means, including ransomware. It is always important to backup your data, both on-prem and in the cloud, to ensure you have several replicas in case data is lost.

## TIP 2. CLOUD IS YOUR FRIEND

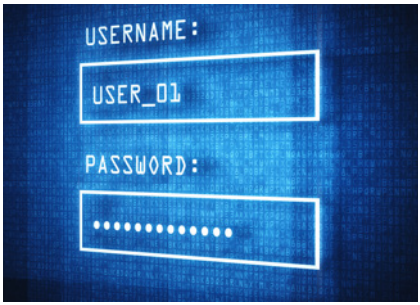
Make good use of cloud technology to store your data securely. Specifically, when dealing with sensitive data, it is advisable not to store the data in plaintext but rather to encrypt them before storing them in the cloud. Multiple techniques are available to secure sensitive data in the cloud, and users need to use those technologies to secure their data.

## TIP 3. CRYPTOGRAPHY IS IMPORTANT

It is essential to understand the importance of cryptography, even though you may only need to know its basics. Cryptography is the fundamental technique to secure an insecure environment. You can secure your data with cryptography, but using the correct cryptography is very important.

## TIP 4. A STRONG PASSWORD IS ESSENTIAL

Try to create a mechanism in your head to create a strong password. Password is the key to allowing anyone to access your resources. Therefore, it is crucial that hackers cannot even guess the password you use. Having a strong password usually means it is hard to remember. This is always a challenge, and it can be overcome using a password generator that can be saved using some utilities to store your primary password. Using multi-factor authentication will provide extra protection.




## TIP 5. DO NOT USE COMMON WORDS AS YOUR PASSWORD PROTECTION

Sometimes, it is easy to think that we should use the words we are familiar with or use our families' names as our passwords. However, they are susceptible to social engineering. Therefore, it is better to avoid using those familiar words, even though they are tempting to be used.

## TIP 6. STAY CALM, DON'T PANIC

You may receive some emails that may threaten you, or state that you have not paid your debt, or ask you to pay a delivery fee or else your goods will not be delivered. Please stay calm. Do not panic. When you panic, you may tend to do things you do not want to happen, such as clicking the link provided, even though you may eventually think that this would be a phishing email.

### TIP 7. DO NOT ALWAYS TRUST YOUR EYES AND THEN QUICKLY ACTION

You may receive a message, in an SMS, or an email stating that you must do something urgently. Just use your common sense and do not act too quickly. They may be a phishing message luring you to go to a fraudulent website which eventually can steal your credentials.

### TIP 8. HAVE A TRUSTED CIRCLE

You should build a trusted circle among your connections. When there is any issue, you can always check with your trusted circle whether those kinds of actions would be wise to do. As stated in the previous tips, it is always good to think properly before actioning on anything.

### TIP 9. BEWARE OF FREEBIES

Occasionally, you may be offered something very friendly present on the Internet while you did not ask for it. Think about whether you have asked for them, or deserve those nice things due to your work. Unfortunately, there is no free lunch. Most of them are provided by scammers who eventually will disadvantage your interest.


### TIP 10. BE CAREFUL OF PUBLIC WIFI

Public WiFi is great when you want to connect quickly, especially when you are travelling. However, it would be best to be careful that important credentials may be stolen when you use public WiFi. So make sure you turn on some protections, such as VPN, before using public WiFi.