DR. SYED AFAQ SHAH, *Senior Lecturer, Edith Cowan University*

LinkedIn/Websitehttps://au.linkedin.com/in/syed-afaq-shah-macs-cp-94820525

Dr. Syed Afaq Shah is a computer scientist with over 17 years of academic research and industry experience. He is also a founder of Intelligaroo, a business that provides artificial intelligence solutions. He has authored over 50 research papers, including a book and two book chapters. He develops reliable and trustworthy artificial intelligence systems with improved resilience to adversarial attacks. He is an Associate Editor of 'Network: Computation in Neural Systems' and 'Frontier in Artificial Intelligence' journals. He is a regular speaker for international conferences.

TIP 1. DISABLE BLUETOOTH CONNECTION

Disable your Bluetooth connectivity when not in use because as a wireless data transfer standard, Bluetooth has some associated cyber security risks. You don't want unauthorised parties to access the data you're transferring via Bluetooth. Avoid using Bluetooth to communicate sensitive information like passwords and such. Only leave your Bluetooth in "discoverable" mode when you're pairing a new peripheral with your phone or laptop. And overall, you should turn Bluetooth off when you're not using it.

TIP 2. STRONG PASSWORDS

We all want our data and personal information to be protected, yet we often rely on the same weak passwords for all our accounts because memorising multiple, complex passwords can be a pain. Unfortunately, this isn't just lazy -- it's dangerous. My advice is to ensure different and complex passwords for social and financial purposes.

TIP 3. EMAIL ATTACHMENTS

Malicious emails remain some of the most common and destructive computer security threats faced by businesses today. Cybercriminals use email-based attacks to steal login credentials, lure individuals into clicking malicious links, and deliver malware. So don't open links or attachments from strangers.

TIP 4. BACK UP YOUR DATA

One should follow the best practices to backup critical data. Incremental local backups are the best plan for less critical information, but the most important data (such as financial data, client details, etc,) should be backed up to a cloud location at a good geographical distance. If you use a laptop, make sure everything on it is backed up to a desktop or other storage regularly in case of theft, loss, or damage. Backing up your data is vital for your company's future and success.

TIP 5. AUTO-LOCK ON PORTABLE DEVICES

Use screen lock or auto-lock on your mobile devices. If someone gets hold of your mobile device and there's no lock screen, the attacker suddenly has access to everything on your device. While some of your apps will require passwords and multifactor authentication, many apps, like your photos and notes, typically do not. Also, if you don't log out of your social media or email accounts on your devices, the attacker can have a field day pretending to be you. For this reason, you should have a lock screen installed on your device, and it should be difficult to get past.

TIP 6. WIRELESS NETWORK ENCRYPTION

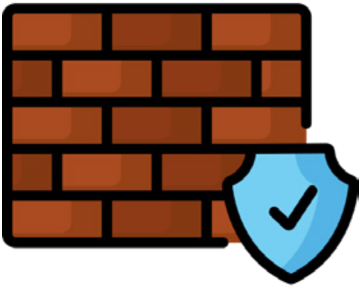
Switch on encryption on your wireless network. Wireless encryption is used to secure your wireless network with an authentication protocol that requires a password or network key when a user or device tries to connect. If your wireless network is not secured with some type of encryption; unauthorised users could access your network and obtain personal information, or use your Internet connection for malicious or illegal activity. Also, your network speed or performance may decrease if people are using your network without your knowledge.

TIP 7. AUTO UPDATE

Auto update ensures your patching is up to date. If you don't perform updates, your security will - over time - continue to get weaker, as vulnerabilities are left open and are available to be exploited. Automatic software updates are simply a means of performing these updates automatically, with the need to download or install them as a user. They can be very useful if utilised properly.

TIP 8. ENABLE FIREWALL

As much of the business world continues to go digital, it is imperative that forward-thinking companies focus on securing their systems from external threats. One of the ways to achieve this is through enabling your firewalls, which serve as a first line of defence to external threats, malware, and hackers trying to gain access to your data and systems. Firewall security is the first step in helping your business grow safely in the ever-changing digital age. Even if your business only relies on technology and networks for a small piece of your operations, it is still equally important that you take proactive steps to keep things protected.



TIP 9. REPORT SUSPICIOUS EMAILS

My next tip is to report emails that you suspect so that others stay protected. Phishing emails are much harder to identify than most people realize. While you may laugh off the obvious ones, hackers are getting smarter and much more sophisticated at dressing up their phony emails to come off as the real deal. Recipients should immediately report suspicious emails to their IT departments.

TIP 10. CHANGE DEFAULT PASSWORDS STRAIGHTAWAY

Default passwords are intended for initial testing, installation, and configuration operations, and many vendors recommend changing the default password before deploying the system in a production environment. Attackers can easily obtain default passwords and identify internet-connected target systems. Change default passwords as soon as possible and absolutely before deploying the system on an untrusted network such as the internet.

Finally, if something seems too good to be true, that may be because it isn't true.