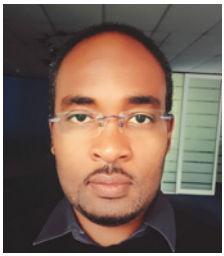

DR. MOHAMED ELYAS, *Research Fellow, CSRIC, Holmes Institute*
https://au.linkedin.com/in/melyas

Dr Elyas is a cybersecurity professional with over 14 years of experience. He currently works as a research fellow at CSRIC, Holmes Institute. He has a PhD in cybersecurity and forensics, master's in information security and bachelor's in mathematics and computer science. Dr Elyas led several initiatives to raise the public awareness of good cybersecurity practice. His current work revolves around the security and privacy of the Internet of Things.

TIP 1. PURCHASE YOUR DEVICE FORM A TRUSTED VENDOR

It may be tempting to base your purchase decision of seemingly similar smart devices on price. Unfortunately, by doing so you may end up losing more in the long-term. All other purchasing factors aside, look for reputable vendors with strong security mindset to purchase your smart devices from – that is: vendors who make explicit claims about security features built into their devices. Verify their claims by reading independent expert reviews.

TIP 2. KNOW WHAT IS CONNECTED TO YOUR NETWORK

A key premise in the Internet of Things is having everything connected to the Internet, that is: EVERYTHING. Thus, it is imperative that you scan your corporate network to know what is connected to it. Forget about security risks that smart technologies may pose to your own network, some smart devices are notoriously vulnerable to proxy attacks. This means your company may end up being liable for attacks perpetrated against OTHER companies.

TIP 3. SEGREGATE YOUR NETWORK

Consider configuring your router such that smart devices are connected to a separate network to that of your main IT. By doing so, any security threats introduced by smart technologies remain isolated from mission-critical servers and the wider network. You can segregate your network by creating separate SSIDs (Service Set Identifier) or activating a guest network. In either case, each device must be fully identified and authenticated before being allowed into your network.

TIP 4. ENCRYPT COMMUNICATIONS

Information communicated in plaintext can easily be intercepted by bad actors. While encryption does not prevent eavesdropping, intercepted information is rendered useless when encrypted. Read the product manual prior to purchasing an IoT device to ensure that data is encrypted at rest and in transit. This is especially important for devices handling sensitive or personally identifiable information. Light cryptography can be used to protect devices with limited computational resources or power.

TIP 5. CHANGE DEFAULT PASSWORDS

In some instances, a password can be the first (and possibly last) line of defence against unauthorised access to a smart device. To enable the initial set-up of a device, a default password is often provided. Many users forget to change the default password, which makes it easy for bad actors to gain access. Remember to change the default credentials when configuring a new device and create a strong password.

TIP 6. FULLY UNDERSTAND YOUR DEVICE

Smart technologies come in all shapes and flavours and it can sometimes be hard to know what data they collect, for what purpose and who will have access to the data. It is important to carefully review product manuals, and the terms and conditions, to fully understand how a device functions to remain in charge of your data. It is also important to understand how the collected data will be secured.

TIP 7. DISCONNECT FROM THE INTERNET

A so-called 'smart device' does not need to always be online to function. Manufacturers know that the value of their product goes off the roof when labelled as 'smart'. Ask yourself whether a device really needs to go online to properly function. If not (or when not in use), disconnect it from the Internet to reduce the risk factor. Also make sure to disable unnecessary functions and deny non-essential permissions.

TIP 8. APPLY SOFTWARE UPDATES

Software updates are often released to add a new functionality, improve an existing functionality or patch security vulnerabilities. If not applied in time, your device may fall victim to cyber attacks. For this reason, it is crucial that you set-up a schedule to update the software and firmware of your smart devices. Critical security updates must be applied immediately. You should also be mindful of product's end-of-life, where technical support discontinues.

TIP 9. BACKUP YOUR DATA

They say prevention is better than cure, so make sure to back-up your data before disaster strikes. You may want to set-up a daily schedule to back-up data collected by smart technologies or sync it to the cloud. Also make sure that you can remotely wipe data out of missing or stolen devices – especially if sensitive information is involved. Use a reputable provider when you back-up data to the cloud.

TIP 10. SAFELY DECOMMISSION YOUR DEVICE

So, you have been long-served by your smart device and now you want to say goodbye? Awesome, you are completely within your rights, but remember do so safely. You may think data stored in a device is gone for good once deleted. Unfortunately, that's not entirely accurate – it CAN almost always be recovered. Thus, to safely sell or decommission an unwanted device, consider removing (or wiping) its storage media beforehand.