MODULE 3

ENHANCING DIGITAL SECURITY

PUBLICATION DETAILS PAGE

First published in March 2020

PUBLISHED BY :
MinorMatters an initiative by the National Christian Evangelical Alliance of Sri Lanka

WEB : www.minormatters.org

EDITOR: Nalaka Gunawardene

PROJECT COORDINATION BY:

Yamini Ravindran, *Director, Legal and Advocacy*
Shalomi Daniel, *Legal and Advocacy Coordinator, Religious Liberty & Social Justice Commission*
Akshina Palihawadana, *Media Strategy Officer, Religious Liberty & Social Justice Commission*

COVER DESIGN: Sanjayan Ariadurai

PAGE LAYOUT AND DESIGN: Shenal Jesudian

DISCLAIMER:
The analysis and opinions expressed in this publication are those of the contributors and editors. They are not necessarily those of the National Christian Evangelical Alliance of Sri Lanka, and do not commit the organisation.

MODULE 3

ENHANCING DIGITAL SECURITY

The internet is a global network of computers that are inter-connected electronically in a way that they can exchange information.

To use a physical world analogy, the internet works like the postal system, but it delivers messages at the speed of light and is far more intricate. Just as the postal service enables people to send one another envelopes containing messages, the internet enables computers to send one another small packets of digital data.

Billions of different devices are connected to the global internet. Among them are supercomputers, personal computers (desktops, laptops or tablets), smartphones and other specialist devices produced by thousands of different manufacturers.

To be able to exchange data among these different devices, they all use a common 'language': a technical standard called TCP/IP (Transmission Control Protocol/Internet Protocol). And every device that connects also has an internet protocol or IP address.

When you post a letter, the postal system handles all the logistics: you don't need to know or worry about its collection, sorting, transporting and eventual delivery. Similarly, packets of internet data are transmitted through a variety of cables, routers and host computers on the way to their destination.

By the end of 2018, an estimated 3.9 billion people were using the internet along with tens of millions of entities that includes governments, companies, charities and other organizations. For the most part, their web using experience is safe and satisfactory. But when so many users and so many devices are connected, sometimes things go wrong. That is why digital security or cyber security is important.

Cybersecurity is about systems and things; cyber safety is about people. In this module we cover the basics of digital security (protecting your digital systems and devices). The next module on cyber safety covers the safety of persons when using digital services.

KEY TERMS

Digital security (also called Information Technology security or IT security): implementing systems to protect and safeguard information stored digitally. These devices may or may not be connected to the internet. In a computing context, security includes both physical security and cybersecurity.

Cybersecurity: Precautions taken to guard digital devices connected to the internet, especially to prevent unauthorized access to (or attack on) computer systems and data.

Cloud computing means storing and accessing data and programs over the internet instead of storing data on a computer's hard drive. The 'cloud' is only a metaphor for the internet.

Source: https://searchsecurity.techtarget.com/definition/cybersecurity

BASICS OF DIGITAL SECURITY AND CYBERSECURITY

When we use any digital system, we enter our data which can include personal data, confidential official data of organizations we work with, creative content and other kinds of data. When we connect to a network of computers – whether one within an organization or on the global internet – we come across other people's data.

It is necessary to protect our own data and devices, and also respect the security of others' data and devices. In an inter-connected network like the internet, everyone needs to pay attention to security because one user's weakness can affect everyone!

Digital security and cybersecurity is not just to guard against unauthorized access. We also need to be careful of accidental data damage or loss by ourselves or anyone else authorized to handle our data. Unforeseen events like floods, fires and electric power surges can also damage data.

Digital security and cybersecurity does not mean having highly complex security systems. Sometimes the best solution may not be very technical. It is also important to keep re-evaluating security practices as new threats keep emerging, especially on the internet.

Please remember: good digital security and cybersecurity requires user involvement, responsibility and vigilance. This is not something that can be 'outsourced' to a vendor that supplied the hardware or software, or to an IT professional or systems administrator.

It is not possible to list here all the steps necessary for digital security and cybersecurity – plenty of free advice is available online. Discussed below are a few basic tips, which represents a commonsense approach.

Source: https://wiobyrne.com/digital-hygiene/

DIGITAL HYGIENE MATTERS!

Digital hygiene is a term used to describe the cleanliness or uncleanliness of one's digital devices, accounts and data.

Good digital hygiene is important both at home and at work. A single compromised account or device could result in someone gaining access to your devices or accounts. If this is done maliciously, that means that someone could lead an attack on your data by stealing files, cracking passwords, hacking accounts, or worse.

HOW TO PROTECT YOUR DATA FROM COMPUTER VIRUSES AND MALWARE

Computer viruses are small programs that spread from one computer to another via emails, email attachments or accessories like USB drives. Viruses can modify or destroy any data and disrupt normal operation of the operating system.

- Use an up to date anti-virus program.
- Make sure your operating system (like Windows) and web browsers (like FireFox and Chrome) are up-to-date. Their latest versions will offer better protection.
- Be cautious with emails links: do not open unknown attachments or content (links) even from a known source.
- Use pop-up blocker for your browser.
- Use a pop-up blocker for your browser. Many pop-ups are spyware and adware that come with malicious payloads and can damage your system.
- Install a firewall: this is a program that screens incoming internet and network traffic. Along with your virus program, it can help prevent unauthorized access to your device.
- Password protect the administrator account.

Note: A device may not always show symptoms even if it is infected. Always perform regular system checks and virus scans to make sure your device is clean.

SYMPTOMS OF A VIRUS INFECTION

Here are a few common symptoms indicating a malware infection:

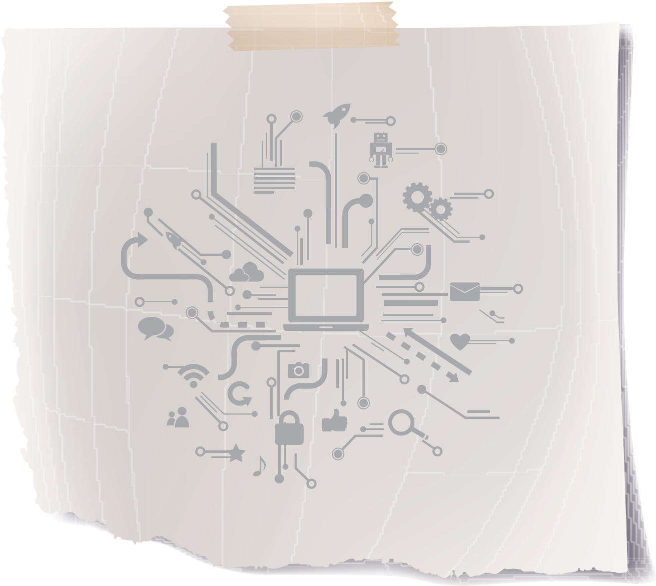
- The device will start to slow down without good reason.
- The device will abruptly restart itself often and will show abnormal behavior.
- Applications installed on the device will not function as expected.
- There might be unusual (typically badly written) error messages.
- There might be new shortcuts or other icons in the device that were not created by the user.
- Lack of storage space.
- Files or applications have been deleted without permission.

BACKING-UP DATA

Data corruption or loss can happen even with the best hardware and software. Data backup is a process of duplicating data to allow retrieval of the duplicate set after a data loss event.

A common data backup method is to download data from a computer's hard drive on to small portable devices like external drives or high capacity USB drives. There is also the option of backing up data remotely to the 'cloud' (web-based data storage, such as Google).

Cloud backup allows users to copy their data to hardware in a remote location. Users can access their data anytime on any device via the internet (when properly accessed). Cloud storage makes it easy to manage data. Most cloud storage service provide a large amount of storage space and encrypt the content for data security. (Some services providers like Google offer a basic online storage capacity for free when we sign up).



ENCRYPTING DATA

Encryption is the process of using an algorithm (automated software) to make data unreadable for unauthorized users. This protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text. Such data may only be decrypted or made readable with a 'key'.

Encrypting data is like storing it in a safe - only those who have the access key can read it. Encryption is a digital form of cryptography, which uses mathematical algorithms to scramble messages, so that only those who have the sender's key (or cipher) can decode the message. Anyone else intercepting encrypted data will see junk.

There are two main methods of encryption: symmetric encryption, which involves securing data with a single private key, and asymmetric encryption, which uses a combination of multiple keys that are both public and private.

Encryption is especially important when communicating through the internet, e.g. email, chat applications and other exchanges. If messages are not encrypted, there are ways for malicious eavesdroppers to intercept or even alter the messages.

End-to-end encryption (E2EE) is a system of communication where only the communicating users can read the messages. It prevents potential eavesdroppers – including telecom providers, internet providers, and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the digital exchange.

Encryption allows making your communication trusted and confidential. When it comes to end-to-end communication over the internet, example include services like WhatsApp, iMessage and Signal (in which E2EE is turned on by default) or Telegram.

DESTROYING SENSITIVE DATA

When you delete a file in your computer, it does not disappear completely. It only removes the reference of the file from the file system table. The file remains on the disk until another file is created over it, and even after that, it might still be possible to recover that data.

If you want to completely get rid of any data, it is best to use a secure deletion tool: it replaces or overwrites the sensitive information. Even after that, digital information could still be read by a skilled person who knows how to recover data.

A process called 'wiping' overwrites files with random data several times. Eraser is another advanced security tool for Windows, which allows users to completely remove sensitive data from the hard drive by overwriting it several times with carefully selected patterns.
Https://eraser.Heidi.Ie/

PROTECTING YOUR DATA WHEN ONLINE

Wi-Fi or wireless internet means connecting to a network using radio waves, without needing wires. It liberates users to remain connected to the internet as they move around, but this facility needs to be used with caution.

Public Wi-Fi can be found in public places like airports, coffee shops, shopping malls, restaurants and hotels — it allows you to access the internet for free. While it is ok to use public Wi-Fi to check social media or browse news articles, it is not advisable for reading email or accessing a bank account.

Why? Because using public Wi-Fi networks increases chances of your data being intercepted by someone else on that network. In fact, it is best to avoid Public Wi-Fi ‘hotspots’ that are run by people you do not know or trust. Criminals can set up hotspots known as 'evil twins' and 'rogue hotspots' to steal users' information.

Another precaution: always study privacy settings on social media platforms as well as other websites. You can often find privacy controls on a site by navigating to a control panel or settings menu. Privacy controls may also be offered during the sign-up process for a new online service or account. Always explore and understand privacy controls available to you on a given website before exploring.

Also, please remember to sign out of your accounts – especially if you use a shared device for accessing your email, social media or another service that requires login. Users at cyber cafes often forget to sign out from their accounts – whoever next uses that shared facility can easily get into your accounts, and even highjack them!

PROTECTING DIGITAL ASSETS

A few simple but important precautions can help protect your digital assets.

A password, also called a passcode, is a memorized secret used to confirm the identity of a user. In the digital context, it is a combination of letters, numbers or punctuation marks arranged in a specific manner.

Using secure passwords is an important step in protecting your digital assets from unauthorized access or hacking. A password need not be an actual word: a non-word may be harder to guess, which is a desirable property of passwords.

Here are a few basic tips for better password protection:

- Always pick strong passwords to secure your accounts. Use a long password made up of numbers, symbols and uppercase and lowercase letters.
- Try using a phrase that only you know as the password
- Avoid using obvious personal information such as your birthday, anniversary, address, city of birth, high school, and relatives and pets
- Use a unique password for each of your accounts: Reusing passwords for important accounts is risky. If someone gets your password for one account, they could access your email, address and even your bank accounts.
- Remember to setup your password recovery options if you forget a password
- Change your passwords regularly - the more often you change your password is better
- Allowing web browsers to remember your passwords may seem convenient but is a risky practice. If someone else enters your device, they can easily access all your accounts.

WHAT ARE DIGITAL ASSETS?

In the simplest terms, a digital asset is content that is stored digitally. That could mean images, photos, videos, files containing text, spreadsheets, or slide sets. Digital assets may be stored on a computer's hard drive, in a smartphone memory or online.

Digital assets also include your accounts for key digital services like email and social media.

USING TWO-STEP AUTHENTICATION

After setting up strong passwords, the next most important step is to enable two factor authentication (also known as two step verification or two step authentication).

It means that in addition to a password, you will need to provide a second piece of information to log in to your accounts -- usually a code that is sent to your registered mobile phone as a text message or SMS (and is valid only for a single use within a few minutes). All major social media platforms, as well as services like Google have now introduced two step authentication as a security option.

If a web service supports both text- and app-based two factor authentication, please select app-based. This is because SMS text messages are not encrypted, and could therefore be intercepted.

PASSWORDS ARE SECRETS!

Passwords are meant to be personal and confidential. They are not for sharing. And certainly not for display in any manner or form. Yet this is one of the most common mistakes many people and some organizations make – often to later regret. So please remember: a password can protect your digital assets only if you keep it secret!

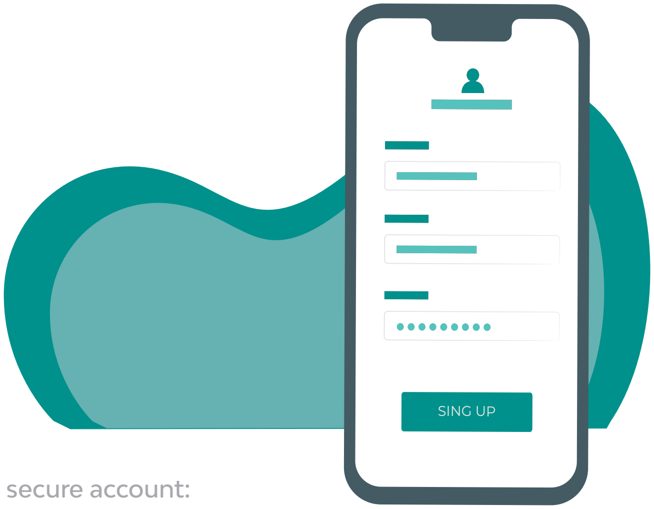
MOBILE PHONE SECURITY

Every mobile phone, GSM modem or device with a built-in phone/modem has a unique 15-digit IMEI (International Mobile Equipment Identity) number.

The IMEI was created because the SIM card number cannot be a permanent identifier of the device. (SIM Card is associated with the user and can be easily transferred from the phone to another phone.) Based on the IMEI number, you can check some information about the device, e.g. its brand and model.

The easiest way to check IMEI on any phone is to use the *#06# sequence. The IMEI number is useful when you would like to send the device for service to fill out warranty forms. Besides that, if you want to report a stolen or a lost phone at the police or network operator, you will need to know the IMEI number. After that you can ask your phone to be blocked, after which the device will be unusable, whether or not the SIM card is changed.

Please make sure you know your phone's IMEI number and have it written somewhere.



[1] Google has some useful advice on creating a strong password and a more secure account: https://support.google.com/accounts/answer/32040?hl=en

Here are a few basic tips for enhancing the security of your mobile phone:

- Set a strong pin number for activating the phone: use a six-digit code minimum.
- Download software updates regularly
- Get antivirus or anti-malware protection for your mobile devices.
- Download apps only from trusted platforms (e.g. Google play store and Apple app store)
- Control app permissions: Both Android and IOS systems have tools to make it easier to control exactly what each app on your devices can and cannot access. Limit the permissions so apps only have permissions to access data that it really needs to function. (Mypermissions.Com is a handy tool that allows you to check your permission settings across a multitude of apps, get reminders to clean your permissions with mobile-friendly apps, and get alerts when apps access your personal information so that you can remove it with a single click)
- Enable remote location and device-wiping: If your device is lost or stolen, tracking apps can tell you where your phone is. These apps also let you wipe sensitive information remotely.
- Disable Bluetooth when you are not using it: Bluetooth opens the door for vulnerabilities. Bluetooth attacks depend on exploiting the permission request/grant process that is the backbone of Bluetooth connectivity. The only way to completely prevent attackers from exploiting that is to turn off the Bluetooth function when not in use. Putting it into invisible or undetectable mode can still expose your device to Bluetooth attacks.

DIGITAL IDENTITY THEFT

Identity theft can happen both online and offline. It means the unauthorized collection of personal information and its subsequent use for criminal purposes such as to open credit cards and bank accounts, redirect mail or email, obtain a mobile phone connection, etc. The consequences can be very serious for the victim.

There are many ways in which an individual's identity can be stolen. People are vulnerable to this when using online services, where criminals can gain access to personal information through different ways.

Identity thieves have several ways of stealing personal information via electronic means. These include:

- Retrieving stored data from discarded electronic equipment such as PCs, mobile phones or USB memory sticks
- Stealing personal information using malware such as keystroke logging or spyware
- Hacking computer systems and databases to gain unauthorized access to large amounts of personal data
- Phishing, which means impersonating trusted organizations (such as a bank or a retailer) via email or SMS messages and prompting users to enter personal financial information
- Compromising weak login passwords (often through calculated guesswork) to gain access to a user's online accounts
- Using social networking sites to attain enough personal details to guess email passwords or impersonate the victim in other ways online
- Diverting victims' emails to attain personal information such as bank and credit card statements, or to prevent the victim from discovering that new accounts have been opened in his/her name

We cannot totally avoid the hazard of identity theft, but we can safeguard ourselves through awareness and constant vigilance. Here are a few tips offered by an online source:

- Beware of being redirected to a “middle-man” website when you think you are on a secure site, such as your bank’s webpage. Check for suspicious URLs.
- Keep track of your credit card and banking statements to check for any suspicious transactions.
- Use only secure websites for financial transactions. If you enter credit card information online to make a purchase, you should see a lock in your browser’s status bar, usually in the left corner. If you don’t see the lock, don’t enter your information.
- Don’t answer emails or follow links in emails claiming to be from reputable institutions like your bank or university that ask for personal information. Contact the institution in question via phone or their website about these emails.
- Use common sense. If an offer sounds too good to be true (“Just enter your credit card number for a free trip to Paris!”), it is likely to be a scam!
- Don’t send any personal information when using public WiFi.
- Look out for emails claiming to be from companies such as Norton Anti-Virus that prompt you to download something. Get in touch with the company independently (do not reply to the email itself) to check on the information.

[2] More information at: https://www.imei.info/
[3] Source: https://www.techopedia.com/definition/13637/identity-theft

CASE STUDIES

CASE STUDY 1: DATA DETOX KIT

It can be difficult to know where to start when it comes to reducing your data trail, becoming more digitally secure, or building a healthier relationship with technology. As our devices become more intertwined with our personal lives, it helps to find a balance.

The Data Detox Kit is a simple, accessible toolkit that walks you through the steps you can take towards a healthier online self. It takes a holistic approach, going through the different aspects of your digital life, from the amount of time you spend on your phone, to the apps that you use, to the passwords you set.

The Data Detox Kit has been produced by Tactical Tech, an international non-profit organization that engages with citizens and civil-society groups to explore and mitigate the impacts of technology on society.

Its printed version has been translated into Dutch, French, German, Indonesian, Norwegian, Polish, Portuguese, Spanish and Swedish. You can request a PDF copy at datadetox@tacticaltech.org, indicating the language you need, as well as your idea of how and where you'd like to use it.

Website: https://datadetoxkit.org/en/home

[4] Source: http://www.digitalresponsibility.org/how-to-avoid-online-identity-theft

CASE STUDY 2: THE DIGITAL FIRST AID KIT

The Digital First Aid Kit came about when a number of organizations working in the digital emergency field observed that once a person is targeted digitally, he or she often does not know what to do or where to turn for assistance. It was inspired by the belief that everyone has the ability to take preventative measures to avoid emergencies and responsive steps when they are in trouble.

The Digital First Aid Kit aims to provide preliminary support for people facing the most common types of digital threats. The Kit offers a set of self-diagnostic tools for human rights defenders, bloggers, activists and journalists facing attacks themselves, as well as providing guidelines for digital first responders to assist a person under threat.

The Kit begins with ways to establish secure communication when you or a contact are facing a digital threat and want to reach out for support. The Kit then moves on to sections on account hijacking, seizure of devices, malware infections and DDoS attacks.

These questions will guide you through a self-assessment or help a first responder better understand the challenges you are facing. It then lays out initial steps to understand and potentially fix the problems. The steps should also help you or a first responder to recognize when to request help from a specialist.

The Digital First Aid Kit gives you tools that can help you make a first assessment of what is happening and determine if you can mitigate the problem on your own. If at any moment you feel uncomfortable or unsure about implementing any of the solutions outlined here, ask for help from trained professionals, say its developers.

The self-diagnostic quality of the Kit should also enable journalists, bloggers, activists and human rights defenders to understand what is happening to their digital assets, to be able to determine more rapidly when they should reach out for help, what kind of help they need, and improve individual digital safety.

More: https://www.digitaldefenders.org/digitalfirstaid/

DISCUSSION POINTS

Here are a few questions and discussion points for further exploring this topic.

- Digital security and cybersecurity is a shared responsibility of the user, and the provider of technology services. Do you agree? Discuss.
- Have you experienced a virus or malware problem and if so, what course of action did you or your organization take to resolve it?
- Have you activated encryption for any of your digital services? If so, describe your experience.
- In the event of a data or privacy breach, what can be done? Do you or your organization have a contingency plan?
- Do you know of any instance of digital identity theft? How did it happen and what recovery was possible?
- Do you use public Wi-Fi when away from your home and office? If so, what precautions do you take?

LEARNING OUTCOMES

By the end of this module, you will have an understanding of the following:

- Cybersecurity is about systems and things; cyber safety is about people.
- Digital security and cybersecurity is a shared responsibility of the user, and the provider of technology services. Good digital security and cybersecurity requires user involvement, responsibility and vigilance.
- Strong passwords, two-step authentication, data encryption and regular data backups are among the precautionary measures that every user of digital services and the web should take. They are part of essential digital responsibility, also called good digital hygiene.
- There is plenty of free and helpful advice online about enhancing digital security and cybersecurity. However, the most important element in this process is you – the user!

FURTHER READING

Good Digital Hygiene: A guide to staying secure in cyberspace
Book by Ed Gelbstein (2013)
http://index-of.co.uk/IT-managment/good-digital-hygiene.pdf

Norton internet security advice
https://us.norton.com/internetsecurity

Google help centre (only for those with a Google account)
https://support.google.com/

Security in-a-Box, a guide to digital security for activists and human rights defenders
https://www.frontlinedefenders.org/en/digital-security-resources

Umbrella is digital and physical security for people at risk on your Android phone
https://secfirst.org/

Information security handbook for journalists
http://www.tcij.org/resources/handbooks/infosec

Electronic Frontier Foundation's Surveillance Self Defence
https://ssd.eff.org/en

Tips on good digital hygiene
https://wiobyrne.com/digital-hygiene/

Digital security for activists, by the Electronic Intifada
https://electronicintifada.net/content/guide-online-security-activists/17536