CyberSAFE in Schools

Safer Internet For All

DiGi

Partners:

CyberSecurity MALAYSIA

An agency under MOSTI

Content

2 Securing Your Digital Device

6 Protecting Your Connectivity

10 Mobile Device Etiquette

Introduction

Today, mobile devices (which include mobile phones and tablets) are being used to stay in touch, take and share photos, surf the internet, capture videos, listen to music, and socialise online, amongst others. That's like having a mini-computer in your pocket or in the palm of your hand.

The rapid evolution of mobile internet, and the ability to access the internet from anywhere at any time has also allowed you to easily store your personal and professional information on these devices. However, if you lose your mobile device, you risk more than just losing your contact lists. You will also lose all other sensitive and personal information stored on it, exposing yourself to greater risk.

We have designed this guide to arm you with information that will help you stay safe online, secure your mobile device and guide you to advocate responsible usage of the internet to your friends and family.

Securing Your Digital Device

You should treat your devices with the same care as any other valuable items, by securing its contents and making sure it is secured.

DID YOU KNOW

People are 15 times more likely to lose a mobile phone than a laptop, making loss the biggest threat to mobile users *(www.Mcafee.com)*

Securing Your Digital Device

Physically Keeping Your Mobile Device Secure

- Configure your device to auto-lock after a certain period of time. Even if it's locked, never leave it unattended as it may easily be misplaced or stolen.
- Exercise caution when using your mobile device in public. If possible, avoid using your mobile device when walking, moving around or in crowded places.
- In the unfortunate event you lose your device, report it immediately to your mobile operator. Remember that you are responsible for the cost of any calls, texts and data usage until your mobile service is blocked.

Leveraging On Original Security Features

1. Most mobile devices have a default built-in security system. By hacking or tampering with your device, you could weaken its security.

2. Only install applications from trustworthy sources. Before downloading, research the application and its publishers, and read user review and ratings. Always keep your applications up-to-date.

3. Read the privacy policy before installing any application on your mobile device. Consider how much personal information and phone access the application requires, and if it will share your information with anyone else. If you are uncomfortable, don't download the application.

DID YOU KNOW

Having a password for the apps in your device is very important.
Some password tips:

- Use complex passwords with a combination of lower and upper case letters, numbers and symbols
- Length of your password should be at least 8 characters and up to 14 characters
- Ensure your password is not your user name, real name, company name, birth date or mobile number

Safeguarding Your iOS And Android Devices

iOS DEVICES

To do list

- **Activate your password or passcode**
  Setting a password or passcode for your iOS device is a great first step in keeping your iOS device secure.
  First, go to Settings, tap General and then tap *Passcode Lock* to setup your *Password* or *Passcode*.

- **Activate *Find My iPhone***
  Whether lost or stolen, increase the chance of getting your mobile devices back by downloading the *Find My iPhone* or *Find my iPad* applications.

- **Set your *Restrictions***
  When you *Enable Restrictions*, you will set a passcode lock that will prevent changes to particular services. For example, a thief could steal your device, and turn off *Find My iPhone* while your passcode lock is off. *Device Restriction* prevents this.
  Go to *Settings*, tap *General*, and then tap Restrictions to choose which services you would like to restrict.

ANDROID DEVICES

19:35

- **Create an Unlock Pattern, PIN, or Password ***
  To secure your phone from people accessing it without your permission, go to *Settings,* tap Security, then tap Screen Lock and choose *Unlock Pattern*, *PIN*, or *Password*.

- **Invest in an effective mobile security application**
  Consider installing an effective mobile security application that provides you with security and protects you against existing and emerging threats. *Lookout* and *Avast!* are good options to consider.

- **Setup different user profiles (device specific)**
  If you often share your device, you are advised to set different user-settings for each user. This will prevent others from fully accessing your personal files. Go to *Settings*, tap *Users* and then tap *Add User*.

** Steps may vary based on Android version and devices manufacturer*

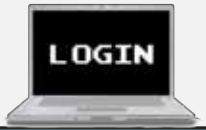
Protecting Your Connectivity

When using your mobile device to send and receive data or surfing the internet, it is important to use a secured connection. Remember that just like in the real world you will face security risks in the digital world. An unsecured connection may expose you to online dangers.

REMEMBER

Always turn off wireless interfaces (Wi-Fi, location services and Bluetooth) when not in use and disable automatic connection function on your device

Protecting Your Connectivity



REMEMBER

Always log out of sites instead of closing just the browser because people who get a hold of your devices can potentially log into all your accounts. Also, never save usernames and passwords in your devices

Types of Connectivity

In today's world of mobile technology, these are the common connectivity options on most devices in the market:

Device to Device

- NFC (Near Field Communication) is a short range wireless technology that connects applications when in very close proximity (eg. Android devices).
- Bluetooth is a wireless technology that enables short range connection or sharing between Bluetooth-compatible devices (eg. laptop, phones, digital cameras, etc.).

Data network

- This refers to the mobile data service you use on your mobile device.

Public WiFi

- Also known as Wi-Fi hotspots, this refers to free or paid wireless access at public locations provided by the owner of the premises to visitors.

Precautions for Public WiFi

- **Nothing is private on public WiFi**
  If you surf on an unsecured connection (eg. Free WiFi at a fastfood restaurant), you are vulnerable to cybercriminals viewing or stealing your information.

- **Do not send or receive sensitive data on public WiFi**
  It always safer to perform sensitive transactions (eg. online banking) on secured networks. Consider using data service by your mobile operator as most mobile networks encrypt data between cell towers and your mobile device.

Protecting Your Connectivity

Precautions for Bluetooth and Geolocation

- **Make it a habit to turn off your Bluetooth or location services when not in use**
  Strangers can connect to your device and send you unwanted messages or locate your whereabouts. Don't reveal your real name on your Bluetooth/wireless identity.

- **Think twice before you post**
  Geolocation allows people to locate you using your mobile device's GPS. For safety, only share your location with people you trust.

- When posting photos, think twice before you geotag the photo. You might not want everyone to know which school you go to.

Mobile Device Etiquette

Mobile device etiquette is not just about knowing how to protect yourself on your mobile device effectively. It is also about using it responsibly. Being a responsible mobile user means you behave in a socially acceptable manner online.

DID YOU KNOW

Most people "overshare" and divulge too much information about themselves online ***(www.intel.com)***

Mobile Device Etiquette

Be information sensitive

For yourself – Never give out personal details that could be used to identify yourself, such as your name, address, telephone number, school, location, parent information, photographs, passwords, My Kad details without permission from your parents.

For others – Just as you keep your own information secure, do the same for others.

Be aware of Cyberbullies

For yourself – If you are bullied online, never be afraid to ask for help from an older sibling, parent or teacher.

For others – Never say online what you will not say to someone face-to-face. Think twice before you post anything online. If you have a friend who is being bullied online, help them seek advice.

BE PHOTO SENSITIVE

108 likes

view all comments

For yourself – A picture can tell a thousand words. When you post your photos online, make sure they do not contain or reveal your personal information. Remember that what you show and what people see can be perceived differently.

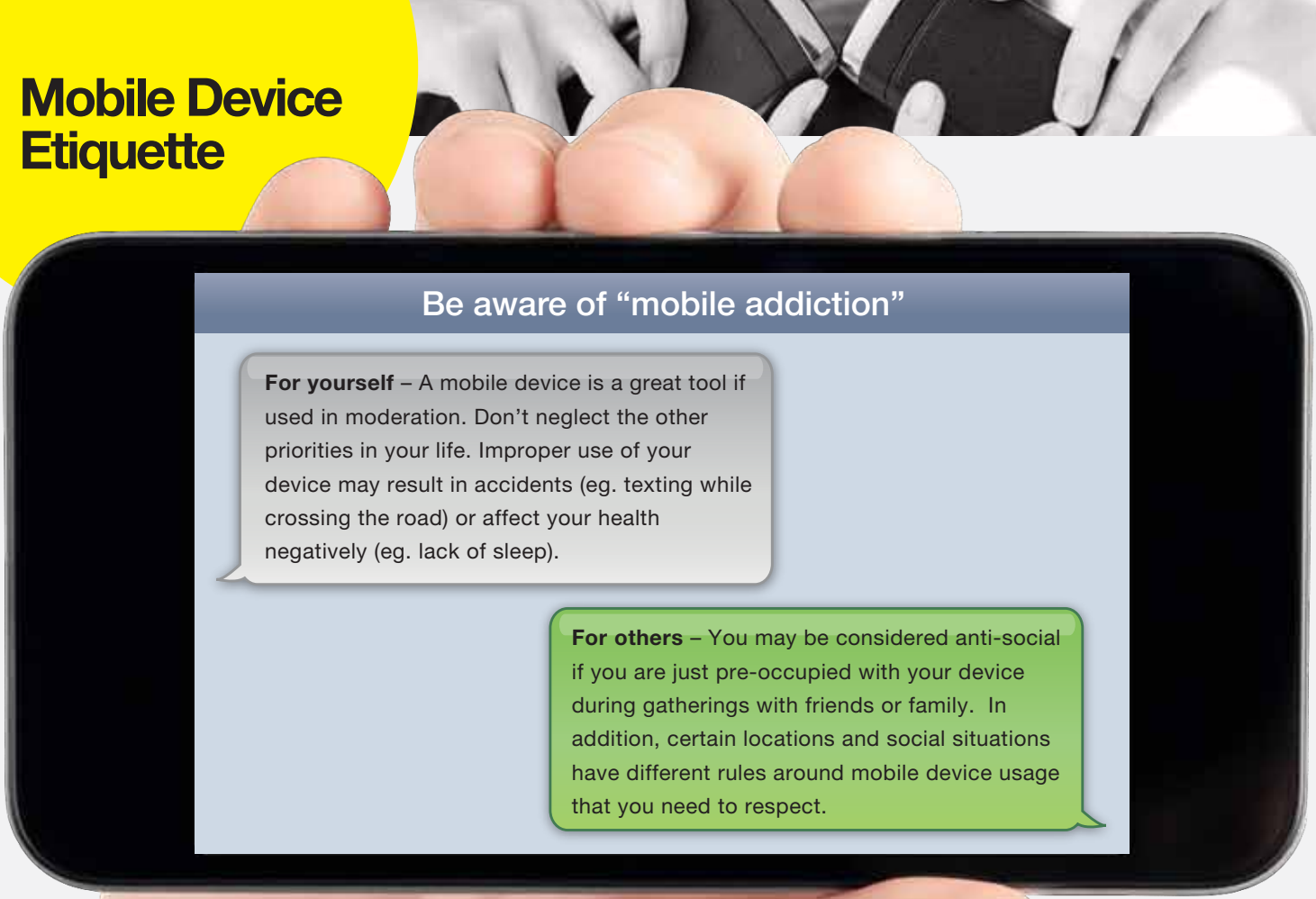
For others – Always ask permission before you take a photo of someone with your camera phone or upload such photos to the internet, particularly if your photo involves children.

Like Comment • • •

REMEMBER

If you can't say or share anything nice, don't say or share anything at all. Cyberbullying is a crime. Cyberbullying (includes harassing text messages and unwanted posts on other people's Facebook pages) is a crime

Mobile Device Etiquette



Be aware of “mobile addiction”

For yourself – A mobile device is a great tool if used in moderation. Don’t neglect the other priorities in your life. Improper use of your device may result in accidents (eg. texting while crossing the road) or affect your health negatively (eg. lack of sleep).

For others – You may be considered anti-social if you are just pre-occupied with your device during gatherings with friends or family. In addition, certain locations and social situations have different rules around mobile device usage that you need to respect.

For more information

www.digi.com.my/digicybersafe

An awareness programme under CyberSecurity Malaysia, the National cyber security specialist centre with the aim of spreading the awareness of safe internet usage. For more information, do visit **www.cybersafe.my**

CyberSecurity MALAYSIA

CyberSAFE
Cyber Security Awareness For Everyone

A cyber security incidents reporting centre. To report incidents, email **cyber999@cybersecurity.my** or call **1-300-88-2999 / 60192665850**

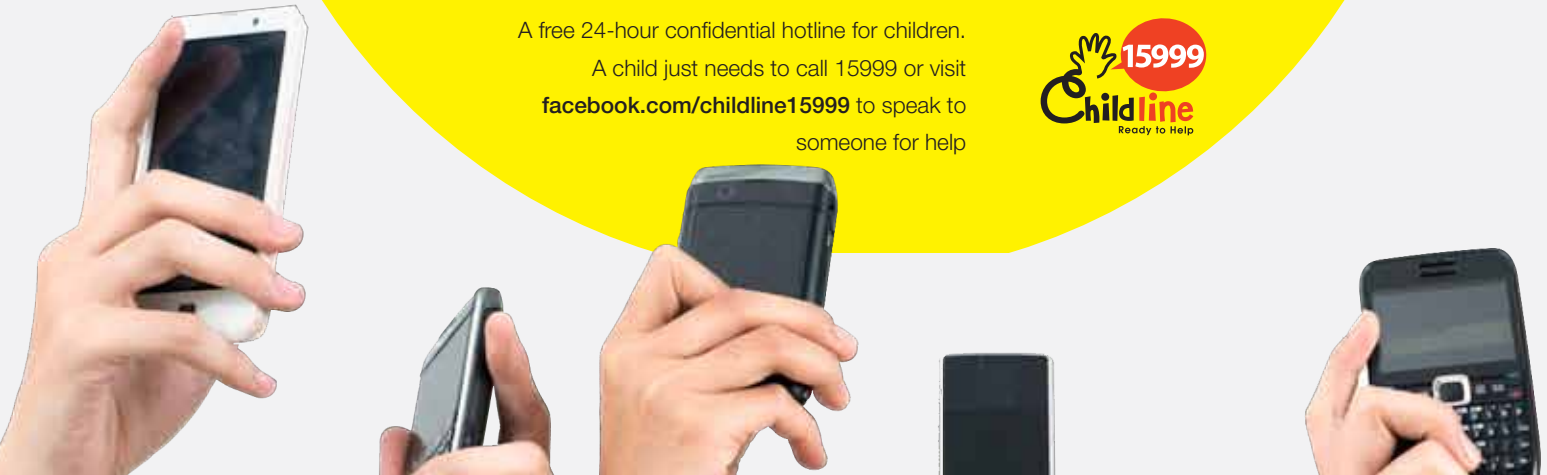
Cyber999

A free 24 hour hotline for early intervention for victims of child abuse, domestic violence and natural disasters.

TALIAN NUR 15999

A free 24-hour confidential hotline for children. A child just needs to call 15999 or visit **facebook.com/childline15999** to speak to someone for help

15999 Childline
Ready to Help



CyberSAFE in Schools

A Guide to Mobile Internet Safety

Safer Internet For All

klik dengan bijak

DiGi

Endorsed by:

Ministry of Women, Family and Community Development

SKMM MCMC

15999 Childline Ready to Help