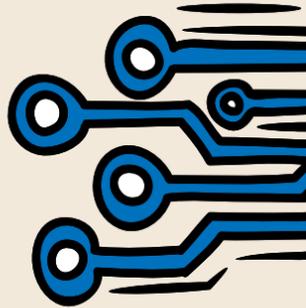# GUIDEBOOK CYBER HYGIENE

## AiSP Cyber Wellness

**1** All About Cyber

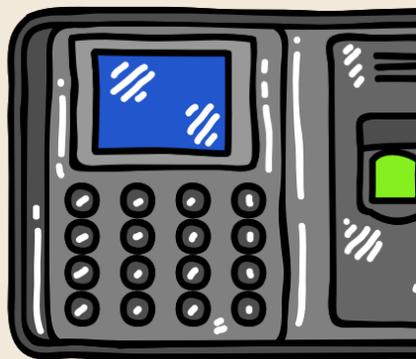**2** Social Media

**3** Cybersecurity Awareness

**4** Scam Awareness

**5** Password

**6** Online Browsing

**7** External Threats

**8** Security

**9** Personal Data

**10** Everyday AI Tips

# ALL ABOUT
# CYBER

**95%**

Cybersecurity breaches are caused by human error

**300 BILLION**

passphrases are used by humans and machines worldswide

"Even the best software will fail if there is human error"

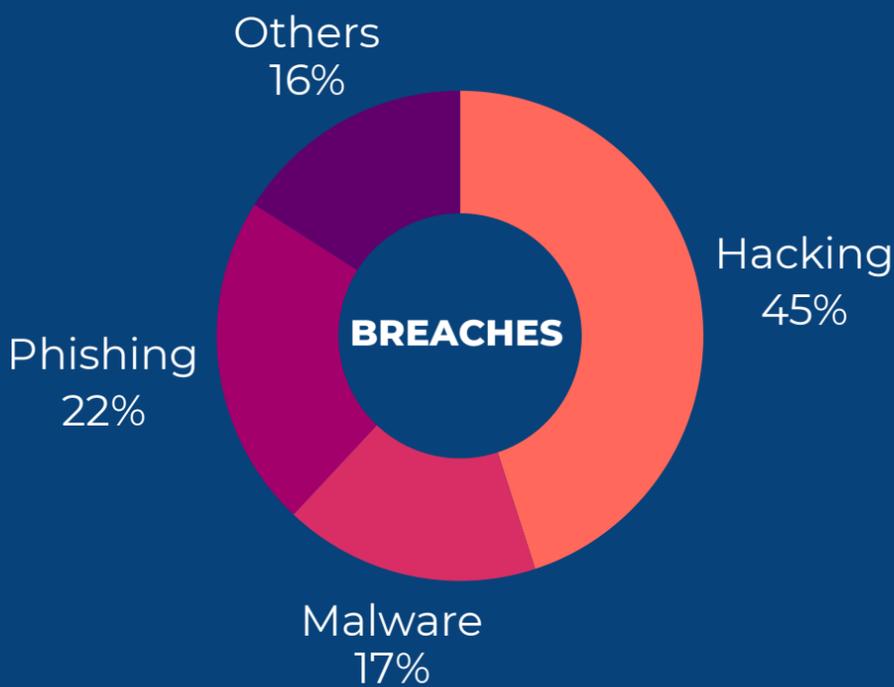Do not put 100% trust in your software and expect to be invulnerable

# TOP MALICIOUS EMAIL ATTACHMENT

**37%**
.doc and .dot

**19%**
.exe

Others
16%

Hacking
45%

**BREACHES**

Phishing
22%

Malware
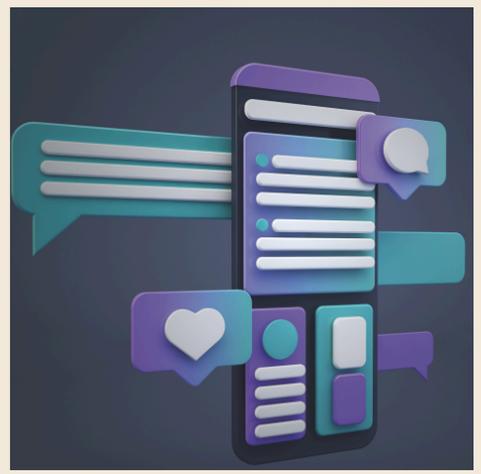17%

# SOCIAL MEDIA

## *Information*
you post can be used to steal your identity or hack into your online accounts

## Check the
privacy settings of your social media accounts and set them so that only people you know can view them

Before posting someone else's information online,

## *Seek approval*

APPROVE

## Do not participate
in facilitating harassment or violence towards someone through your social media posts

## Always consider
the consequences when sharing things online

# CYBERSECURITY AWARENESS

**1** START FROM YOUNG

Cybersecurity awareness starts from a young age. It is advisable to impart this knowledge to our youths.

BEST DEFENSE IS AWARENESS **2**

The best defense to cybersecurity is is be aware. Seek to understand and leverage the various protection features of your security solutions/technologies.
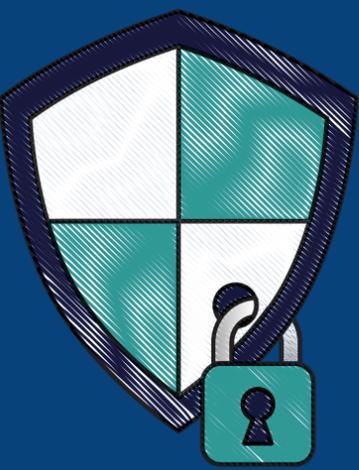
**3** SECURE ENOUGH

Unless your device is offline and physically inaccessible by the rest of the world, there is no such thing as "secure enough".

IT WILL NOT HAPPEN TO ME **4**

Everyone is a potential target for hackers, including you. Do not have a "it will not happen to me" mindset.

**5** INTERNET OF THREATS

Internet of Things (IoT) without security is equivalent to Internet of Threats.

GO SAFE ONLINE **6**

Check out Cyber Security Agency of Singapore's "Go Safe Online" campaign to learn more about protecting yourself on the internet.
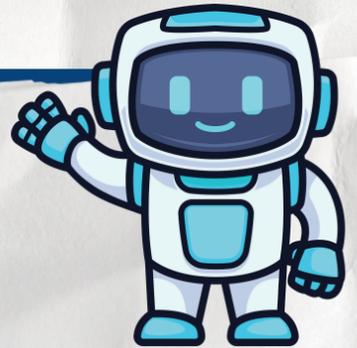
# SCAM

## AWARENESS

## Protect Accounts & Devices

- Strong & unique passwords
- Enable 2FA
- Update apps & devices regularly
- Avoid public Wi-Fi for sensitive accounts

## AI &Cybersecurity

- AI detects threats early but may raise false alarms
- Hackers may use AI for smarter attacks, stay alert!

## Spot Scams Fast

- Urgent emails, calls, or messages asking for info
- "Too good to be true" deals or investments
- Suspicious links or bad grammar

## Take Action!

**STOP** Don't click or share information

✓ Confirm with official sources

☎ ScamShield, SPF Anti-Scam Helpline (1800-722-6688), scamalert.sg

An example of a
# STRONG PASSWORD
is a long catchphrase

# ADD VARIETY
Use uppercase, lowercase, characters, and numbers.

# DON'T RECYCLE
Don't use the same password for all of your accounts.

# DON'T USE PERSONAL INFORMATION
Avoid using birthdates or names from your loved ones.

# BREACHED?
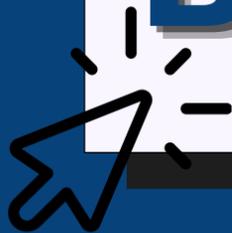Change your password immediately and inform the platform

# CHANGE OFTEN
Passwords are like undergarments, change it frequently and don't share it with others

# USE A MANAGER
Password management apps and sites can help keep track.

# ONLINE BROWSING

Avoid visiting unknown websites or downloading software from untrusted sources
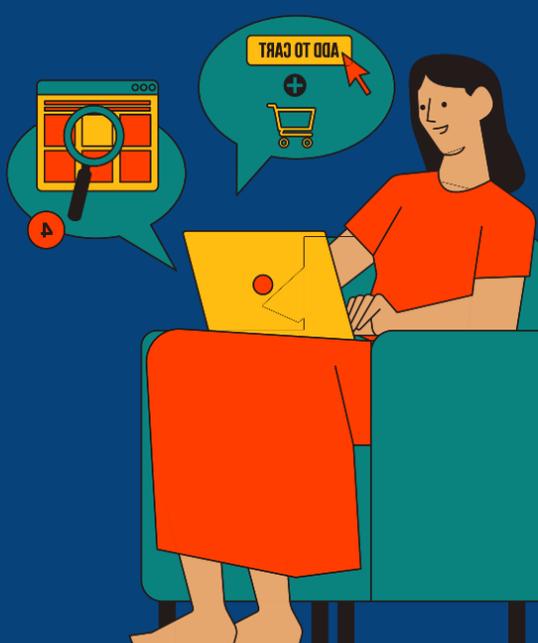
Sensitive broswing, such as banking or shopping, should be only done on your own device

When you connect to a public network, you are vulnerable to risks such as man-in-the middle attacks and data theft

Avoid using public networks or use a VPN when you're connected to one

VPN

# EXTERNAL THREATS

Always update to the latest version of your software to protect yourself from new or existing security vulnerabilities

Scan for viruses regularly, for example, once per week

Always scan external devices for malware before accessing them

Do not click on links given in an email. Manually type in the hyperlink yourself to prevent being redirected

Adware collects information about you to server you more targeted ads. Use anti-adware to clean adware and other unwanted programs from your computer

# SECURITY

Implement application control integrated with antivirus to allow only authorised software to work

Restrict administrator privileges so as not to give attackers privileged rights to compromise systems

Follow documented practices for securing your devices and systems

Enable security features on your devices to prevent unauthorised access

Lock your device every time you leave your desk

Always enable multi-factor authentication (MFA) to keep your accounts more secure

Visit haveibeenpwned.com to find out if any of your accounts have been compromised

Physical security is as important as cybersecurity. Never leave your devices unattended

# PERSONAL DATA

## NAME: YOU
## JOB: CYBER SAFE CITIZEN

## SKILLS:

✅ Always use encryption when storing or transmitting sensitive data

✅ Regularly backup data to cloud or on a local storage device

✅ Destroy/shred hard copy confidential documents that contain information

## JOB EXPERIENCE:

When unsure of why I am asked for personal information, I will call the organisation to check if it is authentic

Stay suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information

# Everyday AI Tips

## Help you write Messages

Gen AI can help you:
- Write WhatsApp messages
- Reply to emails
- Say things politely and clearly

Example:

"Help me write a birthday message for my grandson."

## 🚌 Need to Go Somewhere? Just Ask!

You can ask:
- "How do I go from my home to the hospital?"
- "Which bus should I take?"

Gen AI can:

✓ Explain directions step by step

✓ Help you understand transport options

✓ Make travelling less stressful

## Elderly - Friendly Gen AI Apps

Google Gemini and Chatgpt

Helps answer questions and explain things clearly

Useful daily examples:
- "Explain this news simply."
- "How do I use this app?"
- "What does this letter mean?"

Gemini

ChatGPT

# AiSP

## Our Story

We are an independent cybersecurity association that believes in developing, suporting as well as enhacing industry technical competence and management expertise to promote the integrity, status and interests of Information Security professionals in Singapore

We believe that in promoting the devlopment, increasing and spreading of cybersecurity knowledge, and any related subject, we help shape more resilient economies

We facilitate
THINK TANKS

We build Cyber
SKILLS

We have amazing
PARTNERSHIPS

Organise regular
NETWORKING EVENTS

# AiSP | CYBER WELLNESS

The AiSP Cyber Wellness Programme aims to educate citizens, especially reaching out to the youths and elderly on the importance of Cybersecurity and learn how to stay safe online. There has been an increase in cyber threats, online scams and COVID-19 related phishing activities. With reduced Face-to-Face engagements, the elderly and those with special needs have become more vulnerable to cyber threats. We will reach out to different community groups to raise awareness on the topic of cyber wellness and cybersecurity and participants can pick up cyber knowledge through interactive learning. It is supported by the Digital for Life Fund, an initiative by the Infocomm Media Development Authority (IMDA), that supports digital inclusion projects and activities to help all Singaporeans embrace digital, to enrich lives."

## VISIT OUR WEBSITE BY SCANNING

## LOOK OUT FOR OUR UPCOMING EVENTS

# About Digital for Life movement

The Digital for Life (DfL) national movement, launched by President Halimah Yacob on 8 February 2021, aims to galvanise the community to help Singaporeans embrace digital as a lifelong pursuit, and to enrich their lives through digital. At the same time, President Halimah also launched the flagship DfL Fund to support projects and activities promoting digital inclusion, digital literacy and digital wellness.
Learn more about the DfL movement at www.imda.gov.sg/digitalforlife

If you would like to sponsor AiSP Seminar, events or see how you can be part of the Cyberwellness Programme, please feel free to contact secretariat@aisp.sg.