Digital Media and Information Literacy Framework

DIGITAL DEFENCE

SG:D | GET READY!

Ministry of Communications and Information

Contents

DIGITAL MEDIA AND INFORMATION LITERACY FRAMEWORK

Introduction

Singapore's Digital Readiness vision is for every Singaporean to be ready to seize the opportunities and benefits of technology in everyday living in a Smart Nation. To be digitally ready, each individual should be equipped with a fundamental set of skills and attitudes to thrive in this digital age: to have access to digital technology, the literacy and know-how to use the technology, and the ability to participate meaningfully and create with this technology.

To this end, the Ministry of Communications and Information (MCI) launched the Digital Readiness Blueprint in June 2018, outlining 10 recommendations on how to help Singaporeans embrace technology. These recommendations fall under four strategic thrusts of Digital Access, Digital Literacy, Digital Participation and Digital Inclusion by Design.

One of the key outcomes of being digitally ready is being digitally literate – defined as having the knowledge, understanding and attitudes to use technology safely, meaningfully and responsibly. Today, there are many existing information and media literacy public education programmes, including the Media Literacy Council's Better Internet Campaign, the National Library Board's S.U.R.E. programme, and the Cyber Security Agency of Singapore's National Cybersecurity Awareness Campaign. Many training providers in the people and private sectors also conduct such similar programmes for individuals and organisations.

Against this backdrop, this Digital Media and Information Literacy Framework aims to provide an overarching frame to guide existing public education efforts, with a view to empower Singaporeans to be discerning consumers of information with adequate understanding and appreciation of the possibilities, problems and prospects afforded by technology.

Overview of the Framework

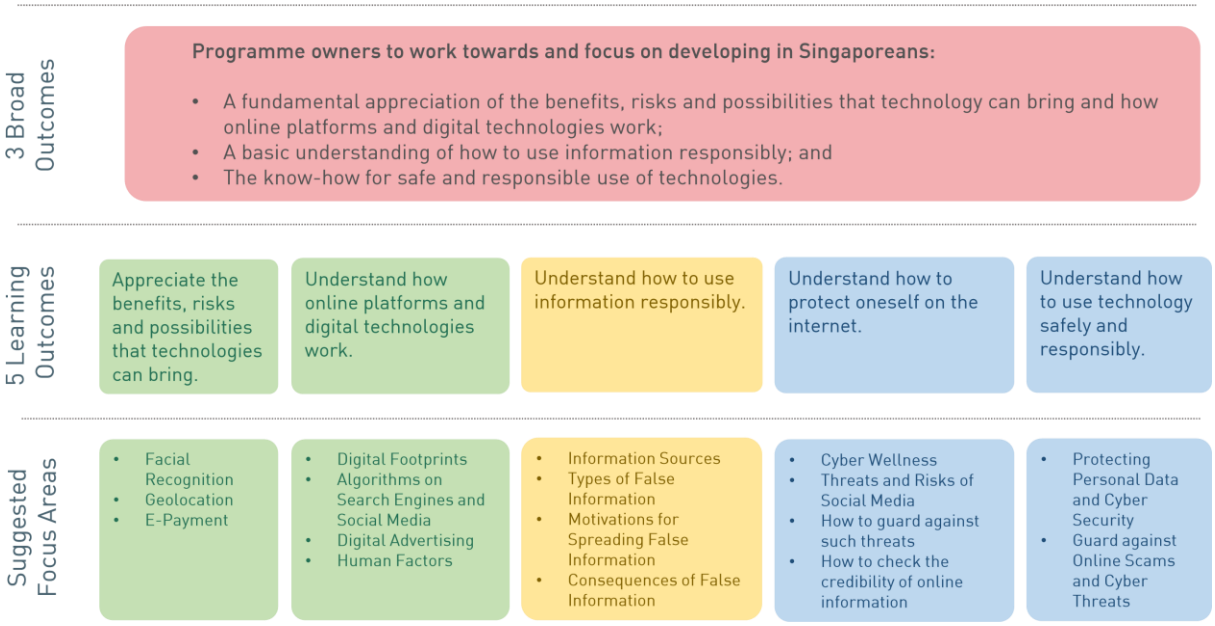
The Digital Media and Information Literacy Framework establishes a set of common outcomes for programme owners to work towards, and focuses on developing in Singaporeans:

a. A fundamental appreciation of the benefits, risks and possibilities that technology can bring and how online platforms and digital technologies work;
b. A basic understanding of how to use information responsibly; and
c. The know-how for safe and responsible use of digital technologies.

The Framework sets out 5 key learning outcomes (LOs):

LO1 Appreciate the benefits, risks and possibilities that technology can bring
LO2 Understand how online platforms and digital technologies work
LO3 Understand how to use information responsibly
LO4 Understand how to protect oneself on the Internet
LO5 Understand how to use digital technologies safely and responsibly

Digital Media and Information Literacy Framework



How to use this Framework

The Learning Outcomes (LOs) provide a common frame for programme owners in their design of digital media literacy and information literacy programmes. To facilitate implementation, LOs are distilled into specific learning objectives, supported by suggested content areas. Programme owners are encouraged to refer to the broad outcomes in designing their programmes, and to adapt and update the content and focus areas to meet the specific needs of the learners.

*Throughout the document, * denotes content that is recommended for all participants (or learner profiles). More information can be found in the supplementary guide at the end of this document.*

Beyond This Framework

Every individual also has a part to play in practising good habits online to make the Internet a safe and conducive space for all. The desired learning outcomes of this framework are fully achieved when individuals also exhibit the following values in their online behaviours[1].

Respect

Treat people with respect despite differences to make our online interactions more meaningful and constructive.

Empathy

Seek to understand other people's perspective and the impact of words used.

Responsibility

Be accountable for words and actions online to ensure that communication does not result in harm to self and to others.

Integrity

Stand up for what is right online to make courtesy the new norm and keep the trolls at bay.

Discernment

Exercise critical thinking and good judgement when interacting online, be smart digital citizens and make informed choices and actions.

[1] This emphasis on being discerning and responsible producers and consumers of online content is also in line with the "Core Values on Digital Literacy for ASEAN", which was adopted at the 14th Meeting of ASEAN Ministers Responsible for Information (AMRI) in May 2018. The Core Values referenced the media literacy values promoted by Singapore's Media Literacy Council to address risky behaviours, uncivil behaviours, and inaccurate or extremist information online.

Learning Outcomes

Learning Outcome 1: Appreciate The Benefits, Risks And Possibilities That Technology Can Bring

The advent of new technologies has transformed many aspects of relationships, business and society. While rapid advances in technology can be daunting and exciting, choosing to embrace and use technology can greatly improve an individual's quality of life. This entails nurturing a greater appreciation of technology, specifically, how it works, and how fast it can evolve. A digitally literate individual, therefore, is one who is aware of the possibilities – both the risks and benefits of technology – and makes an effort to stay in touch with technological changes.

Learning Objectives

Individuals will learn:

- Why it is important to keep up with rapidly advancing technology*
- How technology can bring both benefits and risks*

**Content recommended for all participants.*

Broad Takeaways

- Technology is always advancing; keeping up to date with the changes ensures one is better placed to benefit from it.
- Technology helps make lives better but it can also be abused if it falls into the wrong hands.

Suggested Focus Area #1 – Technological Advancements and its Impact on Our Lives

Learning Objectives:

- ✓ **Why it is important to keep up with rapidly advancing technology***
- ○ How technology can bring both benefits and risks*

Technology has had a significant impact on our lives. It has enabled new tools that has changed the way that we live, work, and play.

One particular milestone in modern technology was the development of the 3G technology in the 1980s; in less than two decades it became widely adopted, and paved the way for the age of the smartphone. Smartphones today allow us to do most of the following things on the go:

- Browse the Internet to search for information, through news websites, research journals, e-books, and online encyclopaedias
- Communicate with others instantly, through emails, instant messaging, social media platforms
- Carry out transactions online, through Internet banking applications, mobile payments and even new forms of online currency

Even as some of these functions have become a part of our daily lives, there are still many new forms of technology that are emerging and getting increasingly complex. The following are some examples of emerging technologies that have disrupted some of our industries:

- **The Internet of Things (IoT)** refers to a network of mobile devices that are connected via the Internet, ranging from mobile phones and wearables (e.g. smart watches) to cars and household appliances like (e.g. microwave, television). IoT has become significant because it enables connectivity of public infrastructure—buildings, transport, municipal services—at a larger scale and introduces the possibility of "smart cities" that allow citizens to enjoy more efficient and effective public services.

- **Artificial Intelligence (AI)** refers to the ability of machines to learn from and simulate human intelligence, including aspects of speech, reasoning and problem solving. Machines do this by gathering and aggregating significant amounts of information about the world, including patterns of our behaviour and preferences. This has made a significant impact on various industries, by introducing "human-like" aspects to entertainment and e-commerce (e.g. predictive algorithms on Netflix or Amazon that recommend similar shows or relevant products), transport (e.g. self-driving vehicles) and services (e.g. chat bots for customer service in banks).

Technology is a powerful tool that brings great benefits, but it can also be abused. Keeping up to date with technology is necessary in order to stay informed of both the value add (and pitfalls) of technology adoption.

Suggested Focus Area #2 – Benefits and Risks of Technology

Learning Objectives:

- Why it is important to keep up with rapidly advancing technology*
- ✓ **How technology can bring both benefits and risks***

Technological advancements have collectively afforded us many benefits. For instance, mobile technologies have made it convenient for us to find information, cheaper and more efficient for us to communicate with others in real-time, and even more secure for us to carry out transactions that involve confidential information.

At the same time, there are also risks to using technology.

The following three examples illustrate that there are always benefits and risks of any type of technology, including those that we may be more familiar with:

Illustration 1: Facial Recognition

Facial recognition uses technology to recognise human faces. The system works by using biometrics to map facial features from a photograph or video, and then compares the information against a database of known faces to find a match. Facial recognition technology is widely used by organisations and individuals, for purposes from security and law enforcement, to retail marketing and even attendance marking.

One example is the facial recognition technology currently being used at automated bag-drop machines at airport terminals. When passengers drop off their luggage at these booths, photographs of their faces are taken and matched against their passport photographs to verify identity. This automated process helps to facilitate more efficient services, which translates to shorter queues for passengers.

While it has its benefits, from improved security to better customer service, facial recognition also raises privacy concerns.

Benefits of Facial Recognition Technology	Potential Risks of Facial Recognition Technology
• **Faster or more convenient:** Facial recognition has been used to unlock phones and doors, and facilitate airport security clearance. • **Improves sales for businesses:** Retailers use facial recognition in various aspects, from tracking customer behaviours and preferences for targeted marketing, to improving checkout process and preventing theft in stores.	• **Identity theft: T**he widespread use of facial recognition means facial data is readily collected and accessible by anyone, including hackers and malicious actors who can use it to achieve their own objectives. • **Safety**: Facial recognition software can be used to identify someone who can then become a target for online harassment and stalking.

Illustration 2: Geolocation

Geolocation services make use of a user's IP location, comprising information on the country, city, postal code and time zone, to determine the real-time location of a particular device. The most common use of geolocation is in Global Positioning System (GPS) technology, which allows users to calculate their exact location, or to locate their specific destinations.

One application of geolocation is Waze, a software app that provides drivers with navigation information that helps drivers get to their desired destinations. The app makes use of GPS technology to provide drivers with information such as live updates on traffic conditions, suggested driving routes, as well as the estimated time it would take for them to get to their destinations.

This technology has not only allowed for the widespread use of online maps and for users to share their real-time location with one another, but has also facilitated the development of autonomous vehicles that are able to navigate roads and traffic with geolocation information.

Benefits of Geolocation Technology	Potential Risks of Geolocation Technology
• **Ability to navigate**: Geolocation has made it much easier for any user with mobile data to navigate in unfamiliar regions. • **Ability to plan ahead:** Information about real-time traffic conditions has enabled users to make more informed choices about their journeys.	• **Overexposure of personal information**: Information from geolocation tags, when used in combination with other personal information, may be used to identify a person's real-time location and be used or shared without their permission. • **Targeted advertising:** When users keep their geolocation services active, businesses may be able to push targeted advertisements to users who are nearby.

Illustration 3: E-payments

E-payment is a national imperative with the potential to create new business models for companies in the digital economy. Singapore has been working on an open and accessible e-payment infrastructure to allow citizens to carry out online transactions in a seamless and secure manner.

In 2014, FAST was launched by the banking industry to enable direct real time transfers between consumers and businesses across different banks. PayNow was first launched in 2017 to enable peer to peer transfers between customers of participating banks using mobile or personal identification number. PayNow Corporate soon followed to cater to businesses and government agencies. E-payment further extended its reach in the same year, when NETS was appointed to develop an interoperable and open access e-payment solution across a network of coffee shops, hawker centres and industrial canteens. In a bid to simplify QR e-payments for both merchants and consumers, the Singapore Quick Response Code (SGQR) standard, which combines multiple payment QR codes into a single SGQR code, was launched in 2018.

The private sector has also launched a few different mobile wallets that enable users to pay for products (e.g. food, clothing) or services (e.g. transport fares, bills) using an app in their mobile phones. Such apps work by prompting users to link their credit cards or bank accounts to the application, so that their purchases can be charged directly to the linked cards or accounts. Some examples include DBS Bank's PayLah!, GrabPay and FavePay.

Overall, e-payment spells convenience for users as transactions can be carried out on most smartphones and completed almost instantaneously. It can also be said to be more secure than conventional means of payments (e.g. cash, cheque), because of the additional verifications required when using online banking.

As with any technology, there are also aspects of e-payment over which to exercise caution. QR-code phishing is one such example. This happens when QR codes are encoded with malicious URLs directing online users to fake websites, which then prompt them for personal information.

Suggested Discussion Points

- How has technology made your life easier?
  [Possible prompts: In the areas of transport, work, communications, etc]

- Can you think of any other technologies that have afforded benefits, but also bring about certain risks to users? What are some of these benefits and risks?
  [Possible prompts: Social media, cloud storage, etc]

Advanced Discussion Points:

- What are some applications of IoT or AI that you have observed in your daily lives?
  [Possible prompts: Applications of IoT include smart lamp posts, smart home appliances; Applications of AI include self-driving cars, transcribing tools, chat bots]

- What are some ethical issues that arise in the applications of IoT? What about in AI and machine learning*?*
  [Possible prompts: Ethical issues in IoT include the potential for more "surveillance"; ethical issues in AI include the potential for racist robots and AI bias, as well as the potential for AI-powered machines not having the ability to carry out moral reasoning]

- If AI technologies allow for machines to have decision-making capabilities that can formulate responses with unsupervised data gathering, what impact could this have on our society?
  [Possible prompts: How has AI changed the future of work and jobs in today's society?]

Learning Outcome 2: Understand How Online Platforms and Digital Technologies Work

Social media platforms, such as Facebook and Instagram, have become one of the most popular means for people to stay connected with one another. Users post pictures, leave comments, and get their news and information from social media and search engines. Online actions like these leave behind a trail, or what is known as a digital footprint, and AI-powered algorithms track these footprints to share them with marketers. Using this data, marketers then target relevant content and advertisements at potential customers. As a tool used by social media companies and marketers, algorithms function to feed or push to users content that they have engaged with in the past, thus reinforcing their existing views and interests. We need to understand how social media works in order to use it in a safe and responsible manner.

Learning Objectives

individuals will learn:

- How digital footprints work and how to manage them*
- How algorithms work on the Internet
- How digital advertising works
- How human factors can influence thinking and behaviour online

**Content recommended for all participants.*

Broad Takeaways

- There are various mechanisms at work on search engines and social media platforms that determine what content we come across or receive.
- There are human factors at play on social media that affect how we think or respond towards others.
- Therefore, it is important for one to actively seek out differing or alternative views, and accept that there is a whole spectrum of viewpoints on any given subject.

Suggested Focus Area #1 - Digital Footprints

Learning Objectives:

- ✓ **How digital footprints work and how to manage them***
- How algorithms work on the Internet
- How digital advertising works
- How human factors can influence thinking and behaviour online

Digital footprints refer to the trail of data about a user that constitutes their online identity. This accessible information is collected by AI-powered algorithms that share the information with marketers and in the process, allow companies to tailor content to users' likes and dislikes. Everyone has a distinct digital footprint that is traceable to the individual. Personal data – such as credit card numbers and personal details – can potentially be extracted through a digital footprint and be used in identity theft and even blackmail. Thus, there is a need to be more mindful of digital footprints and to safeguard against potential abuses.

This section will cover digital footprints and how a user can better manage his/her online footprints.

Types of Digital Footprints

Digital footprints can be broadly categorised into the following types:

- **Social footprint** refers to information that the user actively shares on social media platforms (e.g. Facebook, Instagram, Twitter, Pinterest, LinkedIn, Foursquare) which contributes to the user's social image and digital reputation. The information shared can be used to identify users publicly, both in a negative and positive manner.

  For example, a user's social footprint can be used by prospective educational institutions or employers who may conduct a background check on the individual before making a decision on enrolment/employment.

- **Transactional footprint** refers to information that is unintendedly left behind by the user when performing a transaction online. The interrelated and immediate nature of today's online transactions, coupled with transaction monitoring of users' online activities, means that there will always be transactional footprints that are automatically generated without the user consciously doing so. For example, purchases on online shopping sites can result in unintended installation of cookies that track user activity.

  With transactional footprints, advertisers are able to track the user's data including online activities and generate consumer profiles. While advertisers may be able to anticipate the user's interests and improve their services, users lack control over the collection and dissemination of their personal data as transactional footprints are automatically generated and accumulates over time, even when the user is not aware of it. Hence, users can play a part to manage their footprints online to better control the content pushed forth to them by marketers.

  For example, websites may collect information about the user's activities such as the number of times the user visited the website in a certain time period and the user's Internet Protocol (IP) address. Advertisers can then use the data collected to target advertisements that they deem to be relevant to the user.

Examples of Digital Footprints

The following are examples of digital footprints:

- Search history
- Browser history (even in 'Incognito' mode)
- Text messages (even after deletion)
- Photos and videos (even after deletion)
- Tagged photos (even those that users never wanted to be made public)
- Likes/loves on sites like Facebook and Instagram

How to Manage Digital Footprints

The following are some examples of how to manage one's digital footprints:

- Consider these questions before posting, forwarding, or replying to something online:
    - What would someone who doesn't know me think of me if they saw this? (e.g. a prospective employer, a client, etc.)
    - Would I want someone else to post this about me?
    - If this was on a headline for everyone (my parents, friends, teachers) to see, would I be okay with it?

- Other suggested tips include:
    - Treat others like how they would like to be treated.
    - Set settings on social media sites to 'Private', and check and update this regularly.
    - Check the content they are being tagged in, and remove those that are offensive or inappropriate.
    - If they have posted content that they regret, remove it immediately.
    - If they find that they are posting lots of things that are hurtful to themselves or others, it might be good to take a break from social media for a while.
    - Turn off geo-tagging or location settings on their phones and social media accounts.
    - Use Virtual Private Network (VPN) for more secure connections and transactions.
    - Always log out of the website after they have completed their transactions.
    - Do not use public computers or unsecured Wi-Fi when performing transactions.
    - Clear browser cache regularly.

Suggested Discussion Points

- What are some examples of digital footprints that you can think of? How can digital footprints impact your life?
  [Possible prompt: employers tracing prospective employee's digital footprints on social media platforms to check their background before deciding whether to hire them]

- Can you think of ways to create a positive footprint?
  [Possible prompts: It is important to think before you post something online. It should be something you are happy with or proud of, because it concerns your online reputation. What kind of positive content can you create? What about a video to teach others something new and useful?]

Suggested Focus Area #2 - Algorithms on Search Engines and Social Media

Learning Objectives:

- How digital footprints work and how to manage them*
- ✓ **How algorithms work on the Internet**
- How digital advertising works
- How human factors can influence thinking and behaviour online

Algorithms are typically applied in search engines to generate search results, and on social media feeds to determine what relevant content to display. Algorithms on search engines, for instance, help to filter billions of searches to prioritise some of the results and webpages that is presumed to be most relevant and useful for the user.

Algorithms try to "understand" the user by looking at factors like location, settings, as well as search history. Likewise, social media news feeds tend to be personalised according to criteria such as the frequency of interaction with posts from friends, pages and groups. With this information, platforms like Facebook are then able to make personalised recommendations to users by suggesting similar pages to follow, or pinning posts that the user is likely to be interested in on his or her news feeds.

Marketers also make use of algorithms to measure user engagement, based on reactions to different content types. For instance, marketers are able to tell how positively or negatively a user responds to a certain topic or post on Facebook, based on the different animated emotions used (e.g. Like, Love, Haha, Wow, Sad, Angry). The more positive a reaction to a post, the more likely similar posts will show up on the news feed in future.

Suggested Focus Area #3 – Digital Advertising

Learning Objectives:

- How digital footprints work and how to manage them*
- How algorithms work on the Internet
- ✓ **How digital advertising works**
- ✓ How human factors can influence thinking and behaviour online

Digital advertising is a marketing and advertising strategy that spreads marketing messages through various online channels, including email, search engines or social media feeds.

Digital advertisements are increasingly pervasive. The following are some of the more common examples of digital advertising:

- Display advertisements that are shown when users view websites, play online games or use mobile applications
- Video advertisements that are played before and during online videos
- Sponsored posts by celebrities or influencers on social media platforms
- Search engine marketing, where businesses pay for their products to be more visible in search results
- Websites created by companies to promote their brand
- Email marketing, where marketing messages are circulated using email addresses that people might have provided when signing up for services

It is sometimes difficult to tell whether content encountered online constitutes “advertising”. For instance, influencers or celebrities may not always disclose that they have been paid or sponsored by certain brands when posting about the benefits of certain products. In more extreme cases, malicious actors can exploit these advertising platforms.

This section outlines the mechanisms behind digital advertising and why they present certain risks to the user.

Types of Digital Advertising

There are typically two types of digital advertising that can be found on the Internet:

- **Pay-per-click**: Advertisers pay a fee each time their ad is clicked. It helps to drive traffic to the advertiser's website and therefore sales. When a search is initiated, the publisher or website owner displays the ad in a manner that makes it stand out to the user (e.g. first few of the search results). Depending on the search engine, some ads are also labelled with an 'Ad' icon. Google AdWords is an example of such a platform.

- **Fixed rate**: Advertiser pays a fixed price for the ad, regardless of the number of clicks. This model is often used by content-focused sites where the target audience is already there.

Figure 1: Example of what a Fixed Rate Digital Advertisement can look like

- This sample ad employs eye-catching solid colours that stand out against the white background of possible host sites, such as Facebook.
- Strong use of power words, "SALE" and "GRAB IT NOW", as well as the marketing strategy of a limited time offer, contributes to the appeal.

In both types of advertisements, users who click on the banners would be led to the business' homepage, or a content-specific landing site.

Digital Advertising Strategies

There are several strategies that digital marketers employ, which can include:

(i) **Bribes**, in which the user is promised something free if they buy the product.

> An example of a bribe is a digital ad that shows a free bottle of drink that comes with every purchase of the product.

(ii) **Games**, in which players of a game are offered prizes that require them to purchase products.

> An example of a game is where the user can spin a wheel to win prizes such as a $1 discount code for product purchase.

(iii) **Music,** in which catchy jingles or popular songs are used make the product more memorable to consumers.

> An example is McDonald's catchy "ba-da ba ba ba" hook that is widely associated with their 'I'm Lovin' It' slogan.

(iv) **Sponsorships**, in which individuals are paid to use their personal brands to market products to consumers.

> An example is when businesses sponsor celebrities or influencers to use products, with the aim of inspiring fans to purchase the same products that their idols use.

Understanding the Risks of Digital Advertising

A discerning online user is aware of the various ways in which digital advertising can be exploited for malicious purposes and be wary of the advertisements that we encounter online. This section covers two ways in which digital advertising can be exploited:

- **Malvertising:** This refers to the spreading of malware to inject systems under the guise of digital advertising. Malicious codes can be injected into legitimate online advertising networks which redirect users to malicious sites. If a user clicks on a malicious ad, they will be redirected to a malicious or compromised server, which can then make a connection to the user's device. With an established connection, the server can exploit vulnerabilities on the device's system and install a malware, which can allow it to have full access to, and potentially control of, the device.

  An example would be the incident on MSN.com in 2017, where content provider Taboola was abused by tech support scammers to carry out a malvertisement on MSN. Users were redirected to a malicious page after clicking on a story with a misleading headline that was promoted by Taboola, "After 38 Long Years The Disappearance of Etan Patz Finally Solved". In this case, the headline served as a form of clickbait advertisement, in which users interested in reading the article would be at risk of compromise to the malware host after clicking on the infected link.

- **As a tool for spreading disinformation and misinformation**. The pervasiveness of social media and low barriers of entry make it an ideal tool for spreading content quickly and efficiently. Purveyors of disinformation only require a device, such as a computer, and an Internet connection to reach a potentially huge audience.

  One example of how platforms like YouTube and Facebook were used to spread disinformation is in the anti-vaccination movement. In particular, advertisements or recommendations that vaccines were ineffective and caused autism in children (i.e. "vaccine hoaxes") have showed up more prominently in search results, causing such disinformation to be seem more believable.

Suggested Discussion Points

- What are some risks of digital advertising that online users should be aware of? *[Possible prompts: ad fraud, where bots are used to create the impression that the ads are getting seen by target viewers]*

- Do you think all social media posts on product reviews and recommendations are objective? Why do you say that? What do you look out for to determine if a review or recommendation is objective or not?
  [*Possible prompts: Are games actually marketing certain products?]*

Suggested Focus Area #4 – The Human Factor and Social Media

Learning Objectives:

- How digital footprints work and how to manage them*
- How algorithms work on the Internet
- How digital advertising works
- ✓ **How human factors can influence thinking and behaviour online**

The way algorithms are designed to push content to users can amplify their cognitive biases. The following are examples of human factors at play in the use of social media:

(i) **Homophily** refers to the tendency among people who are similar to be connected to one another, or when "birds of a feather flock together". When social media algorithms customise the content a user sees on his/her news feed, the user is more likely to bond with or seek out others who hold similar world views and preferences.

(ii) **Confirmation bias** refers to the tendency among people to look for and support information that conforms with their initial knowledge of certain issues. People tend to share search results, articles or content that they agree with friends and family, who may affirm the viewpoints expressed in these articles, and thus reinforce their initial opinions on these issues.

(iii) **Echo chambers** refer to the effect of a person's own viewpoints being fed back to the individual, causing him or her to exclude alternative views. This is especially prevalent on social media platforms, where algorithms pick up on preferences and filter the content on news feeds, or when search engines generate results that are similar to previous searches. As a result, the content that users come across online tends to only present information that already conforms with their pre-existing preferences.

(iv) **Information overload** refers to the condition where the volume of content available on social media is far more than any person can possibly manage. The widespread use of these platforms has consequently influenced how users choose their information sources, especially since individuals have limited bandwidth when consuming content. In coping with information overload, individuals tend to rely on a smaller subset of their preferred sources when seeking out the latest news, thus limiting their exposure to information and resulting in a selective retention of information.

(v) **Role of social influence.** The people that a social media user follows or interacts with, be it family and friends or known influencers, have an effect on how they make decisions and how they behave. For example, if the majority of people that a user follows on social media have strong anti-smoking views, it

is likely that the user will be influenced to cut down on smoking, or even quit the habit.

Being conscious of the human factor at play is a good start to ensure social media users are less vulnerable to misinformation. To downplay the effects that the human factor can have, social media users must actively seek out differing or alternative views, and accept that there is a wide spectrum of viewpoints on any given subject.

Suggested Discussion Points

- How do search engines and social media platforms know my preferences? Why would I suddenly start seeing digital advertisements of something that I am thinking of purchasing?
  [Possible prompts: Have you been searching for something online? Have you been sharing your GPS location? Have you been browsing for certain products on online shopping sites?]

- How can I play down the effects of human factors? *[Possible prompts: Be familiar with preference settings and seek informed perspectives towards content on social media]*

Advanced Discussion Points:

- In what ways can social media algorithms be manipulated to spread falsehoods or promote harmful views?
  [Possible prompts: Think about social media algorithms and their effects on social disruption through echo chambers, social segregation through homophily, etc.]

Learning Outcome 3: Understand How to Use Information Responsibly

There are many sources of information online, and it can be difficult to discern sources that provide credible information. The tendency for information to go viral quickly, and the potential for it to cause damage, means that there is a need to be equipped with basic knowledge of information sources and the know-how to evaluate online resources critically.

Learning Objectives

Individuals will learn:

- What are some examples of information sources*
- How to assess the credibility of an information source*
- What is the difference between fact and opinion*
- What are the different types of false information
- What is the difference between disinformation and misinformation
- Why people create and spread false information*
- What is the damage caused by creating and spreading false information*

**Content recommended for all participants.*

Broad Takeaways

- Some information sources are more credible than others.
- A fact is a statement that is true and can be proven.
- An opinion is an expression of one's thought or how one feels, and is not always true.
- False information can result in serious consequences and cause damage, so it is important to take steps to determine the reliability of any information encountered.
- If unsure of the veracity of the information, it would be sensible not to post, share or forward it to others.

Suggested Focus Area #1 – Examples of Information Sources

Learning Objectives**:**

- ✓ **What are some examples of information sources***
- ✓ **How to assess the credibility of an information source***
- ✓ **What is the difference between fact and opinion***
- What are the different types of false information
- What is the difference between disinformation and misinformation
- Why people create and spread false information*
- What is the damage caused by creating and spreading false information*

Where We Get Our Information

Examples of Information Sources:

- **Books,** which may include fiction, non-fiction, biographies, etc
  - Books tend to take a longer time to be published, and may provide in-depth perspective on certain issues, but may not reflect the most current developments.
- **News sources** (both print and online), including articles and op-eds in newspapers, news websites (e.g. The Straits Times, Channel News Asia)
  - News sources tend to provide more up-to-date information on current affairs, and are updated throughout the day.
- **Research papers** that are published in scholarly journals or peer-reviewed
  - Research articles may focus on a more specific issue, and is usually written by academics who have conducted relevant research or work in that area.
- **Reference books,** including dictionaries, encyclopaedias
  - Reference books are useful for finding factual information about a broad range of topics.
- **Internet**, which include search engines such as Google
  - All kinds of information are readily available on the Internet across a wide range of issues, written by individuals with different expertise
- **Webpages** of organisations
- **Word-of-mouth communication** (both online and offline) where individuals share information about an issue or organisation with one another, through online social sites and/or offline physical interactions.

It is important to be diligent in checking the information referenced, repurposed or shared for work or research to ensure its credibility. Generally, the following sources of information tend to be more reliable and credible than others, as they would have undergone a process of peer review or fact-checking prior to publication:

- Articles published by a local or international mainstream media company
  - E.g. The Straits Times, Channel NewsAsia, BBC, The New York Times, etc
- Articles or papers written by respected academics or experts in the field

    - E.g. Academics who are identifiable, have relevant credentials, and have written or published about similar topics
- Journals or publications published by University presses or websites
    - E.g. NUS Press, websites ending with .edu
- Official press or official websites
    - E.g. Official press releases, websites ending with .gov

Assessing the Credibility of a Source

Assessing a source's credibility often relies on the context under which it is produced. Even when reliable sources are used, it is useful to ask the following questions about any source of information:

- **Question the source**: Is it plausible? Are there signs of facts being manipulated?
- **Verify the information**: Does this corroborate with other sources, including expert opinions and authoritative sources? Does the author substantiate arguments with factual, relevant, up-to-date evidence?
- **Check for biases**: Is the author known to have or likely to have any vested interests? Are there certain arguments made that may be biased? Who is the author's intended audience?
- **Follow up and digging deeper:** Can the author be contacted for further information or clarification?

When unsure of the veracity of the information, it would be sensible not to post, share or forward it to others.

Differentiating Fact from Opinion

It can be easy to fall for false information when opinions are disguised as facts. The following definitions explain the difference between fact and opinion:

- **Fact:**
    - A piece of information presented as having objective reality.
    - A statement which could be proved or disproved based on evidence, i.e. either verifiably true or verifiably false.
    - Something that be proven and is evidence-based.
    - The Protection from Online Falsehoods and Manipulation Bill (POFMA) defines a 'statement of fact' as 'a statement which a reasonable person seeing, hearing or otherwise perceiving it would consider to be a representation of fact'.

Example
Bencoolen station is one of the deepest MRT stations in Singapore, with its lowest point built 43 metres below street level.

- **Opinion:**
  - A statement based on one's values and beliefs, which cannot be proved or disproved definitively
  - An expression of personal thoughts on an issue
  - A belief, judgement, or way of thinking about something

Example
Bencoolen station is one of the most difficult stations in Singapore to access, as it takes a long time to get from the street to the platform.

Suggested Discussion Points

- Are the following types of online information likely to be credible?
  - A current affairs blog run by a group of students in a university organisation? (answer: it depends, look at the sources that they cite in their articles, whether they can be identified and contacted, whether they have been cited elsewhere)
  - An opinion article published by an academic? (answer: yes, if the academic has relevant credentials in the subject matter that he/she is writing about)
  - Online discussion forums, where users post and comment with a screen names of their choice? (answer: no, as users are often anonymous and may not have the relevant expertise to comment on issues)
  - Train delays reported by the local media? (answer: yes, check that they have also cited evidence from relevant authorities)
- Can you think of some examples where opinions are disguised as facts? *[Possible prompt: As propaganda, fact manipulation]*

Advanced Discussion Points:

- Can you think of circumstances under which a seemingly reliable source might still be biased? What are some possible topics that come to mind? *[Possible prompts: Get participants to discuss possible motivations that experts, companies or organisations may have in purporting a certain stance on an issue.]*
- Why do you think it is important to know how to differentiate between fact and opinion? *[Possible prompt: Opinions carry personal biases, which would be less reliable than a fact]*
- What are some possible dangers that might arise if such varieties of false information remain unnoticed?

Suggested Focus Area #2 - False Information

Learning Objectives**:**

- What are some examples of information sources*
- How to assess the credibility of an information source*
- What is the difference between fact and opinion*
- ✓ **What are the different types of false information**
- ✓ **What is the difference between disinformation and misinformation**
- ✓ **Why people create and spread false information***
- ✓ **What is the damage caused by creating and spreading false information***

False information can pose real dangers to the society by damaging reputation, causing public alarm, and causing tensions between racial and religious groups, as well as between the public and the Government.

The following are various types of false information that are most commonly found online:

- **False connection**
  - False connection happens when a headline or caption leads to the belief that something is different from the actual content of the writing. Online sites often use false connections to lure more people into clicking an article to gain profit.

Example
When an article's headline is "10 Celebrities Who Died This Year", but includes a photo of someone who is still alive.

- **False context**
  - False context happens when quotes are used entirely without, or with deliberately false information about the context in which it was made.

Example
When a critic writes, "It is amazing how terrible this film was,", and the movie's publicity team simply quotes "Amazing" on their posters.

Imposter Content

- In Singapore, imposter content is most often used to scam people into providing personal information such as NRIC numbers or credit card details.

> ***Example***
> When site owners create webpages that look similar to official government sites and by using URLs that resemble URLs of the actual sites (e.g. fake site www.ica-spg.org versus real site www.ica.gov.sg).

Deepfakes: A Complex Form of False Information

Deepfakes are an AI-based technology, which manipulates audio and videos to look and sound like a real person. It can happen in the form of voice filters, in which a person's speech can be manipulated and altered to say specific content or to sound like a completely different person. This is made possible by voice conversion technology, such as, Modulate.ai, which allows one to sound like the opposite sex, or a celebrity of choice. With the use of deepfake software, online users have been able to create a range of fake online content — from Airbnb listings using AI-generated pictures of rooms and hosts, to manipulated videos of politicians behaving in a violent or unprofessional way in public settings.

Deepfakes are especially problematic because they are difficult to identify and are growing increasingly sophisticated. As the capabilities of AI continue to improve, the technology will get better at impersonating the appearance, voice, and even demeanour of any person.

Nonetheless, it is not impossible to spot deepfake videos. The following are some observable traits of such videos:

- **Quality of video:** The quality of the video is not consistent, and some parts tend to be of lower quality than others, as they may be extracted from different footages or sources.
- **Unnatural movements:** The subjects in the video have unnatural bodily movements, such as eyes that are unblinking or unfocused, mouths that are not synced with the audio of the video, or abrupt body movements.
- **Physical appearance:** The skin tone of the subject is inconsistent or poorly shaded, and pixelated or cropped around facial features like the eyes or mouth.
- **Length of video:** The shorter the length of the video, the easier it is for producers to get away with creating a deepfake video.

Disinformation vs Misinformation

Both ‘disinformation’ and ‘misinformation’ are types of false information that can be misleading and potentially cause harm. The key difference in the two terms lies in the intent of the creator of that false information:

- **Disinformation** refers to sharing false information, usually with the intent of manipulating the truth or influencing opinions on a certain issue.
- **Misinformation** refers to the accidental or unintentional sharing of false information.

Reasons Why People Create and Disseminate False Information

- **Malice**, to intentionally spoil someone’s reputation
- **Monetary gain**, to profit from people who believe in that piece of false information or for advertising revenue
- **Mischief**, to prank people as joke without meaning significant harm
- **Political Influence**, to increase social media following or sway public mindshare or opinion about certain leaders or personalities
- **Racial and religious motivation**, to incite hatred or create tension between groups in society

Consequences of the Creation and Dissemination of False Information

- **Stirring fear**: Falsehoods about violence or criminal activity may cause panic and stir fear in communities, especially when communities find that their safety or well-being is at risk. For example, in 2018, false claims circulated on social media that several men were involved in child trafficking, causing angry mobs in eastern India to subsequently beat them to death.
- **Hurting reputations**: When false incidents or accounts are being shared and taken to be true, the people or organisations at the centre of these falsehoods may find it difficult to repair their reputations. Falsehoods tend to be more damaging and have a lasting impact on influential figures like celebrities and politicians, who may find their work being affected by public opinion.
- **Losing money**: Some of these falsehoods are purported with the clear intent of deceiving people into giving them money, either directly through scams or indirectly through advertising platforms.
- **Threatening social harmony**: As falsehoods increasingly permeate public discourse, segments of society may become increasingly polarised along ideological differences, with increasing confidence that each of their respective stances are more legitimate than the other. In some cases, falsehoods about certain segments of society (e.g. claims around certain ethnic communities inciting violence) may escalate into violence and threaten harmony.

Suggested Discussion Points

- What are some examples of fake news that you have come across? How do you think they affect you as an individual?
  [Possible prompts: In 2018, someone reported that a halal stall in Jurong East was selling pork belly. As a result of that false information being reported, business for the stall was indeed affected.]

- Why do you think fake news is becoming more common?
  [Possible prompts: social media makes it easy and quick to spread fake news, cognitive biases amplified by social media algorithms]

- What are some of the ways that deepfakes can be used to create mischief in Singapore?
  [Possible prompts: Automated voice machine scam impersonating the Criminal Investigation Department, or other authorities, could be made even more convincing with the use of voice conversion technology.]

- Recall the cognitive biases that we had learnt in Section 2. How would some of these cognitive biases cause us to fall for false information?
  [Possible prompts: Cognitive biases covered in LO2 include homophily, confirmation bias, echo chambers.]

- Whose responsibility do you think is it to fight fake news? How can you play a part in our fight against fake news?
  [Possible prompts: Check the veracity of information, call out and correct misinformation, or choose not to post or forward if I am unsure]

Advanced Discussion Points:

- Do you think, as a multi-ethnic society, we should be concerned about fake news? Why do you say that? What can it do to us/ Singapore?
  [Possible prompts: Believing fake news could cause dispute between social groups, particularly among a multi-racial and multi-religious society like Singapore.]

- Get participants to practise and share strategies on how they might urge their friends and family members not to share false information unnecessarily, even when it is not malicious in nature.

Learning Outcome 4: Understand How to Protect Oneself on the Internet

A hyper-connected world means greater convenience and increased possibilities, but it can also mean more online dangers. Understanding this can help to minimise the risks inherent in online communications and interaction. In particular, the widespread use of online platforms to access information has resulted in false information becoming a key aspect of online use that one must understand and protect oneself against.

Learning Objectives

Individuals will learn:

- What is cyber wellness*
- What are the threats and risks of social media*
- How to guard against the threats and risks of social media*
- How to check the credibility of information encountered or received

**Content recommended for all participants.*

Broad Takeaways

- One can be a responsible and positive influence online by upholding basic social media etiquette.
- Social media use carries both benefits and risks, and there are steps that one can take to mitigate those risks.

Suggested Focus Area #1 – What is Cyber Wellness

Learning Objectives**:**

- ✓ **What is cyber wellness***
- ○ What are the threats and risks of social media*
- ○ How to guard against the threats and risks of social media*
- ○ How to check the credibility of information encountered or received

The Ministry of Education (Singapore) has defined cyber wellness as the positive well-being of Internet users. Cyber wellness encompasses the range of skills and values that online users should embody in order to be a responsible and positive influence online.

Using online platforms and social media has become a significant part of our daily lives. As interactions are increasingly moving into the online space, it will be important for online users to observe and uphold basic social media etiquette when using the Internet:

(i) Authenticity

Authenticity is about communicating in an honest and open manner and always being clear about one's intentions.

(ii) Transparency

Transparency is about having good intentions when engaging with others online, and only sharing information that can be helpful to others.

(iii) Communication

Communication is about getting to know people and building connections with people online to establish trust. While it is ethical to use social media to sell products/services, responsible users of technology should not use online platforms to hard-sell products or business.

Cyberbullying

Cyberbullying occurs when social media and digital platforms are used as a means to intentionally hurt someone. This can manifest in many ways, e.g. in the form of hurtful comments being directed at individuals, or having compromising information or photos being shared online against their will.

Examples of Cyberbullying

The following are seven common examples of cyberbullying:

- Flaming: using inflammatory or vulgarities on others online
- Harassment: constantly sending vicious and/or disturbing messages to others
- Cyber stalking: ongoing harassment and denigration against others to the extent that the individual feels considerable fear for his/her safety
- Denigration: sending rumours, false statements, gossips to hurt a person's reputation
- Impersonation/masquerade: sharing offensive messages under another person's name and making the person look bad
- Trickery: fooling someone into sharing personal information and posting it online
- Exclusion: deliberately excluding someone from an online group

Effects of Cyberbullying

- Victims may lose interest in school and social activities
- Victims may experience negative feelings such as depression, loneliness and low self-esteem
- Victims may experience poor physical health
- Culprits may also suffer from the consequences of their actions, and this negative reputation may stay with them long after the incident has occurred

How to Deal with Cyberbullying

- For victims of cyberbullying:
    - Stay calm
    - Do not retaliate
    - Save the evidence (e.g. screenshot comments)
    - Block the sender/bully
    - Update privacy settings
    - Remove content from online services
    - Tell a trusted adult (teacher, parents or counsellors)
    - Report the incident to the provider of the service e.g. social networking sites

- For parents:
    - Understand the situation and context in which the incident occurred
    - Be emotionally supportive
    - Take action to identify the culprit or root cause of the problem, e.g. by approaching the child's school or the Internet service provider
    - Equip the child to deal with similar situations in the future

Digital Addiction

When users are preoccupied with checking their online profiles or communication channels regularly, and continue to use their devices for their online activities even when it is not appropriate to do so, they are said to be digitally addicted.

Signs of Digital Addiction

The following are signs of digital addiction:

- Aggression and violence towards those who attempt to limit their use of the Internet
- Easily irritable and anxious
- Inability to distinguish between the online and offline sphere
- Academic performance is affected
- Decrease commitment to personal hobbies, social activities and relationships
- Inability to focus
- Physical symptoms, e.g. obesity, headaches, insomnia

Managing Digital Addiction

It is important to manage digital addiction in order for the individual to achieve positive well-being.

- For individuals who are experiencing digital addiction:
    - Regularly engage in outdoor activities and hobbies
    - Engage in real-life interaction
    - Set a time limit for online activities and stick to it
    - Have tech-free time daily
    - Turn off all gadgets during sleep time to increase quality of sleep

- For parents:
    - Set and agree to a set of rules around technology and device usage
    - Use Wi-Fi routers with parental controls
    - Set house rules regarding digital device usage
    - Explore offline activities as a family

Suggested Discussion Points

- How can you play a part in contributing to a healthier cyberspace?
  [Possible prompts: What are the actions that you will take if you see your classmate being cyberbullied?]

- How can you help a friend who is digitally addicted?
  [Possible prompts: Organise more social activities and actively encourage your friend to take part.]

- Why it is important for you to practise good social media etiquette?
  [Possible prompts: Get them to discuss what these principles are, and then what happens if they are not open/transparent/authentic in their interactions]

Suggested Focus Area #2 – Threats and Risks of Social Media

Learning Objectives**:**

- What is cyber wellness*
- ✓ **What are the threats and risks of social media***
- How to guard against the threats and risks of social media*
- How to check the credibility of information encountered or received

As more people rely on social media as their primary method of communication, there is an increasing need to develop an awareness of the risks that can be found on social media, and knowing how good habits can be cultivated to stay safe on social media.

The following are risks that social media users are commonly susceptible to:

- **Identity theft**, in which online criminals use information from personal details we leave online to build fake identities, usually for monetary gain (e.g. scams of family and friends related to the stolen identity)
- **Information leak,** which refers to the unintended loss of private information from an organisation or individual (e.g. In April 2018, Cambridge Analytica had harvested the personal data and online profiles of millions of Facebook users for political advertising purposes)
- **Online scams,** where people impersonate as someone else for malicious purposes, usually for monetary gain or to obtain personal information. We will learn more about the topic of online scams in the subsequent section on learning *how to use technologies safely and responsibly*.

Suggested Discussion Points

- What are some of the threats and risks that we might be exposed to on social media? Should we be concerned about these risks? Why do you say that?
  [Possible prompts: Is there anyone that you know who might be susceptible to one or more risks?]

- What are some of the functions on social media that may compromise our safety online?
  [Possible prompts: Selecting the "Save My Password" or "Keep Me Logged In" functions may make it easier for hackers to gain full access of their accounts; turning on their locations in real-time to find location tags more easily might allow others to track them down. After participants have shared, the trainer may also wish to emphasise the same tools that have been built in to social media platforms for our convenience can also inadvertently pose certain risks.]

Suggested Focus Area #3 – How to Guard Against Social Media Threats

Learning Objectives**:**

- What is cyber wellness*
- What are threats and risks of social media*
- ✓ **How to guard against the threats and risks of social media***
- How to check the credibility of information encountered or received

Users of social media ought to be familiar with and take the following steps to ensure a basic level of protection against threats:

- **Do not overshare personal details** e.g. by choosing usernames that do not fully reflect user's full name, not sharing content that includes user's personal information such as flight details and NRIC
- **Manage access rights to blogs, sites or social media pages**, e.g. filter comments on personal blogs or sites to prevent spamming of malware or phishing links, disallow strangers to comment on user's social media posts
- **Be aware of the motivations of social media platform providers,** e.g. many social media platforms are free to use, as platform providers seek to amass big user bases to earn advertising revenues and monetising user information (e.g. personal preference)

Suggested Discussion Points

- What do you think are some of the things you can do to reduce social media risks? *[Possible prompts: keeping social media accounts, e.g. Instagram private, etc]*
- How do social media platforms make money? What does that mean for us, as social media users?
  [Possible prompts: Discuss the business models around social media platforms, and how they may use the information of their users for marketing purposes, which is why it is important for users to selectively disclose personal data]

Suggested Focus Area #4 – How to Check the Credibility of Information Encountered or Received

Learning Objectives**:**

- What is cyber wellness*
- What are threats and risks of social media*
- How to guard against the threats and risks of social media*
- ✓ **How to check the credibility of information encountered or received**

How to assess the credibility of a source online?

The sources that users come across online may come in the form of written articles or multimedia formats, including pictures or videos. While the fundamental steps taken to assess the credibility of information sources do not differ significantly, the following are some additional questions specific to online sources that one might ask to verify the credibility of information:

- **Finding out more about the uploader:** Does the uploader have an online profile? Is it possible to tell anything about the uploader based on his/her previous online activities?
- **Looking through the comments:** What kinds of comments are being made about the content? Who are the types of online users commenting and engaging with the information? Are the commenters identifiable and verifiable?
- **Observe the online activity of the content:** Can the information be found on any other websites? Can images or videos be found on other sites using Google reverse image search or YouTube DataViewer?

Given the speed and ease with which online content can be created and reproduced, it is always important to consider if the content is indeed probable and believable, and to check if there are other credible sources relating the same content. If the content is highly implausible, there is a chance that its producers may have vested interests in presenting an issue in a particular manner.

Suggested Discussion Points

- Why do you think it is important to consider and check the veracity of a story or piece of information that you receive or come across online*?*
  [Possible prompts: Vested interests from different people/stakeholders, different presentation of the issue by different people etc.]

Learning Outcome 5: Understand How to Use Digital Technologies Safely and Responsibly

The previous sections of this framework focus on developing among online users an appreciation of the possibilities that online technologies have to offer, and introduce some of the potential risks that have come with communicating on these new platforms. This section focuses on how to use these technologies effectively and responsibly.

Learning Objectives

Individuals will learn:

Protect Personal Data and Cybersecurity, including:

- How to secure digital devices and online accounts*
- How to adjust privacy settings across different social media platforms
- The difference between secured and unsecured Wi-Fi networks, and implications of using each of them
- Common concepts in cybersecurity like encryption and Virtual Private Networks (VPN)

Guard Against Online Scams and Cyber Threats, including:

- What are the different types of online scams*
- What phishing is and how to recognise the tell-tale signs*
- How to respond to an online scam*
- What are the different types of cyber threats
- What cyber threats and malware can do
- How to guard against cyber threats*

**Content recommended for all participants.*

Broad Takeaways

- There are steps that we can take to protect our online accounts and devices by practising basic cyber hygiene habits, so that our information will not be misused.
- There are tell-tale signs of online scams and cyber threats that we can look out for, so that we do not fall prey to malicious actors seeking to obtain our personal information or monetary gain.

Suggested Focus Area #1 – Protecting Personal Data and Cybersecurity

Protecting Personal Data

Learning Objectives**:**

- ✓ **How to secure digital devices and online accounts***
- ✓ **How to adjust privacy settings across different social media platforms**
- The difference between secured and unsecured Wi-Fi networks, and implications of using each of them
- Common concepts in cybersecurity like encryption and Virtual Private Networks (VPN)

As technology becomes more pervasive, it is important to ensure that one's personal data is not accessed by other parties without knowledge or consent. It is important for online users to secure their digital devices and online accounts, which not only keeps their transactions safe, but also ensures that they do not become targets of mischief or criminal activity, such as identity theft.

The following are steps users can take to ensure a basic level of security on their devices:

- **Use strong passwords**
  - One example of a strong password is to combine different words that relate to a memory that is unique to the user, and ensure that the password contains at least 12 characters, uppercase and lowercase letters, numbers, or symbols, e.g. Learntorideabikeat5!
  - Avoid using the 'Remember Password' feature to store passwords.

- **Enable two-factor authentication (2FA)**
  - 2FA uses more than one type of information to identify the user when granting access to online accounts.
  - The first factor is usually a password that the user will know, while the second factor is usually a one-time password (OTP) received via SMS on a separate device.
  - Biometrics is another form of authentication which is commonly used to ensure a higher level of security on devices, and should be used whenever possible, e.g. Touch ID and Face ID authentication on digital devices.
  - This second layer of security ensures that even if a user account has been hacked into, the account will remain protected unless the hacker is able to obtain the second factor of authentication.

- **Choose protected Wi-Fi networks, where possible**
  - WPA2/WPA (Wi-Fi Protected Access) tend to be more secured than WEP (Wired Equivalent Privacy)
  - As a rule of thumb, users should try to turn off wireless connectivity (Wi-Fi and Bluetooth) on their devices when not in use, to prevent auto connection.

- **Disable browsers' autocomplete features**
  - Avoid having credit card information stored on their browsers by disabling the autocomplete feature.
  - In Chrome, go to Settings and select Advanced. Under the Passwords and Forms section, click Autofill settings. Delete any credit card information that has been stored automatically, and toggle off the option to Autofill forms.

- **Identify secure and reputable websites**
  - This is useful when accessing less secure sites, e.g. non-https sites that lead to password sniffing
  - Look out for 'https' in the URL of websites, which indicates that any kind of data (including personal information, credit card details) that is entered on these websites is encrypted, whereas data that is transferred over other websites are more likely to be copied without users' knowledge.

- **Encrypt devices**
  - Encryption makes devices more secure, as they protect all the information on devices with passcodes that only the owner of the device has possession of. Without the passcode, it would not be possible for anyone else to access or read the data that the owner has stored in his/her device. This ensures that users' information remains protected and cannot be accessed easily by others, in the event of theft.

- **Install anti-virus software**
  - Anti-virus software is important because it helps to "guard" and upkeep the health of users' digital devices and computer systems. In particular, the anti-virus software will flag anomalies, detect threats in their mobile apps or online activities and remove malware.

- **Install the latest software updates**
  - Updated software helps to act against known vulnerabilities on the device, whereas outdated software leaves their devices vulnerable to loopholes that can be exploited.

- **Adjust privacy settings on social media platforms**
  - Review and adjust privacy settings on social media platforms to control and be conscious of the type of information that is shared publicly.
  - Consider the type of information to be shared publicly on social media (e.g. email address, date of birth, location tracking and sharing), and remove the unnecessary information or deactivate the unnecessary information sharing settings.

Control the degree of information (e.g. types of posts and photos) that is shared with different social circles (e.g. family, friends and work colleagues) within a social network. Some platforms allow users to do so by categorising their social network and customising the amount of information users would like to share with each category

Common Concepts in Cybersecurity

Learning Objectives:

- How to secure digital devices and online accounts*
- How to adjust privacy settings across different social media platforms
- ✓ **The difference between secured and unsecured Wi-Fi networks, and implications of using each of them**
- ✓ **Common concepts in cybersecurity like encryption and Virtual Private Networks (VPN)**

The following are some examples of concepts that are commonly used in cybersecurity:

- **Unsecured and secured Wi-Fi networks:**
  - **There are primarily two types of networks**
    1. **Unsecured** networks that can be connected, without security features or authentication; and
    2. **Secured** networks that typically require authentication, have security features and may require users to abide by terms of usage.
  - Users should connect to secured networks whenever possible. If there is really a need to use unsecured networks, encrypt the channel with VPN, or access secured pages (https) only.
  - In general, unsecured networks increase the risk of personal data being accessed or stolen by unauthorised users, especially when online transactions are made.
  - Avoid accessing important accounts (e.g. bank accounts) as it is risky to perform any login activity on unsecured networks.
  - Avoid using Wi-Fi networks or hotspots when overseas, as hackers would be able to track online movements via the network users connect to. Compared to public Wi-Fi, cellular networks are generally more secure.

- **Encryption** refers to the process of encoding a message or information in such a way that only authorised parties can access, such that secure information will appear scrambled and unreadable, and can only be decrypted with a decryption key. An encryption key is a random string of bits generated specifically to scramble and unscramble message.
  - Encryption is important as it prevents information from being read by unintended parties, for example when misplaced smart devices or storage devices are picked up, or when sensitive information is mistakenly sent to wrong parties.
  - There are two types of encryption:
    1. **Symmetric encryption,** where the same key is used for encryption and decryption, and
    2. **Asymmetric encryption,** where a different key is used for the encryption and decryption process. There are commonly two keys, one private and one public.
  - It is useful to note that different encryption standards have different degrees of security, and weak encryptions can be cracked relatively easily with sufficient computing power or bypassed with sophisticated approaches.

- **Virtual Private Network (VPN)** refers to a type of connection where data travelling is encrypted, to shield online activity from being tracked.
- **Anti-virus software** refers to applications that offer the security of detecting and removing malicious codes that could send users' data to hackers. When choosing an anti-virus app, users should consider factors such as automatic updates and scanning, malware removal capabilities and user-friendly features.

Suggested Discussion Points

- Get participants to share the types of privacy and security settings that they currently apply across their devices.
- What types of privacy settings should you apply to your different online accounts? (e.g. Facebook? LinkedIn? Twitter?)
- How do you think our personal data can be used against us?
  [Possible prompts: Our personal information can be used by criminals to commit illegal activity without our knowledge]
- How do you think our personal data can be used against us? *[Possible prompts: our personal information can be used by criminals to commit illegal activity without our knowledge]*
- Get your participants to share if they practise good cyber habits (e.g. use strong passwords/ enabled 2FA/ update software).
- What are your personal challenges to adopting these habits?

Suggested Focus Area #2 – Online Scams and Cyber Threats

Online scams are designed to trick users into giving away money, personal details, or data by offering attractive deals or false information through the digital platforms. On the other hand, cyber threats are malicious attempts that have the potential to cause the loss of digital data by breaching the information system of an individual or organization. Both types of online dangers are common in popular digital platform, and thus it is important for anyone to be aware of these dangers, and know how to identify and respond to them appropriately.

Types of Online Scams

Learning Objectives:

- ✓ **What are the different types of online scams***
- ✓ **What phishing is and how to recognise the tell-tale signs***
- ○ How to respond to an online scam*
- ○ What are the different types of cyber threats
- ○ What cyber threats and malware can do
- ○ How to guard against cyber threats*

The following are definitions and key characteristics of the common types of scams that one might encounter in Singapore:

Phishing Scam

A type of scam characterised by deceiving victims into providing personal information, such as login credentials or credit card number, through various methods. Victims may receive a call informing them that they have won a lucky draw. Another variety of phishing scams involve the creation of fake websites that look very similar to the original website, for the intent of luring victims to provide personal information on the webpage.

The following are signs of phishing that online users should look out for:

- Mismatched and misleading information
- Use of urgent or threatening language
- Promises of attractive rewards
- Requests for confidential information
- Unexpected emails
- Suspicious attachments

Online Purchase Scam

A type of scam where online users are often enticed by seemingly good deals for items such as concert tickets or electronic gadgets. The “seller” would prompt the user to transfer payment before delivering the item. The “seller” will sometimes demand for further payment, under the guise of additional delivery charges. Ultimately, the user never receives the item.

Example: Invalid tickets to Universal Studios Singapore
Between January to April 2019, police received over 100 reports of multiple scams involving the booking of hotel rooms or attractions. In particular, several victims had purchased tickets to the Universal Studios Singapore online, and either received invalid tickets or failed to receive any tickets after the payments were made.

Police has since issued an advisory for buyers to read reviews of sellers before making purchases, or to try to visit platforms that only released payments to buyers after the purchased items have been received.

Credit-for-Sex Scam

A type of scam where a stranger befriends the user through social media platforms like Line, or online dating websites, such as Tinder. The victims are usually asked to purchase a gift card or to make an advanced deposit, in exchange for sexual services. Some of these interactions are also intercepted by third party, usually an intimidating “superior”, who would cut off all further communication or threaten the victims if they refused to proceed with payment.

Example: Credit-for-sex transaction blocked by a “big brother”
In June 2019, a man in his late-twenties was browsing through online classifieds on March 12 when he came across someone claiming to provide sexual services. He agreed to meet her in Hougang at 2pm the next day. Once he had arrived at Hougang, he received a call from a man claiming to be the "big brother" of the woman he was supposed to meet. He transferred almost $700 worth of “protection fees” in three transactions to the scammers, thinking that he was going to meet the woman after. He only realised that he was being scammed when the “big brother” called him again to ask for more money.

Internet Love Scam

These scams are typically characterised by an online user befriending a person online. After gaining the trust of the online user, the scammer would proceed to ask for money as a proof of love, usually on the pretext of an emergency or having fallen into difficult times. The scammer tends to be uncontactable after he/she has received the money.

Example: Woman loses $22,000 to a man that she meets online

In June 2019, a woman reported that she had been scammed by a friend that she had met and developed feelings for through the online dating app, Coffee Meets Bagel. She had been talking to a guy that she had met through the app for over a month, and quickly developed feelings and got engaged to him, despite not having met him in person. He had told her several stories about falling into financial difficulty, including the freezing of his property in Jakarta, which would require him to make a payment of $12,000. By the time she realised that her "fiancé" was no longer coming to meet her and that she had been scammed, she had already accumulated over $22,000 in debt from banks and moneylenders.

Investment Scam

A type of scam where users receive messages from people claiming to be from financial companies on social networking sites like WeChat or WhatsApp. When the user replies to such messages, they will then be exposed to an investment scam where the scammers ask for their personal information, such as NRIC. The user will then be asked to transfer money to specific banks, and to pay administrative fees in order to receive their investment returns. The scammer may sometimes call the user to request for a deposit in order for profits to be released.

Example: Misuse of Finance Minister's name in endorsing bitcoin investment company

In May 2019, an online user was browsing a bitcoin investment site when he saw that Finance Minister Heng Swee Keat had allegedly "supported" a particular bitcoin investment company. The user subsequently opened a trading account with this company, and deposited USD500 into the account. It was only when she received an email requested for a copy of her credit card and additional information that she became suspicious, and called her bank to freeze her card and withhold payments to the scam company.

Loan Scam

A type of scam that involves text messages offering loans and loan services to random users. The lenders tend to claim to be from a licensed moneylender, and interested parties would have to transfer some form of deposit before the loan can be disbursed, often along with personal information like NRIC and contact numbers. The scammer tends to be uncontactable after he/she has received the transfer.

> ***Example: Loan scams involving "processing fees and blocked accounts"***
> In June 2019, online users saw an advertisement on Facebook for loan services. One particular user took up a loan of $5,000, which he would pay back through a monthly instalment plan. However, the user was subsequently asked to pay a series of additional fees before he obtained the loan: $150 to process the loan, another $1,850 to get the loan approved, and etc. The loan company eventually claimed that their accounts were blocked, and that they needed another $10,000 to unblock these accounts.

Impersonation Scam

In impersonation scams, victims tend to be contacted by someone disguising as a government official or representative of an organisation. The scammers subsequently inform victims that they have to make some form of payment or provide some personal information, including identification numbers or bank account numbers, urgently.

> ***Example: Scammers impersonate as IRAS officers to collect overdue taxes***
> In April 2019, the Inland Revenue Authority of Singapore (IRAS) cautioned that several scammers have attempted to pose as IRAS officers to extort money from individuals. In these incidents, scammers have informed victims that their taxes were due for immediate payment, and proceeded to give them a bank account number to transfer money to. Some scammers even used telephone numbers that corresponded with IRAS' Individual Income Tax helpline, or email addresses that ended with 'iras.gov.sg', making these requests appear more legitimate. IRAS has since issued an advisory to remind Singaporeans that the authority would not request for personal information from individuals over the phone or email.

How to Respond to an Online Scam

Learning Objectives**:**

- What are the different types of online scams*
- What phishing is and how to recognise the tell-tale signs*
- ✓ **How to respond to an online scam***
- What are the different types of cyber threats
- What cyber threats and malware can do
- How to guard against cyber threats*

The following are steps that individuals can take in response to an online scam:

- Change the passwords of related accounts immediately
- Run a full system scan with anti-virus software
- Alert bank promptly if they have revealed banking details
- Keep an eye on all their accounts for suspicious activity (e.g. unauthorised purchases, withdrawals)
- Lodge a police report if they incur any monetary loss
- Report phishing attempt to the organisation that was misrepresented and the Singapore Computer Emergency Response Team (SingCERT)
- Report calls or SMSes promoting easy financial loans or get-rich-quick betting to the National Crime Prevention Council, or lodge a police report
- Call the anti-scam helpline, and access other related resources at www.scamalert.sg

Types of Cyber Threats

Learning Objectives**:**

- What are the different types of online scams*
- What phishing is and how to recognise the tell-tale signs*
- How to respond to an online scam*
- ✓ **What are the different types of cyber threats**
- ✓ **What cyber threats and malware can do**
- How to guard against cyber threats*

The following are the common types of cyber threats:

- **Website defacements**: Refers to an attack on a website that alters the visual appearance of the page to replace the hosted webpage with one of their own sites.
- **Phishing**: Refers to any deliberate attempt to obtain confidential information, including personal details or bank account information, by falsifying their identity and posing as some form of authority.
- **Malware:** Malware, which is short for malicious software, are programs devised to compromise the security of a computer system or mobile device.
- **Compromised systems**: Computer systems being broken into without permission or knowledge and use for malicious activities.
- **Ransomware**: A type of malicious software that denies access to a computer or data system until a ransom is paid, typically spread through phishing emails

How to Guard Against Cyber Threats

Learning Objectives:

- What are the different types of online scams*
- What phishing is and how to recognise the tell-tale signs*
- How to respond to an online scam*
- What are the different types of cyber threats
- What cyber threats and malware can do
- ✓ **How to guard against cyber threats***

The following are steps that users can take to safeguard against cyber threats and malware:

- Exercise caution when clicking on links (including ads and social media posts), especially if they appear dubious
- To ensure that the URL is the same as the actual website that the link purportedly leads to, hover mouse cursor over the links to ensure that the URL of the link is not mismatched
- Install and update anti-virus software to prevent malware infections
- Only install software (especially executables (with .exe, .pkg, or .dmg extensions)) from trusted sources,
- Maintain user and location privacy by using browser extensions that block plug-ins

Suggested Discussion Points:

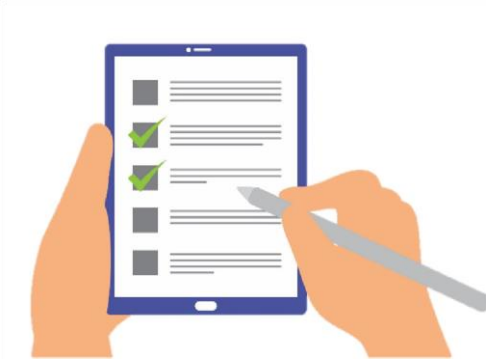
- What are some types of online scams you could or have encountered? Do you know how to respond and guard against them?
  [Possible prompts: Have you seen online shopping deals that are too good to be true, or receive messages or requests from people that you do not know? Cyber criminals often take advantage of popular periods, such as during promotional events, to carry out scams.]

- Do you know how to verify the identity of the person or entity, if you receive communications (e.g. message, email, phone call) from a source that you are unsure of?
  [Possible prompts: If you receive an email claiming to be from your bank, would your bank be able to confirm this if you contacted the bank separately to verify the authenticity of the email?]

- Do you know where you can go to for up to date information on scams in Singapore?
  [Possible prompts: SPF Scam Alert]

- What are some simple steps that you can take to safeguard against cyber threats and malware?
  [Possible prompts: Are unknown executable files (e.g. .exe files) safe to open? Are websites with dubious-looking URL safe?]

For Programme Owners



A Guide to Using the Framework

For Programme Owners:
Guide to Using the Framework

The Digital Media and Information Literacy Framework establishes a set of common outcomes for programme owners to work towards, and focuses on developing in Singaporeans:

a. A fundamental appreciation of the benefits, risks and possibilities that technology can bring and how online platforms and digital technologies work;
b. A basic understanding of how to use information responsibly,
c. The know-how for safe and responsible use of digital technologies.

The Framework sets out 5 key learning outcomes (LOs):

LO1 Appreciate the benefits, risks and possibilities that technology can bring
LO2 Understand how online platforms and digital technologies work
LO3 Understand how to use information responsibly
LO4 Understand how to protect oneself on the Internet
LO5 Understand how to use technology safely and responsibly

Application of the Framework

The broad outcomes set the direction for all Singaporeans to work towards. The learning outcomes would apply to all individuals, regardless of where they are at in their digital journey.

It is recommended that the delivery of learning objectives be customised according to the needs of the specific programme audience (e.g. with the use of appropriately pitched examples and scenarios). This should be based on the target segment's comfort level with digital technology.

The table below outlines the minimal level of coverage for all individuals, including those who are less digitally savvy.

LEARNING OUTCOMES (LOS)	CORRESPONDING LEARNING OBJECTIVES	LEVEL/S
LO 1 **Appreciate the benefits, risks and possibilities that technology can bring**	☐ Why it is important to keep up with rapidly advancing technology ☐ How technology can bring both benefits and risks *At end of LO1, any individual should minimally be able to articulate the following:* ☐ *Technology is always advancing; keeping up to date with the changes ensures one is better placed to benefit from it.*	☐ All (Fundamental)

LEARNING OUTCOMES (LOS)	CORRESPONDING LEARNING OBJECTIVES	LEVEL/S
	☐ *Technology helps make lives better but it can also be abused if it falls into the wrong hands.*	
LO 2 **Understand how online platforms and digital technologies work**	☐ How digital footprints work and how to manage them *<u>At end of LO2, any individual should minimally be able to articulate the following:</u>* ☐ *There are various mechanisms at work on search engines and social media platforms that determine what content we come across or receive.* ☐ *There are human factors at play on social media that affect how we think or respond towards others.* ☐ *Therefore, it is important for one to actively seek out differing or alternative views, and accept that there is a whole spectrum of viewpoints on any given subject.*	☐ All (Fundamental)
	☐ How algorithms work on the Internet ☐ How digital advertising works ☐ How human factors can influence thinking and behaviour online	☐ Intermediate & onwards
LO 3 **Understand how to use information responsibly**	☐ What are some examples of information sources ☐ How to assess the credibility of an information source ☐ What is the difference between fact and opinion ☐ Why people create and spread false information ☐ What is the damage caused by creating and spreading false information *<u>At end of LO3, any individual should minimally be able to articulate the following:</u>* ☐ *Some information sources are more credible than others.*	☐ All (Fundamental)

LEARNING OUTCOMES (LOS)	CORRESPONDING LEARNING OBJECTIVES	LEVEL/S
	☐ *A fact is a statement that is true and can be proven, or a statement which a reasonable person seeing, hearing or otherwise perceiving it would consider to be a representation of fact.* ☐ *An opinion is an expression of one's thought or how one feels, and is not always true.* ☐ *False information can result in serious consequences and cause damage, so it is important to take steps to determine the reliability of any information encountered.* ☐ *If unsure of the veracity of the information, it would be sensible not to post, share or forward it to others.*	
	☐ What are the different types of false information ☐ What is the difference between disinformation and misinformation	☐ Intermediate & onwards
LO4 **Understand how to protect oneself on the Internet**	☐ What is cyber wellness ☐ What are the threats and risks of social media ☐ How to guard against the threats and risks of social media *<u>At end of LO4, any individual should minimally be able to articulate the following:</u>* ☐ *One can be a responsible and positive influence online by upholding basic social media etiquette.* ☐ *Social media use carries both benefits and risks, and there are steps that one can take to mitigate those risks.*	☐ All (Fundamental)
	☐ How to check the credibility of information encountered or received	☐ Intermediate & onwards
LO 5 **Understand how to use technology safely and responsibly**	<u>Protect Personal Data and Cybersecurity, including</u> ☐ How to secure digital devices and online accounts	☐ All (Fundamental)

LEARNING OUTCOMES (LOS)	CORRESPONDING LEARNING OBJECTIVES	LEVEL/S
	<u>Guard against Online Scams and Cyber Threats, including</u> ☐ What are the different types of online scams ☐ What phishing is and how to recognise the tell-tale signs ☐ How to respond to an online scam ☐ How to guard against cyber threats <u>*At end of LO5, any individual should minimally be able to articulate the following:*</u> ☐ *There are steps that we can take to protect our online accounts and devices by practising basic cyber hygiene habits, so that our information will not be misused.* ☐ *There are tell-tale signs of online scams and cyber threats that we can look out for, so that we do not fall prey to malicious actors seeking to obtain our personal information or monetary gain.*	
	<u>Protect Personal Data and Cybersecurity, including</u> ☐ How to adjust privacy settings across different social media platforms ☐ The difference between secured and unsecured Wi-Fi networks, and implications of using each of them ☐ Common concepts in cybersecurity like encryption and Virtual Private Networks (VPN) <u>Guard against Online Scams and Cyber Threats, including</u> ☐ What are the different types of cyber threats ☐ What cyber threats and malware can do	☐ Intermediate & onwards

For Individuals

Self-Assessment Checklist

For Individuals:
Self-Assessment Checklist

This checklist helps individuals to assess the extent to which they have met the three broad outcomes set out in the digital media and information literacy framework. The broad outcomes for all Singaporeans have been distilled into the following 5 learning outcomes (LOs) outlined in the framework:

For Individuals	For Programme Owners	
Appreciation of Technology	**LO1**	Appreciate the benefits, risks and possibilities that technology can bring
	LO2	Understand how online platforms and digital technologies work
Basic Understanding of How to Use Information Responsibly	**LO3**	Understand how to use information responsibly
Know-how for Safe and Responsible Use of Technology	**LO4**	Understand how to protect oneself on the Internet
	LO5	Understand how to use digital technologies safely and responsibly

Read each statement and check the box (Agree, Disagree) accordingly.

	Disagree	Agree
Appreciation of Technology		
It is important for me to keep up to date with the changes in technology.	□	□
I understand that technology can help to make lives better, but it can also be abused if it falls into the wrong hands.	□	□
I know how to manage my digital footprints.	□	□
I have a general idea of how algorithms work on the Internet.	□	□
I know that there are risks associated with digital advertising.	□	□
I know there are human factors at play on social media that affect how we think or respond towards others.	□	□

If you have answered 'Disagree' to any of the above questions, you are encouraged to check out Learning Outcomes 1 and 2 of the Digital Media and Information Literacy Framework.

Read each statement and check the box (Agree, Disagree) accordingly.

	Disagree	Agree
Basic Understanding of How to Use Information Responsibly		
I know what are some examples of credible sources of information.	□	□
I can explain the difference between fact and opinion.	□	□
False information can result in serious consequence and cause damage.	□	□
I know how to determine the reliability of any information that I encounter.	□	□
If I am unsure about whether the information is true or not, I should avoid posting, sharing or forwarding information.	□	□

If you have answered 'Disagree' to any of the above questions, you are encouraged to check out Learning Outcome 3 of the Digital Media and Information Literacy Framework.

Read each statement and check the box (Agree, Disagree) accordingly.

	Disagree	Agree
Know-how for Safe and Responsible Use of Technology		
I know what I can do to be a responsible and positive influence on social media.	□	□
I know what are some of the threats and risks of social media.	□	□
I know how to guard against the threats and risks of social media.	□	□
I know how to check the credibility of information encountered or received	□	□
I know what to do to secure my digital devices and online accounts.	□	□
I know how to adjust my privacy settings across different social media platforms.	□	□
I know what is the difference between secured and unsecured Wi-Fi networks.	□	□
I know what encryption and Virtual Private Network is.	□	□
I can name the different types of online scams.	□	□
I know how to recognise the tell-tale signs of phishing.	□	□
I know how to respond to an online scam.	□	□
I know what the different types of cyber threats are.	□	□
I know what cyber threats and malware can do.	□	□
I know what to do to guard against cyber threats.	□	□

If you have answered 'Disagree' to any of the above questions, you are encouraged to check out Learning Outcomes 4 and 5 of the Digital Media and Information Literacy Framework.

Additional Resources

Additional Resources

Here are some additional websites for individuals and organisations to keep up to date on the latest information, news and resources around digital media and information literacy:

- The Media Literacy Council (MLC)'s **Better Internet Campaign** website contains various articles, tip sheets and guides for parents, youth and educators on a range of digital literacy issues, including cyber-bullying, fake news and privacy concerns.

- The National Crime Prevention Council (NCPC)'s **Scam Alert** website contains a repository of the latest scam stories, statistics and multi-media resources for the general public. Find out more at https://www.scamalert.sg/.

- The National Library Board (NLB)'s **Source. Understand. Research. Evaluate. (S.U.R.E.)** website contains resources and tip sheets on fact-checking and information literacy in all four languages. Find out more at http://www.nlb.gov.sg/sure/sure-campaign/.

- The Cyber Security Agency of Singapore (CSA)'s **Gosafeonline** website contains various resources for parents, students and businesses on topics around good cyber security practices. Find out more at https://www.csa.gov.sg/gosafeonline.

- The Personal Data Protection Commission Singapore (PDPC)'s website contains resources for organisations and individuals on protecting personal data and more information about the Personal Data Protection Act. Find out more at https://www.pdpc.gov.sg/.

Glossary of Terms

Term	Definition
A	
Anti-virus Software	A program that monitors a device or network to detect or identify major types of malicious codes and to prevent or contain malware incidents, sometimes by neutralizing or removing malware codes.
Authoritative Information	Information obtained from a source that is highly trusted, reliable and accurate. Examples include archival documents or databases, recognised publications by industry experts or peer-reviewed publications and journals.
C	
Compromised System	A system that has been maliciously broken into.
Confirmation Bias	The tendency to interpret new evidence as confirmation of one's existing beliefs or theories.
Credit-for-Sex Scam	A type of scam where a stranger befriends the user through social media platforms, then talks the user into buying them a purchase or gift card, often in exchange for a meet-up, date or sexual favours.
Cyber Bullying	When electronic gadgets are used as a means to intentionally hurt someone in cyberspace.
Cyber Threats	The malicious attempt to damage or disrupt computer networks or systems (e.g. to propagate viruses and worms, website defacements, malware infections) by cyber criminals.
D	
Deepfake	An AI-based technology which manipulates audio and videos to look and sound like a real person, saying something that that person has never said.
Digital Addiction	The excessive compulsion to use digital technology.
Digital Advertising	A type of marketing and advertising that uses the Internet to send marketing messages to people online. Examples of digital advertising include advertisements that are played before a user can access a product, sponsored posts on social media platforms.
Digital Footprint	The trail of data that a user creates while using the Internet. Examples of digital footprints include a user's search history, text messages, photos and videos accessed or uploaded, tagged photos, 'likes' on social media sites, etc.
Digital Media	A type of content that can be read and transferred on digital platforms such as computer networks and the Internet.
Disinformation	The deliberate creation and non-accidental sharing of false information.
E	
Echo Chamber	An environment in which a person encounters only beliefs or opinions that coincide with their own, so that their existing views are reinforced and alternative ideas are not considered.
Electronic Personhood	A term used to describe the potential legal status of sophisticated robots and other manifestations of artificial intelligence.
F	
Fact	A statement that can be proven and is evidence-based.
Fake News	A very specific type of false information, which is (1) driven by intention to deceive, (2) politically and/or economically motivated, (3) deliberate

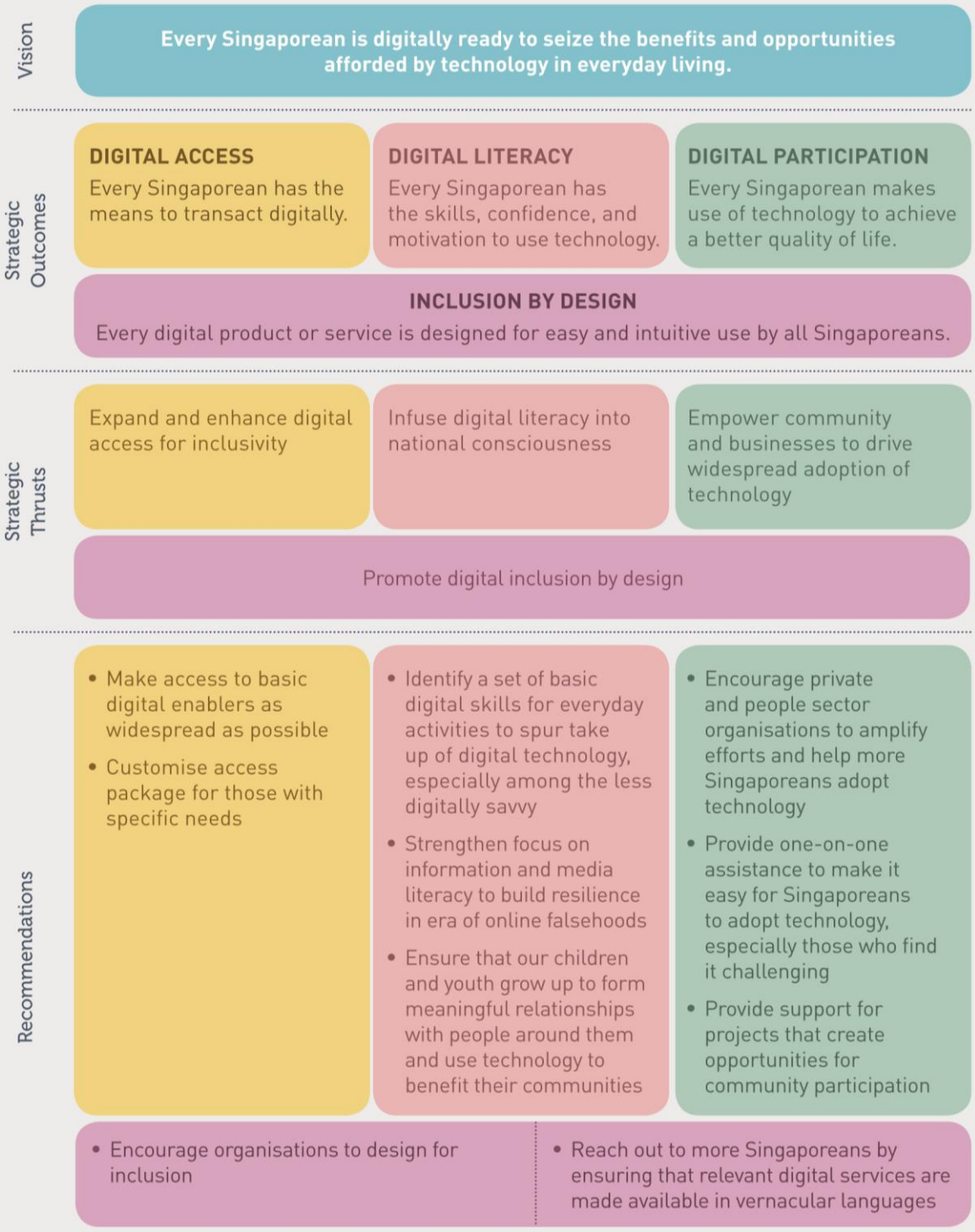
	fabrication of false content and (4) assumes the form and appearance of authoritative news sources.
False Connection	When a headline or caption leads to the belief that something is different from the actual content of the writing.
False Context	When quotes are used entirely without, or with deliberately false, information about the context in which it was made.
H	
Homophily	The tendency for people to seek out or be attracted to those who are similar to, and hold similar views to themselves.
I	
Identity Theft	The deliberate use of someone else's identity, usually as a means to make a financial profit or other benefits in the other person's name.
Impersonation Scam	A type of scam where the scammer impersonates a government official.
Imposter Content	When webpages are created to look similar to legitimate government sites, often to scam people of their private information.
Information Ecosystem	The entire landscape of information that is available for public consumption and reference.
Information Literacy	An awareness of when information is required, and the competency to locate, evaluate and apply that information in its appropriate context.
Information Leak	The unintended loss of sensitive data by an organisation or individual.
Internet Love Scam	A type of scam where an online user befriends a person online. After gaining the trust of the online user, the scammer would proceed to ask for money as a proof of love, usually on the pretext of an emergency or having fallen into difficult times.
Investment Scam	A type of scam where users receive messages from people claiming to be stockbrokers or bank or financial company employees on social networking sites.
L	
Loan Scam	A type of scam that involves text messages offering loans and loan services to random users.
M	
Malvertising	The use of online, malicious advertisements to spread malware and compromise systems.
Malware	A computer software intentionally designed to cause damage to a computer, serve, client or computer network or mobile device.
Misinformation	The unintentional sharing of false information.
Misleading Content	When writers sometimes use real information to make an issue or person seem different from what they really are.
O	
Online Falsehoods	A false statement of fact that is communicated electronically, and includes fake news, disinformation and misinformation.
Online Purchase Scam	A type of scam where online users are often tempted by what seems like a good deal, then prompted to transfer payment to the "seller". Ultimately, the victim never receives the item.
Online Scams	The dishonest schemes and attempts by criminals to take advantage of unsuspecting people to gain a benefit, whether in terms of money or access to personal details, through interactions or activities that take place online (e.g. spam emails, phishing links).
Opinion	A statement based on one's values and beliefs, and could not be proved or disproved definitively.
P	

Phishing	A method of trying to solicit personal information using deceptive emails and websites, by someone posing as a legitimate authority or organisation.
R	
Ransomware	A type of malware which restricts access to the computer system it infects, and demands a random to be paid to the owner of the malware in order for the restriction to be lifted.
S	
Social Media Algorithms	A set of calculations that can be used to determine what content is delivered to the user.
Social Media Etiquette	A code of behaviour within the context of social media platforms.
V	
Virtual Private Network (VPN)	A technology that creates a safe and encrypted connection over a less secure network, such as the Internet.
W	
Website Defacement	An attack on a website that changes the visual appearance of the site or the webpage.

Digital Readiness Blueprint Recommendations

Strategic Thrusts

To achieve the desired outcomes described earlier, this blueprint offers 10 recommendations which are categorised into four strategic thrusts.



References

List of References

"Anti-Cyberbullying Tips", *Better Internet Campaign* www.betterinternet.sg/SID-Campaign-2018/Tipsheets/Cyberbullying
"A Parent's Guide to Keeping Children Safe & Smart Online", *Latest resources for parents* https://www.betterinternet.sg/-/media/Resources/PDFs/Parents-Guides/Safe-and-Smart-Online-Parent-Guide.pdf
"Artificial Intelligence in Advertising: How Marketers Can Leverage Artificial Intelligence Along the Consumer Journey". *Journal of Advertising Research. 58. 263-267.* https://www.researchgate.net/publication/327500836_Artificial_Intelligence_in_Advertising_How_Marketers_Can_Leverage_Artificial_Intelligence_Along_the_Consumer_Journey/citation/download.
Balanced Use of ICT ictconnection.moe.edu.sg/cyber-wellness/cyber-wellness-101/balanced-use-of-ict_
"Business Slow at Westgate Stall after Confusion over Halal Status.", *The New Paper* www.tnp.sg/news/singapore/business-slow-westgate-stall-after-confusion-over-halal-status.
"Cyber Attack - What Are Common Cyberthreats?", *Cisco Systems* www.cisco.com/c/en/us/products/security/common-cyberattacks.html.
"Cyber-Bullying", *Better Internet Campaign* www.betterinternet.sg/Resources/Resources-Listing/Youth---cyber-bullying
"Cyber Threat.", *Computer Security Resource Center* https://csrc.nist.gov/glossary/term/cyber_threat
"Cyber Tip - Use Strong Passwords And Enable 2FA.", *Cyber Security Agency of Singapore*, www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/use-strong-passwords.
Cyber Wellness Syllabus https://www.moe.gov.sg/education-in-sg/our-programmes/cyber-wellness
"Defending Against Infocomm Threats Masterclass.", QED Consulting, https://www.qed.sg/masterclass/defending-against-information-communication-threats-workshop.
"Digital Advertising.", *Better Internet Campaign 2019* www.betterinternet.sg/.
"Digital Footprint.", *Better Internet Campaign 2019* www.betterinternet.sg/.
"Digital Footprints: Creation, Implication, and Higher Education", *NSUWorks,* nsu.nova.edu/fdla-journal/vol3/iss1/11/.
"Dis/Misinformation Training.", *Storyful* storyful.com/.

"E-Payment Learning Journey", IMDA, https://www.imda.gov.sg/imsilver/whats_new/e-payment-learning-journey-2018
"Facebook Says Data Leak Hits 87 Million Users, Widening Privacy...", *Reuters* www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM.
"Facebook, Twitter and the Digital Disinformation Mess.", *Bloomberg* www.bloomberg.com/news/articles/2019-05-18/facebook-twitter-and-the-digital-disinformation-mess-quicktake.
"Fake News Glossary.", *S.U.R.E.* www.nlb.gov.sg/sure/fake-news-glossary/.
"Feedback Loops and Echo Chambers: How Algorithms Amplify Viewpoints.", *The Conversation* https://theconversation.com/feedback-loops-and-echo-chambers-how-algorithms-amplify-viewpoints-107935
"General Perception of Word-of-Mouth Communication as a Source of Information: The Case of Singapore", *Asia-Australia Marketing Journal* www.sciencedirect.com/science/article/pii/S1320164695702702
"Help Protect Your Digital Footprint from Prying Eyes.", *Norton by Symantec* us.norton.com/internetsecurity-privacy-clean-up-online-digital-footprint.html.
"Helping Your Students Cope with Cyberbullying", *Better Internet Campaign* https://www.betterinternet.sg/SID-Campaign-2018/Tipsheets/-/media/915BFCD92602444A875490B4AB8DA0D3.ashx
"HK Robot Sophia Gets Saudi Citizenship. Did She Convert to Islam?", *South China Morning Post* https://www.scmp.com/news/world/middle-east/article/2117568/saudi-arabia-grants-citizenship-hong-kong-robot-sophia-rights
"How does Facial Recognition Work?" *Norton Symantec Corporation* https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html
"How to Spot a Fake Government Website.", *Singapore Government* https://www.gov.sg/article/watch-out-for-fake-govt-websites-and-links-by-scammers-taking-advantage-of-covid-19-situation
"Let's Fight Scams.", *ScamAlert* www.scamalert.sg/
"LibGuides: Information Literacy Guide: Types of Information Sources", *Types of Information Sources – Information Literacy Guide - -LibGuides at University of Fort Hare* ufh.za.libguides.com/c.php?g=91523&p=590868
"Malvertising.", *Center for Internet Security* www.cisecurity.org/blog/malvertising/
"Media Literacy Tips for Adult.", *Better Internet Campaign 2019* www.betterinternet.sg/

"News and Media Literacy Toolkit", *Better Internet Campaign 2019* www.betterinternet.sg/Resources/Resources-Listing/Educators---CSE-Toolkit.
"Police Warn of More Business Email Impersonation Scams.", *Channel News Asia* www.channelnewsasia.com/news/singapore/business-emails-fake-hacked-scams-suppliers-10704198.
"Protect Yourself With These Tips When Shopping Online", *Cyber Security Agency,* https://www.csa.gov.sg/Tips-Resource/Resources/gosafeonline/2018/Protect-Yourself-With-These-Tips-When-Shopping-Online
"Singapore Cyber Landscape 2018", *Cyber Security Agency of Singapore* https://www.csa.gov.sg/Tips-Resource/publications/2019/Singapore-Cyber-Landscape-2018
"Social Media: How to Protect Yourself from Threats.", *Norton by Symantec* uk.norton.com/norton-blog/2016/12/social_media_howto.html.
"Social Media Isn't an Echo Chamber, You Are.", *World Economic Forum* www.weforum.org/agenda/2018/04/actually-social-media-isn-t-an-echo-chamber/.
"S.U.R.E. Campaign.", *S.U.R.E.* www.nlb.gov.sg/sure/sure-campaign/.
"The Danger of Fake News", *Infocomm Media Development Authority* www.imda.gov.sg/imsilver/whats_new/the-danger-of-fake-news.
"The Do's and Don'ts of Using Public Wi-Fi.", *Norton by Symantec* us.norton.com/internetsecurity-wifi-the-dos-and-donts-of-using-public-wi-fi.html.
"Tips to Counter Bullying", Better Internet Campaign https://www.betterinternet.sg/SID-Campaign-2018/Tipsheets/-/media/17B1E4D64D9B4324A8569F161CEB2CF0.ashx
"Types of Fake News.", *Online Discernment (Fact-Checking)* www.betterinternet.sg/SID-Campaign-2018/Tipsheets/Online-Discernment.
"What Is a Scam.", *ScamAlert* www.scamalert.sg/.
"What We Believe In.", *Better Internet Campaign 2019* www.betterinternet.sg/.
"Why Am I Seeing This? We Have an Answer for You.", *Facebook Newsroom* newsroom.fb.com/news/2019/03/why-am-i-seeing-this/.