WiFI DX
Women ICT Frontier Initiative

APCICT
Asian and Pacific Training Centre for Information and Communication Technology for Development
ESCAP

Course on

# Trust and Security Using Digital Technologies

# Trust and Security Using Digital Technologies

## Women Entrepreneur Track

ESCAP
APCICT
Asian and Pacific Training Centre for Information and Communication Technology for Development

## Trust and Security Using Digital Technologies



Disclaimers: The views expressed herein are those of the authors, and do not necessarily reflect the views of the United Nations. This publication has been issued without formal editing, and the designations employed, and material presented do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.
Mention of firm names and commercial products does not imply the endorsement of the United Nations.

Correspondence concerning this report should be addressed to the email: apcict@un.org


Printed in Republic of Korea
Cover design: Amal Kadir

Contact:
Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT/ESCAP)
5th Floor G-Tower, 175 Art Center Daero
Yeonsu-gu, Incheon, Republic of Korea
Tel +82 32 458 6650

Email: apcict@un.org

# PREFACE

The Women ICT Frontier Initiative (WIFI), launched in 2016, is APCICT's flagship ICT capacity-building programme for women's entrepreneurship. It aims to enhance the skills of women entrepreneurs in utilizing digital tools in their businesses. It also seeks to support policymakers in creating an environment that is conducive for digitally-empowered women entrepreneurs.

Recent challenges in the global landscape, such as the COVID-19 pandemic, necessitated a review of APCICT's training support for women entrepreneurs. The pandemic was a wake-up call that significantly impacted women-owned enterprises and underscored the importance of the digital transformation of businesses. It not only exposed vulnerabilities but also the need for women entrepreneurs to harness the power of technology in a holistic manner.

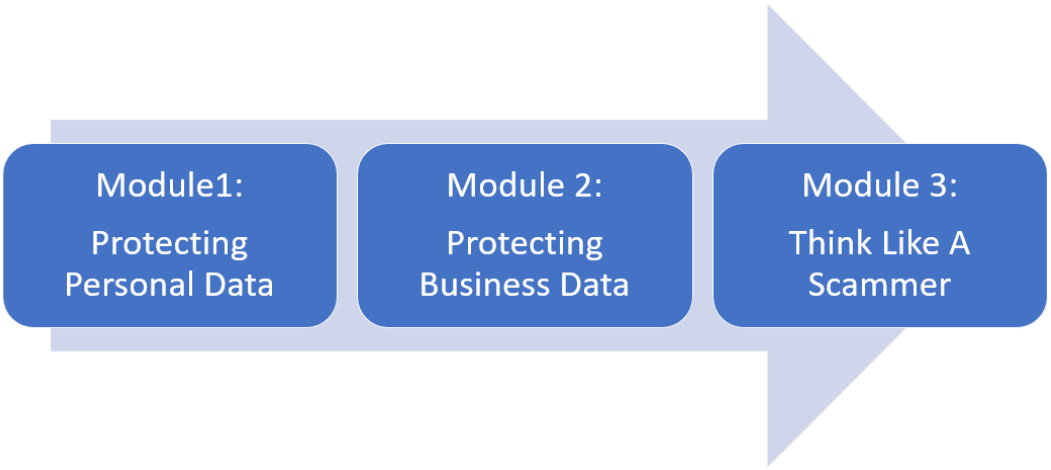
APCICT revamped the WIFI programme (now called WIFI DX) to equip women entrepreneurs with practical tools to navigate disruptions and harness the benefits of digital transformation effectively. With WIFI DX, new courses have been developed, encompassing e-commerce and digital marketing, digital financial literacy, data analytics, trust and security, and business continuity planning.

It is our hope that WIFI DX programme will serve as a valuable resource for women entrepreneurs in the region, so that their enterprises can thrive, become more productive, and sustainable.

**Kiyoung Ko**
**Director**
**APCICT/ESCAP**

## ABOUT THE COURSE

The course on Trust and Security will look into the fundamental key on how users can be safe online, it will touch on key information in protecting ones own data as well as business data. The key to being safe online is to have good habits when interacting online – the most basic of these activities is having a strong password and being very careful online. The course will also cover overall safety guidelines with the topic of Think Like A Scammer. The overview of the modules is shown below:




This course is designed to equip the participants with a deeper understanding on how to protect one's data and leverage the digital functions available to ensure a safe online experience. The scope and purpose of the course include:

1. Knowing how to keep personal data safe.
2. Knowledge on how to protect and secure a business in cyberspace.
3. Increase confidence in using ICTs and digital tools.
4. Understanding data protection.
5. Basic practices in keeping own data/password safe.

Participants will be introduced to various training delivery methodologies, including:

1. Microlearning modules
2. Hands on (online and offline)
3. Case studies (identify weak points and how to overcome)
4. Gamification (pop quiz)

This course is to be used with the training slides provided with this guideline.

## Course Target Audience

- Women entrepreneurs who are online and using online services such as social media, online banking etc.
- Women entrepreneurs who have started collecting customer data and keeping track of their own business growth online.
- Women who are interested in having greater security practices on their online profile.

## Course Learning Objectives

**Knowledge**

- Understanding the concept of security and personal data protection.
- Understanding how data is used and stored online.
- Learning about Personal Data Protection.

**Skills**

- Learn basic steps in keeping safe online.
- Identify useful methods to strengthen emails and social media accounts.

**Competency**

- Identifying weak points in our businesses when it goes online.
- Knowing how scammers think to avoid being a victim.

## Course Learning Outcomes

**By the end of this course, participants will:**

1. Learn how to protect their personal data, business data and customer data.
2. Understand that the greatest protection is having a strong password and using common sense.
3. Know how to avoid getting scammed and becoming a spam engine.
4. Be aware that the greatest data leak threat is from inside, need to have processes in place to protect the data.
5. Have a better understanding on having prcesses in place to protect your data.

## Acknowledgements

The Trust and Security Using Digital Technologies module was developed under the overall guidance of Kiyoung Ko, Director of the Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT/ESCAP).

The developed module was coordinated by Robert de Jesus. The module was written by Nuraizah Shamsul Baharin. The cover design and proofreading was done by Amal Kadir and Regina Ulibasa Patricia. Publication layout was provided by Ho-Din Ligay. Joo-Eun Chung and Van Anh Nguyen undertook adminsitrative processing necessary for the issuance of the module.

# Contents

# List of Figures

# MODULE 1: PROTECTING PERSONAL DATA

## Description

Module 1 will cover various areas women can stay safe while surfing the internet. These are the topics that will be covered in this module:

- How to stay safe going online.
- Best practices in creating passwords - what to do and what not to do.
- Know what to share and what to keep private on social media.
- Know what to do when on public Wi-Fi and private Wi-Fi.
- Identifying a pyramid and love scheme.
- How to protect your email from becoming a spam engine.
- How to protect your PC from viruses and hijack.
- Managing mobile app downloads which includes using mobile banking and mobile wallet.
- Safe practices when signing up to services on mobile apps.

## Objectives

The goal of this module is to provide the following objective:

- Understanding practices to keep yourself safe online.
- Gain the skills and online security knowledge to keep you ahead of the scammers.

## Learning Outcomes

The expected outcomes from this module:

- Increased understanding in password creation to create a strong password.
- Better understanding of spamming and viruses that can be sent via email.
- What not to do on public Wi-Fi.
- Protecting your email and social media with multi factor authentication and practicing safer interactions online.

- Awareness on how mobile apps can act as the tool that hackers use to get your data and passwords.

**Key messages**

**The module key message**

Protect yourself by protecting your personal data.

Having a strong password is the key step you can take in protecting yourself.

## Lesson 1: Staying safe online

### Lesson Introduction

This lesson will provide the participants a chance to learn how to identify what we can share online and how to create better passwords through group discussions.

### Activity/Something to do

- Trainer to conduct a facilitated open session discussing the question of how much should you share on social media? Get everyone's opinion on this.
- Direct the discussion to cover the basic steps on staying safe online.
- Have participants take this basic online quiz and find out how people scored.
    - Link to quiz: https://www.nist.gov/quiz/are-you-safe-online
    - Walk through the questions after participants are done.

## Content Discussion

When we talk about personal data safety, let's look at what we can do to increase personal safety when we interact online.

In today's world, it is impossible not to be online – whether we are working, shopping, looking for information and especially after the pandemic, for kids to use the internet for school. Altogether, the ASEAN member states have a population of around 630 million but 700 million digital consumers are in the region, which suggests that many individuals use multiple devices. Most Southeast Asian countries, including Vietnam, Indonesia, and the Philippines, show a mobile penetration rate of over 100 per cent (Southeast Asia digital, social and mobile 2019 - ASEAN UP, 2019).

Having the internet is a necessity now though the more accounts and devices that we have, the more opportunities we provide for people to target us.

Below is a list of just some of the biggest internet dangers we need to watch out for:

- Identity theft.
- Data breaches.
- Malware and viruses.
- Phishing and scam emails.
- Fake websites.
- Online scams.
- Romance scams.
- Inappropriate content.
- Cyberbullying.
- Faulty privacy settings.

To avoid all of these dangers, Kaspersky (2020) recommends following their essential internet safety tips when you or your family are online:

**1. Make sure you are using a secure internet connection**

Be extra careful when you are using public Wi-Fi. There could be people "listening in" and monitoring your online activity. Avoid doing personal transactions that use sensitive data, such as online banking or online shopping. Using a VPN (Virtual Private Network) will keep you safe but this is not something most people would have.

**2. Choose strong passwords**

Passwords are one of the easiest way to get hacked and bring the biggest weak spots when it comes to cybersecurity. We often choose passwords that are easy to remember which contains dates and names related to us. This makes it easier for hackers to crack using hacking soft-ware. When we use the same passwords and user names, once one password is compromised, hackers can access all accounts using the same login details.

Refer to the exercises in training slides on how to create strong passwords.

We can use a password manager to help store different passwords. Google also offers suggestions of strong passwords and the ability to remember them.

**3. Enable multi-factor authentication where you can**

Multifactor authentication (MFA) is an authentication method that asks users to provide two or more ways to authenticate that it is really the user accessing. Examples of additional information requested:

- An extra one-time password that the website's authentication servers send to the user's phone or email address.
- Answers to personal security questions.
- A fingerprint or other biometric information, such as voice or face recognition.

MFA is usually available for your emails and social media accounts. Turning this on will further protect your accounts from cyberattacks.

**4. Keep software and operating systems updated**

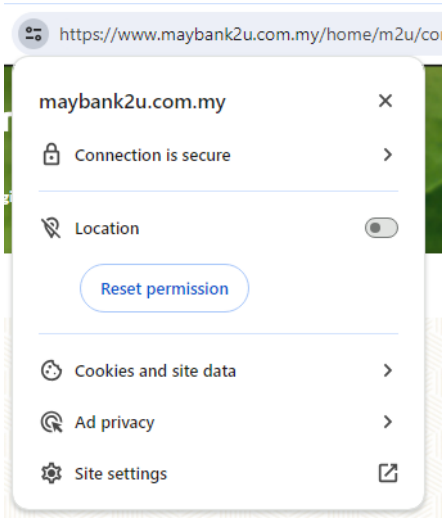
It is often time consuming to keep updating our softwares and operating systems. This is done by the provider to constantly keep ahead of the latest virus or threats that can access your personal and private information. Do install all the latest patches, especially the security patches. It is also important to update mobile apps constantly.

**5. Check that websites visited look and feel reliable**

Look out for webside that start with "HTTPS" instead of just "HTTP" (the "S" stands for "secure") and have a padlock icon in the address bar. Most browsers will only take you to sites that have these SSL/.security certificate. Do not conduct any financial transactions on sites that do not start with this HTTPS.

On training slides, refer to this display:

Figure 1. How to know a website is secure




Other trust signals include:

- Text which is free from spelling and grammar mistakes – reputable brands will make an effort to ensure their websites are well-written and proofread.
- Images that are not pixelated and fit the screen's width correctly.
- Ads that feel organic and are not too overpowering.

- No sudden changes in color or theme. In some cases, where users have interacted with a particular website and returned to a familiar page from a link, subtle color or design changes might indicate forgery.
- The accepted standards of online payments – legitimate e-commerce websites use credit or debit card portals or PayPal only. If a website is using another form of digital money transfer to accept payments, it is probably fraudulent.

**6. Review your privacy settings and understand privacy policies**

When you click on a website, it will ask you to allow "cookies" – this is how marketers know what you browse, how long you spend on a page, how you use your social media pages. Be careful how much you share. When you download a mobile app, it will ask if it can send notifications, choose "Don't allow". Nowadays it also ask if it can track your activity across other companies' apps and websites; definitely choose "Ask app not to track" for this.

Both web browsers and mobile operating systems have settings to protect your privacy online. Social media sites such as Facebook, Twitter, Instagram, LinkedIn, amongst others, have privacy-enhancing settings that you can activate. We are used to just accepting cookies and ticking the "I accept the privacy policy" without actually reading them. Take the time to review your privacy settings.

However, bear in mind that even if your settings are set to private, very little data online is totally private. Hackers, website administrators and law enforcement could still have access to the information you regard as private.

**7. Be careful of suspicious links and where you click**

We see quite a lot of clickbait news featuring popular artists being caught doing something wrong, or free offers, claim a gift or unsolicited ads – avoid clicking on this since it is usually a link that can expose your personal data or infect your devices with malware. Avoid opening unknown emails with attachment and even if the sender is known, please be careful about opening it. If there is no reason for an email to have a link or an attachment was sent that you didn't request, it could be a spam.

Refer to the training slides for examples on these.

**8. Make sure your devices are secure**

It is good practice to use password, passcodes or finger/face scans to protect your devices – phones, computers, tablets, smartwatches, smart TVs, etc.

**9. Backup data regularly**

It is important to backup important personal information on external hard drives and regularly create new backups. You should also backup your backup in case the hard drives fails. Ransomware – a type of malware – involves cybercriminals locking your computer so you can't access valuable files. Backing up your data helps mitigate the impact of a ransomware attack. You can protect yourself further with appropriate security software. Other forms of malware deny you access to your personal data by overwhelming your system or simply deleting files, so be careful.

**10. Close unused accounts**

How many accounts have we opened over the years and no longer use it but have not closed it? Do try to delete these accounts, as nowadays most applications will delete users after a period of inactivity. The old systems and applications would be easier to hack and details that you kept in your account can be accessed by hackers.

**11. Be careful what you download**

The top goal of cybercriminals is to trick you into downloading malware, which can be used to create a "backdoor" access to your machine. Malware might be disguised as an app – anything from a popular game to something that checks traffic or the weather. Or, it could be hidden on a malicious website that attempts to install malware on your device.

When downloading an app, always do it from an app store since it would have been reviewed by the store before it is uploaded. Always check the news to see what apps have been found to be collecting data or behaving suspiciously. The usual ways for hackers to get to you would be via a popular service like hiremaid or an app that makes you more beautiful. Be careful with these.

**12. Be careful what you post and where**

The internet does not have a delete key. Any comment or image you post online may stay online forever because removing the original won't remove any copies that other people may have made. There is no way for you to 'take back' a comment you wish you hadn't made or remove an embarrassing image you posted. So, do not put anything online that you would not want a parent or prospective employer to see.

Similarly, be careful about disclosing personal information about yourself online. For example, avoid disclosing your social security/identification number, address or date of birth in social media bios. You wouldn't share personal information out to strangers individually, so don't hand it out to millions of people online.

Be careful about where you display or submit your email address. It's good to have a secondary, throwaway email account that you use solely for email sign-ups and subscriptions, separate from the one you use for friends and family, and separate from the one you use for work.

**13. Be careful who you meet online**

People you meet online are not always who they claim to be. Indeed, they may not even be real. Fake social media profiles are a popular way for hackers to groom unwary internet users and pick their cyber pockets. Apply the same caution in your online social life as you would for your in-person social life.

**14. Double check online information**

In today's world, fake news, misinformation and disinformation are all present on the internet. It is easy to feel lost with the flood of information we are exposed to every day. If you read something you are unsure of, do your own research to establish the facts. Reliable websites will have references to the original information and source materials. Suspicious pages would not offer any references at all.

**15. Use a good antivirus and keep it updated**

As well as following safety tips for online behavior, it is essential to use a good quality antivirus provider. Internet security software guards your devices and data and blocks common threats like viruses and malware. As with all operating systems and apps, it is essential to keep your antivirus updated to stay ahead of the latest cyberthreats.

## Lesson 1 Summary

To be safe online, we need to be as careful and paranoid as possible. Always assumer that someone out there is trying to steal your data, and remember the safety tips in ensuring a safer online experience. Do not neglect the importance of having a strong password, it is like the key to opening the door and you want to make sure you have a strong lock

*****Notes to Trainers**

For this lesson, the main thought process is we are all responsible to protect ourselves online – when information is stolen, majority of the time is due to unsafe behavior online.

**Something to think about:**

- The more you share online, the easier it is for hackers to target you.

**Something to remember:**

- You can never be too careful - be as paranoid as possible.

## Lesson 2: Shopping online

### Lesson Introduction

Lesson 2 will touch more on how online consumers can ensure a safe online shopping experience when looking through the various websites and shopping apps available.

### Content Discussion

Online shopping has become the norm especially since the pandemic. With governments enforcing lockdowns, people had no choice but to learn how to shop online. This has been really helpful for the e-commerce industry but it also opens up ways for scammers to come in. The safest method to shopping online is using your credit card since they provide ways where you can dispute a payment made within 30 days.

### Activity/Something to do

Before we start this lesson, let's view a video on how to maximize online security when surfing the internet (On YouTube, you may search "5 EASY Tips to Maximize Online Security as You Surf the Internet" or type in this URL link: "https://www.youtube.com/watch?v=M--Yk6_f8MU")

Tip 1: Choose a great password.
Tip 2: Keep all software up to date.
Tip 3: Use a VPN when accessing public WiFi.
Tip 4: Check your social media privacy settings.
Tip 5: Monitor your bank accounts daily.
Tip 6: Use common sense.

Below are some of the recommended tips for a better and safer business transaction – based on this article by Safewise (URL: https://www.safewise.com/blog/10-cybersecurity-tips-for-online-shopping/)

**1. Use a credit card or payment service**

When shopping online, the safest choice is to use credit cards or payment services like Paypal. These choices offer better protection and you have time to report a suspicious transaction or refute a payment made where the credit card company will reverse the charge and block further transactions on your card if needed. If you use a debit card, the amount is deducted immediately and it will be a long and difficult process to get your money back. You are also exposing your bank account with a debit card payment.

**2. Shop secure sites only**

Based on Lesson 1, we have learnt how to verify a secure site – look for "HTTPS" in the address bar and also the padlock sign. If the site looks strange or feels suspicious, trust your instincts and do not proceed further.

**3. Update your software**

Updating your software is one of the easiest things you can do to protect your information, but many people simply ignored it. Software updates are often released to help improve security and fight new attacks that are being developed constantly. It may seem inconvenient to have to wait for your computer (or your smartphone) to go through updates and restart, but the protective benefits are well worth it. Next time you see an alert to update your software, do it. Do also use an antivirus or malware software.

**4. Beef up your passwords**

There's a reason this advice is repeated over and over again - the best way to keep your information safe is to have a strong password. Using the same password for many sites will put you at risk of being hacked. Remember to use password manager to keep track of different and more complicated passwords. Certain browsers like Chrome can also generate complex passwords and store it for you.

**5. Don't click on links**

Look out for unbelievable offers and holiday gifts and bonuses. If you're really tempted by an offer, do some research or find out if anyone else has tried to take advantage of the deal before clicking. Beware of links that offer things that are too good to be true.

**6. Secure your devices at all times**

When shopping online, make sure every device that you shop from has a passcode to access your tablet or smartphone, and log off your computer or lock the screen when you walk away from it. After accessing a shopping or banking site, be sure to completely log out of the site before exiting, you can also clear your cache. Remember, do not let your computer or device remember your usernames, passwords, or credit card information.

**7. Outsmart email scams**

Keep an eye out for email scammers that send out viruses and malware in the guise of a gift or special offer. Do not open emails from someone you don't know or a site you have not visited. Another way scammers try to get you is with phony messages from your bank or other financial institution saying there is an alert or problem with your account. Always call the bank directly to verify any potential problems and never enter your account information in response to an email like this.

Unfortunately, a lot of suspicious brands are popping up all over our favorite online shopping sites and social media. It can be hard to tell the fakes from the real deal. You can check this by:

- **Read customer reviews.** Look for too many super-positive reviews and repeated language or phrases.
- **Scrutinize photos.** See if you can find the origin of the photo. If it's a stock image, beware.
- **Get help.** You can use Fakespot (URL: www.fakespot.com) to check if the reviews are real.

**8. Never give more info than needed**

Most websites you visit or shop on will ask you for information to complete your purchase or start a wish list. Give them only the information they require you to provide. If a complete address or phone number is optional, then skip those fields. The more info you put out there, the more accessible you are to the bad guy. And before committing your information to a site, take the time to read their privacy policy and find out exactly where and how your information will be shared.

**9. Don't go public**

Free hotspots are convenient, but hackers like them even more than you do. Because public networks are not secured, any information you enter on a public network is a golden opportunity for hackers. Do not log in to banking sites or payment sites like Paypal on a public network — and make sure that you are logged out of such sites on mobile devices before connecting to a public network.

**10. Be smart about shopping apps**

Apps make everything more convenient, including stealing your private information. Only download shopping apps from a reliable source like the Apple App Store or Google Play. Pay attention to the permissions that the app asks for. If you see something that doesn't make sense, like access to your contacts, make sure you don't allow the app access to it. Checking out the comments and reviews of an app before downloading is another way to identify suspicious activity. Nowadays apps will ask if they can track you across all other apps and websites that you access on your phone. Do not allow access.

## Lesson 2 Summary

When you shop online, practice safe behavior. Check and verify the validity of the site before making a purchase. When you make a purchase online, be sure to use either a credit card or a payment service. Avoid giving more information than needed when signing up, do check the terms and conditions to find out how your data will be used.

**Something to think about:**

- Are you shopping at a legitimate site? Check and double check before you enter your payment details. Use a credit card, not debit card.

**Something to remember:**

- Any money lost via a fraudulent online transaction is very difficult to recover.

## Lesson 3: Create a good password

### Lesson Introduction

Lesson 3 will cover how online users can create a strong password that is secure and are less likely to be cracked by the hackers.

### Content Discussion

Passwords are one of the biggest weak spots when it comes to cybersecurity. People often choose passwords that are easy to remember and, therefore, easy for hackers to crack with hacking software. In addition to this, using the same password for multiple sites puts your data at further risk. If hackers obtain your passwords from one site, they can easily access other websites which use the same login details.

Select strong passwords that are harder for cybercriminals to crack. A strong password is:

- Long – made up of at least 12 characters (ideally more).
- A mix of characters – upper-case and lower-case letters plus symbols and numbers.
- Avoids the obvious – such as using sequential numbers ("1234") or personal information that someone who knows you might guess (or that might already be online), such as your date of birth or a pet's name.

Using a password manager can help. Password managers help users create strong passwords, store them in a digital vault (which is protected by a single master password) and retrieve them when logging into accounts online.

## Activity/Something to do

- Trainer to conduct the exercise below as a pop quiz for all the participants on what is the most common passwords used around the world and how many people use it– please refer to the training slides.

  The top 10 most common passwords worldwide are:

  1. "password," guessed in less than one second, used by nearly 5 million people
  2. "123456," less than one second, 1.5 million users have this password
  3. "123456789," less than one second, 413,000 users
  4. "guest," 10 seconds, 376,000 users
  5. "qwerty," less than one second, 309,000 users
  6. "12345678," less than one second, 284,000 users
  7. "111111," less than one second, 229,000 users
  8. "12345," less than one second, 188,000 users
  9. "col123456," 11 seconds, 140,000 users
  10. ""123123"" less than one second, 127,000 users

- The next exercise allows participant to create various styles of passwords, please refer to training slides 24 and 25.
    - The longer your password is, the better. Many websites ask you to create eight-character passwords, but we recommend going for at least 15 characters.
    - Avoid ties to your personal information, such as your name, surname, address, or date of birth.
    - Use a combination of numbers, symbols, and upper- and lowercase letters in random order.
    - Don't use sequential letters and numbers.
    - Avoid substitution: "kangaroo" and "k@ng@r00" are both equally weak passwords, and a brute-force attack can easily crack them.
    - Don't reuse the same password for multiple accounts.

Figure 2. Top ways to create a good password

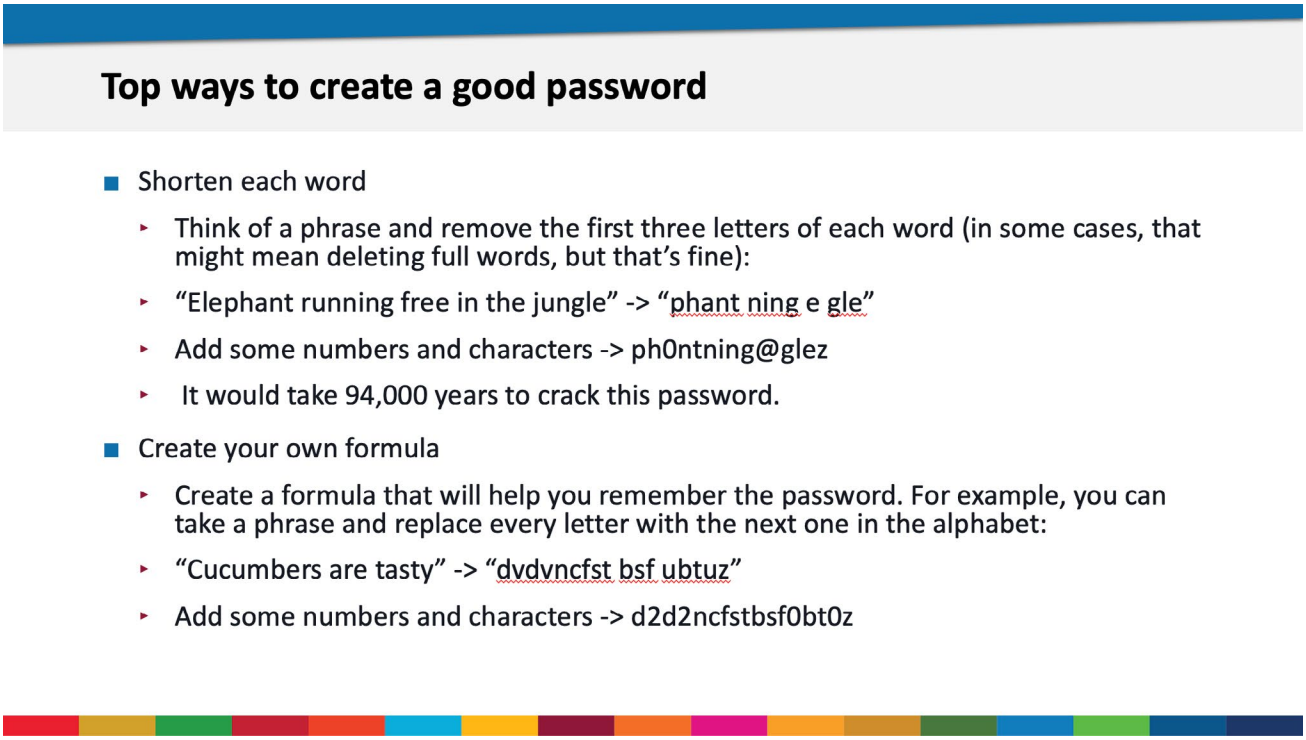
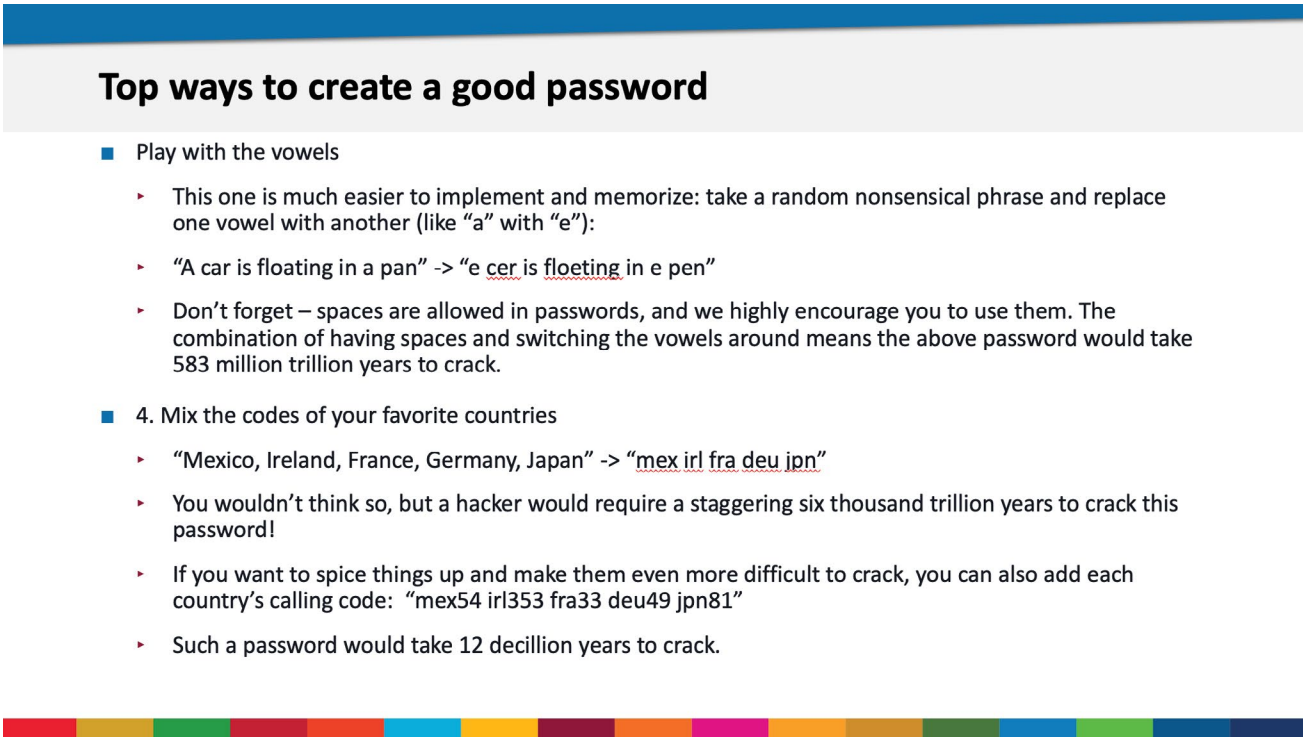


Figure 3. Top ways to create a good password (cont.)




The most important step that you can take to protect yourself is to have a good, strong password, think of it as your shield and the key to your personal data protection. Use a password manager to keep track of different passwords.

*****Notes to Trainers**

Run the password creation exercises with participants to help them understand better. This can be done as a group or individual activities.

**Something to think about:**

- Strengthening your password is like having a strong lock on the door to your home.

**Something to remember:**

- Using the same password everywhere will increase your chances of getting hacked.

# Lesson 4: Love me or love me not?

## Lesson Introduction

Romance scams happen when victims are deceived into 'false' relationships by fraudsters who aim to steal their money or personal information. Romance fraud is typically carried out by criminals using fake profiles. In this lesson, we will identify the signs that can point to whether your love interest is an actual person or is a scammer.

## Activity/Something to do

- Trainer can start by discussing what kind of love scams happens in the country to understand the local context
- Trainer can also identify the reasons why this happens

As you go through the content, you will also have some real life examples to share.

## Content Discussion

Women all around the world have become victims to these love scams, though some of them are highly educated, yet they fall to the trap made by these predators. They are very good at convincing women and winning their way into someone's trust. Anyone can become a victim. Most women are too ashamed to tell people what happened but this is needed to increase awareness on this scams and to stop others from becoming prey. Women just have to stay more vigilant and increase their paranoia.

## How to spot and avoid romance scams?

Scammers are very good at building trust and convincing their target about their legitimacy. They like to target women who are lonely and looking for love, they can see this from your social media interactions

and content you share online. These are several tips that can help you detect if you are interacting with a scammer. Equifax (n.d.) released an article on how an average user can spot a scammer according to these factors below. Some of the things to watch out for include the following:

- You meet on a dating app or website. They convince you to move to instant messaging or text and phone calls. Why? On dating websites, etc., they have implemented security to protect all parties.
- That person is asking so many personal questions and tells you "it is so I can know you better".
- When you ask to know more about the person, they often do not share much about themselves. Sometimes the questions are not normal. The details that they do tell you seem made up or don't reflect reality. For instance, they may say that they are university educated, but their spelling and grammar is poor.
- They are fast to establish a bond. For example, they may give you an endearing pet name or tell you that 'they've never felt like this before'.
- They always ask for financial help. It could be that they are sick or have a parent in need of money. They usually tell you about money problems and often, in the hope that you will offer to help.
- Check their social media pages and see if they have friends. Scammers create social media as proof that they are real. You can tell it is a fake when you:
    - Never meet them in person. They may promise to see you, but either cancel every time or offer excuses which delay meeting up, such as financial troubles.
    - Perform a reverse image search of their profile photo and it seems to belong to someone else.

## What are the signs you're being scammed?

Love scams can be devastating, and it's essential to recognize the signs to protect yourself. Here are some ways to spot a romance scam:

1. **Quick professions of love:** If someone claims to be deeply in love with you within a short period, be cautious. Scammers often use this tactic to manipulate emotions and gain trust.
2. **Suspicious language:** Pay attention to the language they use. Scammers employ flattering and validating words to connect with victims. Be wary if someone seems too good to be true.
3. **Avoidance of in-person meetings:** If your online admirer consistently avoids meeting in person or makes excuses, it's a red flag. Legitimate relationships involve face-to-face interactions.
4. **Financial requests:** The moment your online connection asks for financial aid, cease contact immediately. Scammers often create elaborate stories to solicit money from victims.

## How can we recognize a fake profile?

Recognizing fake profiles on social media platforms is crucial to protect yourself from scams and fraudulent activities. Here are some tell-tale signs to watch out for:

1. **Profile picture and photos:**
    - Reverse image search: Use tools like Google Reverse Image Search to check if the profile picture appears elsewhere online. Scammers often use stolen images.
    - Too good to be true: If the profile picture looks like a model or celebrity, be cautious. Scammers often use attractive photos to lure victims.
2. **Limited information:**
    - Sparse details: Fake profiles often lack substantial information. If the profile has minimal details, it might be suspicious.
    - Inconsistencies: Check for inconsistencies in the profile's bio, education, work history, and other personal information.

3. **Activity and posts:**
    - Recent activity: Look at the profile's activity. If it's inactive or has only recent posts, it could be a sign of a fake account.
    - Generic posts: Scammers often post generic content or share popular memes without personalization.
4. **Friend count and followers:**
    - Low friend count: If the profile has very few friends or followers, be cautious.
    - High friend count with no interaction: A large friend list with no interactions (likes, comments) could indicate a fake profile.
5. **Communication patterns:**
    - Too eager: Scammers may be overly eager to connect or express romantic interest.
    - Broken English or odd language: Poor grammar, unusual phrases, or language inconsistencies are red flags.
6. **Avoidance of in-person meetings:**
    - If the person consistently avoids meeting in person or makes excuses, be wary. Legitimate relationships involve face-to-face interactions.
7. **Financial requests:**
    - Immediate financial needs: If the person asks for money or financial assistance, cease contact immediately. Scammers create elaborate stories to solicit money.

**What are some real life cases?**

1. **Online swindle:**

   Emma met an aid worker named 'John' on a dating website. John claimed to be in Iraq. They spoke frequently, and John shared a heartbreaking story about losing his wife and brother to cancer—similar to Emma's own experience. After a while, John asked Emma to give him money so he can move to her country and meet her in person.

2. **Real-life romance scam:**

   A woman in her 50s was duped out of US$100,000 dollars by a man she met on social media. Despite never meeting in person, the scammer manipulated her emotions, leading her to believe in a future together. The victim fell prey to false promises and financial requests.

3. **Military romance scam:**

   A businessman lost more than US$50,000 dollars due to an online love scam involving his 14-year-old son. The son befriended a girl online who persuaded him to lend her money. The scammer exploited their trust and emotions.

4. **Catfishing and love bombing:**

   Scammers create too-good-to-be-true personas, express intense emotions, and manipulate victims into providing financial assistance. These scams often occur on dating apps and social media platforms.

Remember to stay vigilant, ask questions, and be cautious when interacting with online acquaintances. If something feels off, trust your instincts and protect yourself from potential love scams.

## How to protect yourself from being scammed

Here are some things which may help you avoid being scammed:

- **Do not share personal details**
  If you share personal information like your full name, date of birth

and home address with a stranger, you may not know what they will do with it. Try not to share personal details online with people whom you already know, either – you may end up sending it to a fraudster pretending to be them. You should also be careful when picking your user name on dating websites – don't include personal information like your location (for example, 'JaneFromLondon').

- **Do not send or receive money**
  Do not send or receive money from anyone you've met online, no matter how convincing their story is. This applies to cash as well as your bank account,credit card or other financial details. If the request is coming from someone you think you know, check with them offline to ensure that it's really them.

- **Use trusted dating websites**
  Fraudsters tend to want to take their criminal activity off reputable dating websites as soon as possible. They are likely to try to convince you to interact with them via social media or text messaging. This is so that the dating website has no proof of them asking you for money. If you're in touch with someone on this type of website, communicate with them through the site's messaging services.

- **Do not share personal contact details**
  Use a website that will allow you to keep your personal details private until you're ready to share them. These include your contact details, such as your phone number or email or home address.

- **Think twice before using your webcam**
  Be careful when using your webcam with a new online love interest, even if it's someone whom you think you know. The footage could be used against you. This applies to cameras on all devices, from computers and laptops to smartphones and tablets.

- **Trust your instincts**
  If you feel like something is wrong, it may be. Be careful.

## Lesson 4 Summary

When meeting people online, it is very difficult to know if they are genuine. They work on building your trust and then If they start asking you for money, assume the worst. Anyone can be a target, and these people are professionals and know how to get you to trust them. Always be wary and strict with sharing your personal and financial information.

***Notes to Trainers**
You can read more here: How to spot and avoid romance scams | Equifax UK (https://www.equifax.co.uk/resources/identity-protection/how-to-spot-and-avoid-romance-scams.html)

**Something to think about:**

- When a new person you meet asks you for money, stop and review upon your relationship. Is it real?

**Something to remember:**

- Love is not measured by how much money you give, so beware of love promises in exchange of money.

## Summary of Module 1

In Module 1, we looked at the following topics at ways where we can protect our personal data online.

- We started with the basics on how we interact and keep safe online which was covered.
- We covered the basics of staying protected when we shop online.
- We covered the actual steps that can be taken to create a good password with examples on how this can be done.
- We also looked at how to protect ourselves as women are more susceptible to the romance scams.

# MODULE 2: PROTECTING BUSINESS DATA

## Description

Module 2 will cover how participants can protect their business data. These are the topics that will be covered in this module:

- Understanding infrastructure limitations and advantages – where is your data stored when it is online?
- How we collect data and what type of information should be protected?
- How to keep our customer data safe.
- How to collect online payments safely.

## Objectives

The goal of this module is to provide the following objective:

- Understanding basic skills and increase awareness and knowledge.
- Gain the ability to audit your own business and have an idea how to improve your security level.

## Learning Outcomes

The expected outcomes from this module:

- Knowledge on how to protect other people's data.
- Ability to identify best practices in collecting customer data.
- Practice standard operating processes for employees.

## Key Messages

**The module key message**

Deliver customer satisfaction and increase your customer retention by having a proactive and robust policies and processes that protect your customer data, including their payment details,

# Lesson 1: What is cyber security?

## Lesson Introduction

When we look at the topic of business data, let's start with our understanding of what is the definition of cyber security and data privacy. Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

Why is cybersecurity important? We can lose important data like when a hacker holds our online content at ransom or takes over our social media. As organizations, a cyber attack for a bank exposes their customer to great loss of privacy, money and personal information.

## Activity/Something to do

- Trainer can show a video on cybersecurity, for example this video by Kaspersky - (On YouTube, you may search "What is Cyber Security? How You Can Protect Yourself from Cyber Attacks" or type in this URL link: "https://www.youtube.com/watch?v=88-FENio9Yw ")

## Content Discussion

Cybersecurity encompasses various contexts, including business operations, mobile computing, and disaster recovery. Here are some key aspects of cybersecurity as identified by Kaspersky (2019):

1. **Network security:** This involves securing computer networks from intruders, whether they are targeted attackers or opportunistic malware.
2. **Application security:** Focuses on keeping software and devices free of threats. A compromised application could provide unauthorized access to sensitive data. Successful security begins during the design stage, well before deployment.
3. **Information security:** Protects the integrity and privacy of data, both in storage and during transmission.
4. **Operational security:** Encompasses processes and decisions related to handling and safeguarding data assets. It includes user permissions, data storage practices, and sharing protocols.
5. **Disaster recovery and business continuity:** These define an organization's response to cyber-security incidents or other events that disrupt operations or cause data loss. Disaster recovery policies guide how an organization restores operations, while business continuity plans help maintain functionality during resource shortages.
6. **End-user education:** Addresses the unpredictable human factor. Educating users about security practices—such as avoiding suspicious email attachments and not plugging in unidentified USB drives—is vital for overall organizational security.

The global cyber threat continues to evolve rapidly, with a rising number of data breaches each year. In the first nine months of 2019 alone, a staggering 7.9 billion records were exposed by data breaches, more than double the number from the same period in 2018. Sectors such as medical services, retailers, and public entities are particularly vulnerable. As the cyber threat escalates, global spending on cybersecurity solutions is projected to reach USD188.3 billion in 2023 and surpass USD260 billion globally by 2026 (Kaspersky, 2019).

The following are threats that happens online:

- **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.
- **Cyber-attack** often involves politically motivated information gathering.
- **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

## Data privacy

Data privacy covers how and what data should be collected, stored, managed and share within the organization and any third parties. This also includes compliance with applicable laws. Most countries have a personal data protection act or law which governs the ethics and legal usage of personal data collected.

What needs to be covered for data privacy?

- Inform customers on what data is collected, disclose how it is stored, how long will be stored and under what circumstances that the data will be share.
- If you provide an online shopping service, you would need the customer to open an account and provide information like name, email address, contact number and shipping address.
- All online and e-commerce stores are legally required to have a data privacy policy in most countries. Make sure you have this for your business.
- Do also include a way for customers to interact with you so that they feel supported should any issues occur.

Let's delve into the personal data protection laws in the ASEAN region, the United States, and the European Union.

1. **ASEAN Region**
    - Over the past two years, there have been significant developments in personal data protection laws within the ASEAN region (Kumar et al., n.d.).
    - Thailand introduced the Personal Data Protection Act (Thai PDPA) in May 2019. This law largely aligns with the European Union's General Data Protection Regulation (GDPR). Key provisions include:
        - Appointing a data protection officer.
        - Notifying in case of a data breach.
        - Adhering to principles such as purpose limitation, lawfulness, fairness, and data minimization.
        - The Thai PDPA has an extraterritorial effect, potentially impacting data controllers and processors outside Thailand.
        - Violations may result in administrative fines (up to THB 5 million) and criminal penalties
    - Vietnam has consolidated its personal data protection regulations into a single piece of legislation called the Draft Decree on Personal Data Protection. This move aims to enhance data protection within the country.
    - In Malaysia, the Personal Data Protection Act 2010 (PDPA) regulates the processing of personal data in commercial transactions and applies to anyone who processes personal data in the context of commercial activities.

2. **United States:**
    - The United States does not have a comprehensive federal data protection law like the GDPR.
    - Instead, it relies on sector-specific laws such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data and the Gramm-Leach-Bliley Act (GLBA) for financial data.

- Additionally, some states have enacted their own data protection laws, such as the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (VCDPA).
- These state laws focus on consumer rights, data breach notifications, and opt-out mechanisms.

3. **European Union (EU):**
   - The General Data Protection Regulation (GDPR) is the gold standard for data protection laws globally.
   - Key features of the GDPR include:
     - Consent: Organizations must obtain clear and informed consent from individuals for data processing.
     - Rights of data subjects: Individuals have rights regarding access, rectification, erasure, and portability of their personal data.
     - Data Protection Officer (DPO): Some organizations are required to appoint a DPO.
     - Breach Notification: Organizations must report data breaches to authorities within 72 hours.
     - Fines: Violations can result in substantial fines (up to EUR 20 million euros or 4 per cent of global annual turnover).
   - The GDPR has influenced data protection laws worldwide, including those in the ASEAN region.

In summary, while the ASEAN countries are making strides toward aligning their laws with the GDPR, the United States relies on a patchwork of sector-specific and state-level regulations. The EU's GDPR remains the benchmark for robust data protection practices

## Lesson 1 Summary

This first lesson covers the concept of cyber security and data privacy as well as the laws that protect them. We also look at how these laws differ based on countries and regions.

**Something to think about:**

- Cyber security practices keep your business operations business data safe.

**Something to remember:**

- Most countries have data privacy policies, do read and implement to avoic getting into legal issues.

## Lesson 2: Where does data exist online?

### Lesson introduction

Where do we share data?

Data is commonly gathered via:

- Social media
- Google forms
- Website & Database
- Online banking
- E-commerce websites
- Mobile Apps (WhatsApp, FoodPanda, Uber etc.)
- Subscription Services (Netflix, News, Udemy, Coursera etc.)

## Activity/Something to do

- Trainers to get participants' understanding what data they give online and what data they collect on their customers.

## Content Discussion

Most data is stored here:

- Most data resides in traditional data servers and cloud data centers.
- There are approximately 600 hyperscale data centers worldwide, with over 5,000 servers each.
- 39 per cent of the data centers are in the US; 30 per cent in China, Japan, UK, Germany and Australia.
- In 2019, online users generated 500 million tweets, 294 billion emails, 4 million gigabytes of Facebook posts, 65 billion WhatsApp messages and 720,000 hours of new content added daily on YouTube.

# Lesson 3: What type of information should be protected?

## Activity/Something to do

- Trainers to get participants' understanding on what data they give online and what data they collect on their customers.
- From the slides, trainer shall engage with participants and get participants to decide if these are private or public data.
- Then ask the participants to work in a group to answers these 3 questions:
    - What kind of data are usually collected by e-commerce sites?
    - What kind of data can be shared?
    - What kind of data should be kept private?

Figure 4. Examples of information shown by hotel, food, and beverage companies

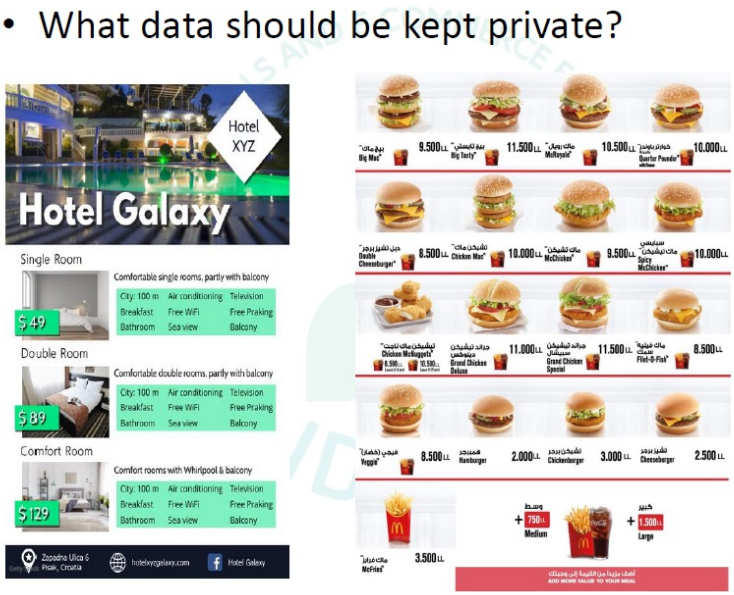
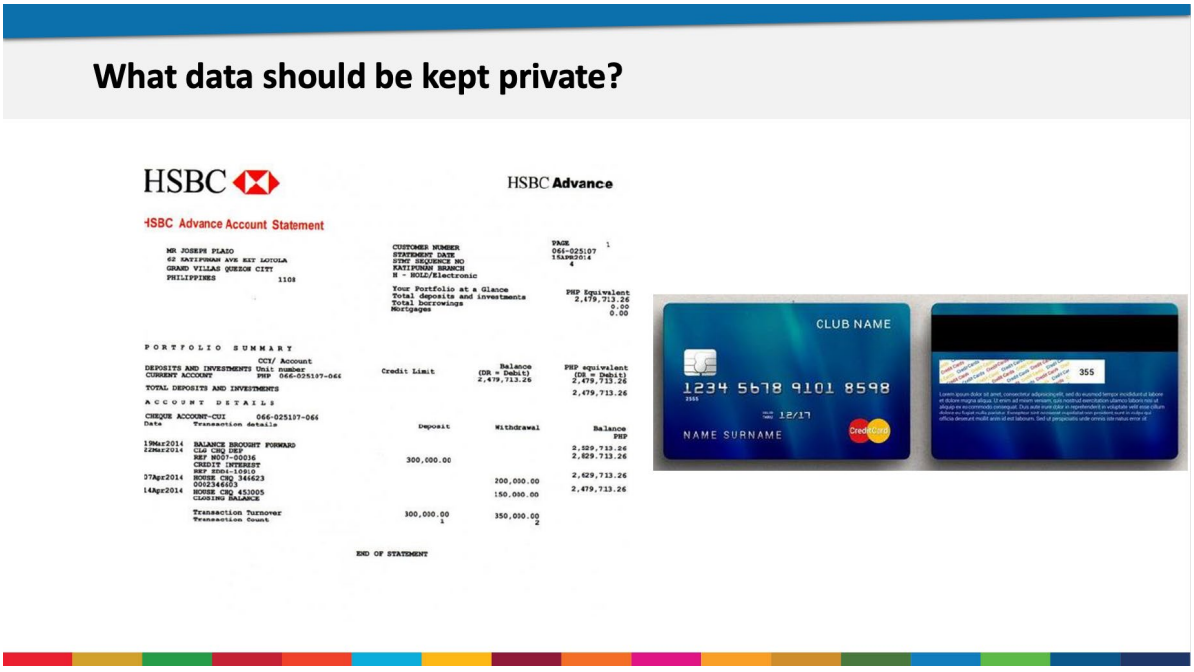



Figure 5. Examples of information shown by bank and credit card companies



## Lesson Introduction

## What kind of customer information must be secured?

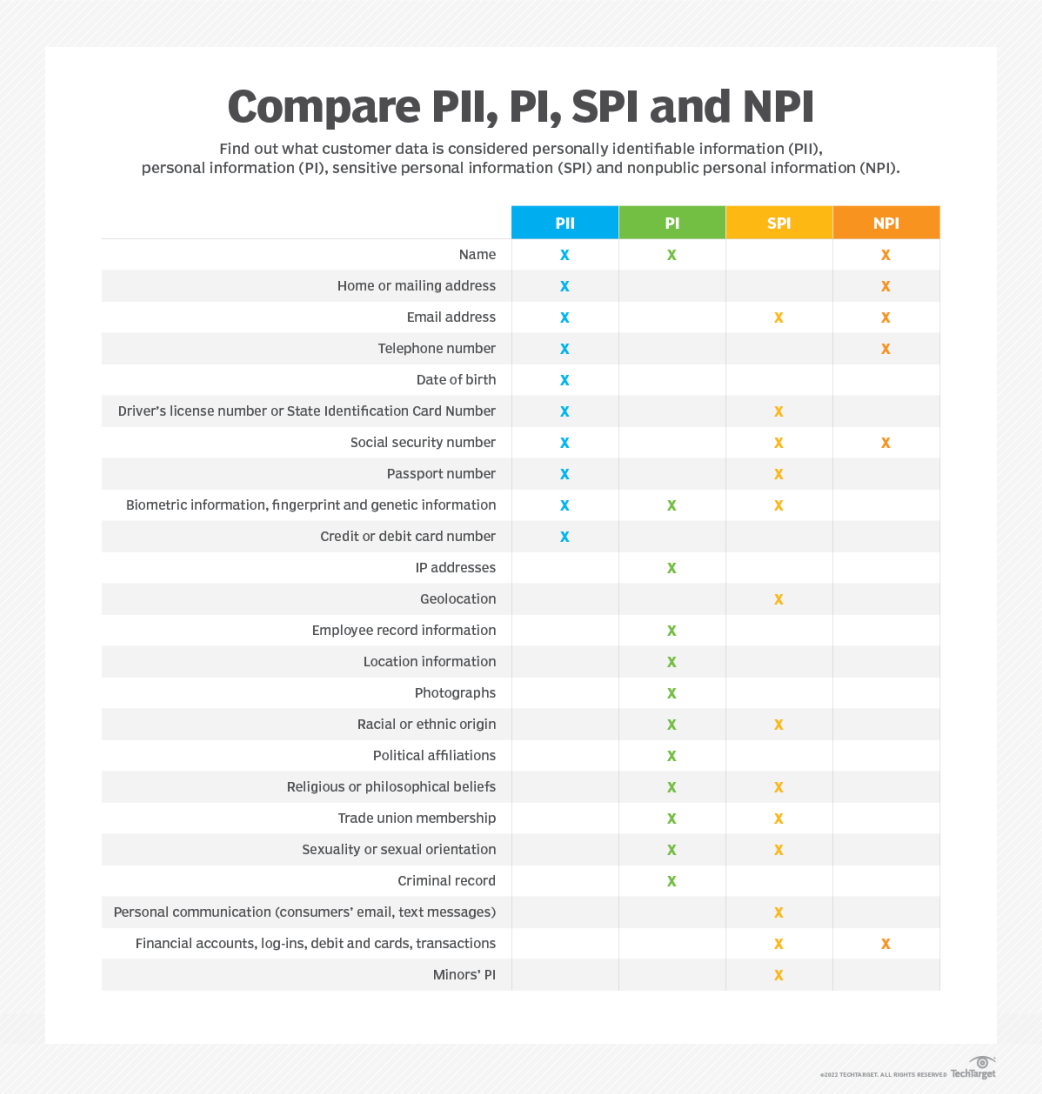
There are 4 different classification that companies collect which should be added into your organization's data security policy (Mathis, 2022).

- **Personally identifiable information (PII).** PII refers to information that can distinguish or trace a person's identity by itself or with other personal or identifying information linked to that individual.
- **Personal information (PI).** PI can directly or indirectly identify, relate to or describe a person or household. PI is relatively broad and can include data associated with someone's identity, often overlapping with PII.
- **Sensitive personal information (SPI).** SPI covers personal data that does not directly identify an individual but may cause harm if made public. It also protects minors and their PI.
- **Nonpublic personal information (NPI).** NPI specifically regulates financial services institutions and includes information they obtain directly from customers or through transactions. NPI does not include publicly available information.

## Why must we keep sensitive data private?

- Privacy protection
- Prevention from identity theft
- Financial security
- Business reputation
- Compliance with regulations
- Competitive advantage
- Personal safety
- Preserving trust in digital services

## Figure 6. Comparison of PII, PI, SPI and NPI



### Compare PII, PI, SPI and NPI

Find out what customer data is considered personally identifiable information (PII), personal information (PI), sensitive personal information (SPI) and nonpublic personal information (NPI).

| | PII | PI | SPI | NPI |
|---|---|---|---|---|
| Name | X | X | | X |
| Home or mailing address | X | | | X |
| Email address | X | | X | X |
| Telephone number | X | | | X |
| Date of birth | X | | | |
| Driver's license number or State Identification Card Number | X | | X | |
| Social security number | X | | X | X |
| Passport number | X | | X | |
| Biometric information, fingerprint and genetic information | X | X | X | |
| Credit or debit card number | X | | | |
| IP addresses | | X | | |
| Geolocation | | | X | |
| Employee record information | | X | | |
| Location information | | X | | |
| Photographs | | X | | |
| Racial or ethnic origin | | X | X | |
| Political affiliations | | X | | |
| Religious or philosophical beliefs | | X | X | |
| Trade union membership | | X | X | |
| Sexuality or sexual orientation | | X | X | |
| Criminal record | | X | | |
| Personal communication (consumers' email, text messages) | | | X | |
| Financial accounts, log-ins, debit and cards, transactions | | | X | X |
| Minors' PI | | | X | |



## Lesson 3 Summary

When we talk about personal data protection, it refers to all data collected by the organization and it is the organization's responsibility to keep that data safe. There are laws in most countries that govern personal data protection so do find out more about what laws are present in your country.

*****Notes to Trainers**

Use the activities slides to engage with participants.

**Something to think about:**

- When you collect data about your customer, it is your responsibility to keep that data safe.

**Something to remember:**

- Retain your customers by taking all steps to protect their data. Trust is hard to gain but easy to lose.

## Lesson 4: How can data be protected?

### Lesson Introduction

Gathering customer data is important for companies to be able to provide better targeted service to your customers but keeping their data safe is paramount in building trust between your business and your customers. To do this, companies must take the precautions necessary from technology perspective as well as processes in operations and data protection.

### Activity/Something to do

- Trainer can start by asking participants on a major data breach that has happened in your country.
- Cover the top 10 biggest data breach in the world in the last decade (as can be gathered in from this link https://tech.co/news/10-biggest-data-breaches).

  Here are the top ten biggest data breaches ever, and how many records were leaked in the process:

  1. Yahoo (2013) – 3 billion
  2. First American Corporation (2019) – 885 million
  3. Facebook (2019) – 540 million

4. Marriott International (2018) – 500 million
5. Yahoo (2014) – 500 million
6. Friend Finder Network (2016) – 412 million
7. Exactis (2018) – 340 million
8. Airtel (2019) – 320 million
9. Truecaller (2019) – 299 million
10. MongoDB (2019) – 275 million

## Content Discussion

Here are some general guidelines in protecting customer data, organizations can take the following steps:

- Collect only data that is important to doing business with customers, avoid storing data that is highly sensitive.
- Limit who in your organisation can access customer data, leaks more often happen from inside the organization. Set up internal safety measures to safeguard the data. Do not share passwords in accessing data. Boost cybersecurity and control access through password management tools, anyone who acess the data should have own passwords.
- Implement a data management strategy, look at encryption for your data and files that you keep and store the data in a centralized location, avoid storing the data in multiple sites.
- Set minimum security standards with which the organization complies. For example, any tool must comply with ISO 27001 (Information Security).
- Display your data privacy policy on your website and make it visible upon customers signing up or sharing any data.
- Integrate antivirus and malware protection where you store your data.
- Consider higher protection using blockchain if you have mission critical data.
- Setup a two factor authentication method for accounts that your customer sets up.

## Lesson 4 Summary

In this lesson, we learnt what are the guidelines in keeping data protected and looked at the organizations that had the biggest data breach in the last 10 years.

**Something to think about:**

- When you collect data about your customer, take measures to keep that data safe and invest in technology.

**Something to remember:**

- The bigger you are as an organization, the more attractive you become to hackers.

## Lesson 5: How can online transactions be protected?

### Lesson Introduction

Having a way to collect payment is essential for any online business, but they also pose significant risks for your customers' financial data and privacy. If you fail to protect their sensitive information, you could face legal, financial, and reputational consequences. In this lesson, you will learn some of the best practices and tips to secure your payment systems and ensure your customers' trust and loyalty.

### Activity/Something to do

- Trainer can start by recapping what we have learnt so far on data collected for e-commerce and online payments.
- Find out if anyone has experienced a fraud case, suspicious transactions or any other failures.

## Content Discussion

LinkedIn (n.d.) experts have provided a recommendation on how to protect your customers' data and privacy when using the Payment Systems. Below are the points:

**1. Choose a reliable payment provider**

The first step to protect your customers' data and privacy is to choose a reputable and trustworthy payment provider. You should look for a provider that complies with the Payment Card Industry Data Security Standard (PCI DSS), which is a set of guidelines and requirements for handling cardholder data. You should also check the provider's security features, such as encryption, tokenization, fraud prevention, and authentication. Additionally, you should review the provider's privacy policy and terms of service, and make sure they respect your customers' rights and preferences.

**2. Use HTTPS and SSL certificates**

The second step to protect your customers' data and privacy is to use HTTPS and SSL certificates on your website. HTTPS is a protocol that encrypts the communication between your website and your customers' browsers, preventing anyone from intercepting or tampering with the data. SSL certificates are digital certificates that verify the identity and authenticity of your website, and show a padlock icon and a green address bar in the browser. These elements help your customers feel more confident and secure when entering their payment details on your website.

**3. Collect only necessary data**

The third step to protect your customers' data and privacy is to collect only the data that you need for processing the payment and delivering the service or product. You should avoid asking for irrelevant or excessive information, such as social security numbers, birth dates, or personal preferences, unless you have a valid and transparent reason. You should also inform your customers about the purpose and duration of the data

collection, and obtain their consent before using or sharing their data with third parties.

**4. Store and dispose data securely**

The fourth step to protect your customers' data and privacy is to store and dispose of their data securely. You should use encryption, password protection, and access control to prevent unauthorized access, modification, or disclosure of the data. You should also backup the data regularly, and use a secure cloud service or a dedicated server. Furthermore, you should delete or anonymize the data when it is no longer needed, and follow the applicable laws and regulations regarding data retention and disposal.

**5. Monitor and update your payment systems**

The fifth step to protect your customers' data and privacy is to monitor and update your payment systems regularly. You should track and audit the transactions, activities, and events that occur on your payment systems, and look for any signs of suspicious or fraudulent behavior. You should also update your payment systems with the latest security patches, fixes, and features, and test them for any vulnerabilities or errors. Additionally, you should train your staff and educate your customers on how to use your payment systems safely and responsibly.

**6. Respond to data breaches and incidents**

The sixth step to protect your customers' data and privacy is to respond to any data breaches or incidents that may affect your payment systems. You should have a clear and comprehensive plan to deal with such situations, and follow the best practices and standards for incident response. You should also notify your customers, payment provider, and relevant authorities as soon as possible, and provide them with the necessary information and support. Moreover, you should investigate the cause and impact of the breach or incident, and take corrective and preventive measures to avoid recurrence.

## Lesson 5 Summary

Using payment companies that have applied PCI DSS would be very more secure for the business to work with that vendor. As a consumer, it is better not to save any card data on browsers or websites that suggest keeping the data for the next transactions.

**Something to think about:**

- Out of all the data that you can keep, the most critical one is data relating to someone's bank details. Use a trusted payment provider to manage collections instead of doing it yourself.

**Something to remember:**

- Safety first.

## Summary of Module 2

In Module 2, we looked at the following topics for the management of business data:

- Cyber security –This covers the definition and threats that requires cyber security; plus data privacy and Personal Data Protection Acts in various countries.
- Understand where data is collected and where they exist online.
- Understand the types of information collected and which data should be kept private and which can be shared publicly.
- Understand how data can be protected.
- Understand how online transactions can be protected.

# MODULE 3: THINK LIKE A SCAMMER

**Description**

Our last module will allow participants to explore the mind of a scammer and reflect on the various types of scam available to prevent further incidences. This lesson will provide the participants a chance to learn how to identify the various methods scammers use to trick users and what are the safety tips when you are targeted through group discussions.

These are the topics that will be covered in this module:

- Learn how scammers think and act.
- Identify a pyramid scheme and a love scheme.
- Protecting social media accounts from being hijacked.
- How to stop your email from being a scam engine.
- How data is lost through disgruntled employees.
- How scammers target our children.

**Objectives**

The goal of this module is to provide the following objective:

- Increase awareness to activate self- protection behavior.
- Be aware of scammers and how they convince to believe them.

**Learning Outcomes**

The expected outcomes from this module:

- Strengthen your website, email and social media accounts.

**Key messages**

**The module key message**

Always think it is a scam

# Lesson 1: Identifying a scam

## Lesson Introduction

Scams can come in many forms, but all are designed to get hold of your money. They do this by getting you to reveal your personal details, stealing your information, or even tricking you into willingly handing over the cash. It is important to know how to recognise a scam so you can protect yourself from fraudsters. This lesson will also cover what to do if you think you've been targeted or have fallen victim.

Chances are, you've come across the most common type of scams. Here are the top 3 types of scams that we will look at:

- Spam emails saying you're about to come into some money from a government agency or your bank.
- Texts claiming payment is required for a package to be delivered.
- The WhatsApp 'mum and dad' scam, when scammers using WhatsApp pose as family members in order to manipulate victims into transferring money.

## Activity/Something to do

- Trainer can start by discussing what kinds of scams that participans have seen or gotten in trouble with.
- We will be listing the Top 10 scams; ask the participants which ones they have experienced.

## Content Discussion

Knowing what to look out for when it comes to scams is one of the best ways to protect yourself. Below are some of the characteristics you can

identify to rule out if the information is a scam or not. For the full article, please go to (https://www.moneyhelper.org.uk/en/money-troubles/scams/a-beginners-guide-to-scams )

- Unsolicited or unexpected contact - If you received any kind of contact, particularly a phone call out of the blue, it is best to avoid it.
- Email address - If you get an email, expand the pane at the top of the message and see exactly who it has come from. If it is a scam, the email address the message come from might not match up with the sender's name, have misspellings, random numbers or be from one of your contacts that's been hacked.
- Text messages – Modern scammers can make their numbers look like ones you trust, like your bank's. The scam text message might even appear in the same conversation as legitimate texts you've had before. This is known as 'number spoofing'. Just in case, don't click links in text messages, and if in doubt, contact the company directly using contact details from their website or correspondence to check whether it's a real message.
- If it sounds too good to be true, it usually is. This is something you normally find with pension or investment scams, where the fraudster guarantees you huge returns, but tells you it is low risk.
- Request for personal details, full PIN codes and passwords. These are things no legitimate company will ask you for.
- Quick decisions. If you are pushed into making a decision on the spot, be suspicious. Scammers don't want you to have time to think about it. Any legitimate company who calls you won't mind if you hang up and call them back later. Use the phone number you find on letters from the company or the back of your card.
- Random competitions, particularly if you don't remember entering them, should ring alarm bells.
- Spelling errors or poor grammar on emails and in texts are other signs of a scam.

## The Northern Territory Government of Australia (2015) identified the ten most common types of scams as below:

| No. | Type of scam | Description |
|---|---|---|
| 1 | Advance fee fraud | A scammer requests fees up front or personal information in return for goods, services, money or rewards that they never supply.<br><br>Scammers invent convincing and seemingly genuine reasons for requesting payment, such as to cover fees or taxes. They often ask for payment by international wire transfer. These are usually sent by mail or email. |
| 2 | Lottery, sweepstakes and competition scams | An email, letter or text message from an overseas lottery or sweepstakes company arrives from out of nowhere. It says you have won a lot of money or fantastic prizes in a lottery or sweepstakes competition you did not enter.<br><br>These scams try to trick you into giving money upfront or your personal details in order to receive the prize. They will say fees or taxes before your winnings or prize can be released.<br><br>Remember, you cannot win a prize if you haven't entered. |
| 3 | Dating and romance scams | Scammers create fake profiles on legitimate dating websites.<br><br>They use these profiles to try to enter into a relationship with you so they can get a hold of your money and personal details.<br><br>The scammer will develop a strong rapport with you then ask for money to help cover costs associated with illness, injury, travel or a family crisis.<br><br>Scammers seek to exploit your emotions by pulling on your heart strings. Sometimes the scammers will take months and months to build up the rapport. |

| | | |
|---|---|---|
| 4 | Computer hacking | Phishing emails are commonly used by scammers to trick you into giving them access to your computer.<br><br>They 'fish' for your personal details by encouraging you to click on a link or attachment.<br>If you click, malicious software will be installed and the hacker will have access to files and information stored on your computer.<br><br>A phishing email often appears to come from an organisation that you know and trust, like a bank or financial institution, asking you to enter your account password on a fake copy of the site's login page.<br><br>If you provide your account details, the scammer can hack into your account and take control of your profile. |
| 5 | Online shopping, classified and auction scams | Scammers like shopping online for victims. Not getting what you paid for is a common scam targeting online shoppers.<br><br>A scammer will sell a product and send a faulty or inferior quality item, or nothing at all. They may also pretend to sell a product just to gather your credit card or bank account details.<br><br>These scams can also be found on reputable online classified pages.<br><br>An online auction scam involves a scammer claiming that you have a second chance to buy an item that you placed a bid on because the winner has pulled out.<br><br>The scammer will ask you to pay outside of the auction site's secure payment facility.<br><br>If you do, your money will be lost and the auction site will not be able to help you. |

| | | |
|---|---|---|
| 6 | Banking, credit card and online account scams | Scammers send emails or text messages that appear to be from your bank, a financial institution or an online payment service.<br><br>They usually claim that there is a problem with your account and request that you verify your details on a fake but convincing copy of the bank's website.<br><br>Card skimming is the copying of information from the magnetic strip of a credit card or automatic teller machine (ATM) card.<br><br>Scammers skim your card by putting a discreet attachment on an ATM or EFTPOS machine. They may even install a camera to capture your pin.<br><br>Once your card is skimmed, scammers can create copies and make charges to your account. |
| 7 | Small business scams | If you own a small business you can be targeted by scams such as the issuing of fake bills for unwanted or unauthorised listings, advertisements, products or services.<br><br>A well-known example is where you receive a bill for a listing in a supposedly well-known business directory.<br><br>Scammers trick you to sign up by disguising the offer as an outstanding invoice or a free entry, but with a hidden subscription agreement in the fine print.<br><br>Scammers can also call your business pretending that a service or product has already been ordered and ask for payment over the phone. |
| 8 | Job and employment scams | These scams involve offers to work from home or set up and invest in a business opportunity. Scammers promise a job, high salary or large investment return following initial upfront payments.<br><br>These payments may be for a business plan, training course, software, uniforms, security clearance, taxes or fees.<br><br>These scams are often promoted through spam email or advertisements in well-known classifieds, including websites. |

| | | |
|---|---|---|
| 9 | Golden opportunity and gambling scams | Scams often begin with an unexpected phone call or email from a scammer offering a not-to-be-missed high return or guaranteed investment in shares, real estate, options or foreign currency trading.<br><br>While it may seem convincing, in reality the scammer will take your money and you will never receive the promised returns.<br><br>Another scam promises to accurately predict the results of horse races, sports events, stock market movements or lotteries.<br><br>Scammers promise you huge returns based on past results and trends. In order to participate, you may be asked to pay for membership fees, special calculators, newsletter subscriptions or computer software programs. |
| 10 | Charity and medical scams | Scammers are unscrupulous and take advantage of people who want to donate to a good cause or find an answer to a health problem.<br><br>Charity scams involve scammers collecting money by pretending to work for a legitimate cause or charity, or a fictitious one they have created.<br><br>Often scammers will exploit a recent natural disaster or crisis that has been in the news.<br><br>They may also play on your emotions by claiming to collect for a cause that will secure your sympathy, for example to help sick children.<br><br>Medical scams offer a range of products and services that can appear to be legitimate alternative medicines, usually promising quick and effective remedies for serious medical conditions.<br><br>The treatments are often promoted using false testimonies from people who have been cured. |

## Four Signs of a Scam, according to the United States'Federal Trade Commission on Consumer Advice (2020):

**1. Scammers pretend to be from an organization you know.**
Scammers often pretend to be contacting you on behalf of the government. They might use a real name, like a bank, tax agency, or make up a name that sounds official. Some pretend to be from a business you know, like your electric company or even a charity asking for donations.

They use technology to change the phone number that appears on your caller ID. So the name and number you see might not be real.

**2. Scammers say there is a problem or a prize.**
They might say you're in trouble with the government. Or you owe money. Or someone in your family had an emergency. Or that there's a virus on your computer.

Some scammers say there is a problem with one of your accounts and that you need to verify some information. Others will lie and say you won money in a lottery or sweepstakes but have to pay a fee to get it.

**3. Scammers pressure you to act immediately.**
Scammers want you to act before you have time to think. If you are on the phone, they might tell you not to hang up so you are not able to verify their story. They might threaten to arrest you, sue you, take away your driver's or business license, or deport you. They might say your computer is about to be corrupted.

**4. Scammers tell you to pay in a specific way.**
They often insist that you can only pay by using cryptocurrency, wiring money through a company like MoneyGram or Western Union, using a payment app, or putting money on a gift card and then giving them the numbers on the back of the card.

Some will send you a check (that will later turn out to be fake), then tell you to deposit it and send them money.

## How to protect yourself against scams

The next step to avoiding scams is to know how to protect yourself both off and online.

- Avoid any unexpected contact. Do not answer phone calls, letters or emails if they look unfamiliar. If you are a customer of the company use the contact details given to you in official paperwork or on their website to check if the person approaching you is legitimate.
- Never give out personal information. This can be used to steal your identity and access accounts. In particular, you should never share your full PIN or password with anyone. Your bank will ask you to use a card reader or ask for a few digits of your password if they need it.
- Keep operating system and virus protection software up-to-date. Do not ignore updates as these can often include patches to protect against new kinds of scams, viruses and ransomware. This goes for mobile devices as well.
- Make sure all your accounts have strong passwords. Do not use the same password for multiple accounts and change them regularly.
- Do not make any payments until you are sure the company you're dealing with is legitimate. Check with the company directly before making any payments.
- Never transfer money to a 'holding account'. This is a common scam. Someone will call you pretending to be from your bank's fraud team and ask you to transfer your money over to a safe account to protect it. But, if you do that, you are just sending a scammer your savings.
- If you are unsure about a financial services company, check your country's central bank website or securities commission of

regulated companies. If they are not on it, do not engage with them.

- If you are unsure about any other kind of company, you can look them up on the registrar of companies or equivalent agency in your country to find out their background or search for reviews online.
- Use safe and secure WiFi connections and avoid public WiFi. Your standard mobile network connection is often more secure than the one in the coffee shop or restaurant.
- Make sure any websites you are using are secure. Check to see if the web address starts with HTTPS, not just HTTP.
- Sign-up for a call blocking service that may be provided by your telephone operator. This might not stop all scam calls as they operate outside the legal guidelines, but it will stop cold-callers. This means any suspicious or unexpected calls you do receive are almost certainly from people you do not want to deal with.

## Lesson 1 Summary

We have seen many ways that scammers scam – our job is to not fall into their trap. If it sounds to good to be true, it is probably a scam.

**Something to think about:**

- Scammers are everywhere and the scam methods changes all the time.

**Something to remember:**

- Be suspicious all the time.

## How To Avoid a Scam

- Block unwanted calls and text messages.
- Don't give your personal or financial information in response to a request that you did not expect.
- If you get an email or text message from a company you do business with and you think is real, it is still best not to click on any links. Instead, contact them using a website you know is trustworthy.
- Resist the pressure to act immediately. Anyone who pressures you to pay or give them your personal information is a scammer.
- Know how scammers tell you to pay. Never pay someone who insists that you can only pay with cryptocurrency, a wire transfer service like Western Union or MoneyGram, a payment app, or a gift card. And never deposit a check and send money back to someone.
- Stop and talk to someone you trust. Before you do anything else, tell someone — a friend, a family member, a neighbor — what happened. Talking about it could help you realize it's a scam.

# Lesson 2: Protect your email account from hackers

## Lesson Introduction

We will be looking at how to protect our email from being hacked and it all starts by having a strong password and practicing safe behavior. For the full article, please refer to 3 Ways to Protect Your Email Account from Hackers - wikiHow (https://www.wikihow.com/Protect-Your-Email-Account-from-Hackers)

## Activity/Something to do

- Trainer to discuss what not to do when receiving suspicious emails

## Content Discussion

## Setting up your email account

**1. Create a strong password.**
A good password is hard for other people to guess, difficult for software to crack, but easy for you to remember. It can be difficult to come up with a password that meets all of your email service's criteria that's actually easy to remember, but here are a few tips:

- Your password should be long: The golden rule now is that a password should be 12 characters and contain a mix of uppercase letters, lowercase letters, numbers, and symbols.
- Password-protect your phone or tablet: Even if it makes it take a little longer to access your home screen, always password-protect your mobile devices. If someone else gains access to your unlocked phone or tablet, they will have access to all of your apps, including your email.

**2. Use a unique password for your email account.**
Avoid the temptation of reusing passwords on multiple accounts. If you use the same password to log in to your favorite website as you do your email, you are putting your email at risk—if someone cracks your password on that site, they will also have your email password.

- Since there are so many passwords to remember nowadays, search for a password manager app and choose one that has a great review.
- Avoid choosing the option to save your passwords on the web. If you save your password to make it easier to log in, anyone using your computer may access your email. This is especially important when you're using a public computer.

**3. Turn on two-step verification.**
Most of the popular email services, such as Gmail and Outlook, allow you to enable two-step verification, which adds a second layer of protection to your account. When two-step verification is turned on, you'll also have to enter a special security code that is sent to you via SMS or in an authentication app when logging in from an unknown source (a computer in a different area than you usually log in from). If someone manages to crack your email password, they would also need access to your phone to actually sign in.

**4. Make sure your computer is up-to-date and protected.**
To stay safe, make sure your antivirus or anti-malware software is up-to-date, and that you're running the latest version of your operating system and email application. Out-of-date security suites often do not have the coding necessary to deal with newer viruses or hacks.

- Also, be careful when installing free software—sometimes software comes with sketchy malware. Research apps before you install them.
- If you are using Gmail, you should frequently check which apps you've allowed access to your account or perform a Security Check. If you are using Outlook, you can check your account history to make sure nothing you haven't approved has happened.

## Be Careful:

**1. Avoid opening attachments unless you already know what it is.**
Unless you know exactly who the sender is and what the attachment is for, resist the urge to click anything in the email. Attachments can install malware on your computer, which makes it easy for hackers to access your email and your other personal information.

**2. Do not click any login links or buttons in an email message.**
Scam emails might also include fake login links or buttons that redirect you to a different website that captures your password. These emails are often very convincing and look like they come from a legitimate company or service you do business with. Even clicking the link can bring you to a site that looks like one you use often.

- If an email asks you to log in to update information or correct a billing error, open a web browser window, go to the address of the website directly, and log in that way to see if anything needs to be changed.

**3. Learn to identify phishing scams.**
Scammers may use email to target victims—they'll often send emails requesting personal information that can be used to forge your identity, such as your social security number or banking information. Never provide any personal information over email unless you know exactly who is requesting the information.

- If you are using Gmail or Outlook, a red or yellow message at the top of the email will appear, signaling that the email might be spam or a phishing scam.
- Check the return email address—is the person claiming to represent a certain company but using a free email account? Check the domain name (the part that comes after the @ sign) in the email address—is that actually the company's domain name? Sometimes scammers register fake domain names that look like the real thing to bait victims. For example, you could get an email from @netfl1x.com instead of the actual site, @ netflix.com.
- Does the message contain an offer that is considered too good to be true, or a claim that you have won a contest you never actually entered? Are you being asked to wire money to someone you do not know? These are all signs of scams.
- If a scammer claims to be affiliated with a company, contact

the company or service directly by phone or on their website. If there's a phone number provided in the email, double check by going directly to the company's official website and locate the phone number there. Sometimes scammers include fake contact information.

**4. Do not share your password with anyone.**
If anyone ever asks you for your password—even if they claim to work for your email service's support team—do not give them your password. There is never a need for a technical support representative to ask you for your password over the phone or email. Your password is meant to be private.

**5. Make your security question answers difficult to guess.**
If your email provider allows you to set up security questions in the event that you lose your password, do not enter answers that someone else can figure out, such as your mother's maiden name or your first pet's name.

- If the questions provided are pretty simple, you may want to enter something that is not the actual answer to the question—such as "Flamingo" as your mother's maiden name. Just make sure not to forget what you enter!

## Lesson 2 Summary

- Relook on having a strong password that is more than 12 characters and a mix of numbers and upper and lowercase numbers. Further protect your accounts with 2-factor authentication.
- Do not open attachments or click links in emails unless you are positive that they are safe. Always verify the sender's email address.
- Make sure your computer is up to date and is running a current version of protection software.

**Something to think about:**

- Having a good password is essential.

**Something to remember:**

- Avoid putting your computer and data in danger when you open attachments and links from unknown senders.

## Lesson 3: Protect your social media

### Lesson Introduction

Lesson 3 builds participants' awareness on how to better protect their social media accounts. It touches on the ways users can adopt and practice to prevent the social media accounts from being hacked. We will also cover Malware, how to detect if you are infected and best practices to be safer.

### Activity/Something to do

- Trainer to show a video on how to activate the multi factor authentication (MFA) for participant's social media account.
- Encourage participants to do the same as well if they haven't activated MFA.

### Content Discussion

These are activities to protect your social media account, specifically Facebook but all other social media accounts should follow the similar ways. For the full guide, please refer to an article from the Facebook Help Center at (https://www.facebook.com/help/213481848684090?cms_platform=ipad-app&helpref=platform_switcher)

### 1. Protect your password

- Do not use your social media password anywhere else online, and never share it with other people.
- Your password should be hard to guess, so avoid including your name or common words. Refer to Module 1, Lesson 3 on creating passwords.

### 2. Never share your login information

- Scammers may create fake websites that look like real social media websites and ask you to log in with your email and password.
- Always check the website's URL before you enter your login information. For instance, when in doubt, type www.facebook.com into your browser to get to Facebook.
- Do not forward emails received from official social media websites to other people, since they may have sensitive information about your account.

### 3. Log out of social media websites when using a shared computer

- If you forget, you can log out remotely by accessing the websites on your device.

### 4. Do not accept friend requests from people you do not know

- Scammers may create fake accounts to friend people.
- Becoming friends with scammers might allow them to spam your timeline, tag you in posts and send you malicious messages.

### 5. Watch out for malicious software

- Malicious software can cause damage to a computer, server or computer network.
- Watch out for signs of an infected computer or device and how to remove malicious software.

- Keep your web browser up to date and remove suspicious applications or browser add-ons.

**6. Never click suspicious links, even if they appear to come from a friend or a company you know**

- This includes links on your social media pages (example: on posts) or in emails.
- Keep in mind that social media accounts will never ask you for your password in an email.

## What are signs that you are infected by Malware?

Malicious software (Malware) is any harmful application or file designed to gain access to your computer or online accounts, such as your Facebook account. If you're infected, malicious software can collect information from you and take unwanted actions on your behalf (example: posting spam on your timeline).

- **On Facebook (FB)**
  - Your account is posting spam or sending unwanted messages.
  - Strange or suspicious log in locations are appearing in your FB account history.
  - You see messages or posts in your FB activity log you don't remember sending.

- **On your computer or mobile device**
  - Your applications run slower or tasks take longer than usual to complete.
  - You notice new applications you don't remember installing.
  - You notice strange pop ups or other ads without opening a web browser.

- **On your web browser**
  - You notice strange pop ups or other ads you don't remember seeing before.
  - Your search engine or home page has changed and you don't remember changing it.

## There are many types of Malware as listed below:

- **Virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.
- **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.
- **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.
- **Ransomware:** Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.
- **Adware:** Advertising software which can be used to spread malware.
- **Botnets:** Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

## How to remove and protect from Malware?

You can remove most malicious software from your computer or mobile device by following these steps:

1. Scan your device using an anti-virus tools.
2. Clean your web browser.
   - You can remove suspicious browser add-ons or undo recent changes to your web browser settings.

- If you use Chrome, you can also download the Chrome Cleanup tool for help with malicious software.

3. Update your web browser.
    - Running the latest version of your web browser ensures you have the latest security updates.
    - If your account was infected by malicious software, it is often used to follow people and like Pages that you have never heard of.
    - You can review your activity log and delete any posts you didn't mean to post and any Pages you didn't mean to like.

## Lesson 3 Summary

In this lesson, we learnt that the key to protecting your social media account is having a strong password and being aware of suspicious activities in your account.

**Something to think about:**

- Activate multi factor authentication and be aware of suspicious activities in your account.

**Something to remember:**

- Hackers attack accounts that have a lot of followers so be extra careful if you are one of them.

# Lesson 4: How to protect our kids online

## Lesson Introduction

As parents, we generally do everything we can to keep our children safe and well, like from getting them to  being careful when crossing a road and always wearing a helmet when cycling. But what are you doing to protect them from bullies, predators and inappropriate content online? This lesson will cover the points parents can utilize to ensure their child is protected online.

## Activity/Something to do

- Trainers to discuss with the partcipants what dangers kids faced online and how to mitigate those.
- Participants can take a kids safety test to see how we can educate on good online behavior with your children.
    - The link to this test:  (https://www.safekids.com/quiz/)
    - Trainers can walk through the quiz together and explain the questions.

## Content Discussion

How do we encourage our children to know how to be safe online?  Here are some great tips Laura Esterbrook (2017) have suggested on what every parent can do to keep their kids safe online | Children's Health Queensland  (https://www.childrens.health.qld.gov.au/about-us/news/feature-articles/10-things-every-parent-can-do-to-keep-their-kids-safe-online)

**1. Talk openly with your child about their online activity**
As soon as your child starts accessing the internet, talk to them about what they are reading, watching and who they are communicating with online – and keep the conversation going as they grow older. Ask your child what sites they visit or apps they use, write a list, and look at

them together. Talk to your child about what you think is appropriate, and remind them that this may be different for other parents and their children.

Listen to your child and reach an agreement about what is right for your family. Remember the time will come when they will access the internet outside the safety of home and you want them to be prepared for that.

It's vital to teach them about their online reputation, too, and how they must be careful about how they behave, interact with people and represent themselves in such a public forum. They must always remember that the internet isn't private.

**2. Keep screens and devices where you can see them**
Always monitor your child's time online, particularly younger children. Keep the computer in a central spot in the home where it's easy to keep an eye on what your child is doing and viewing online. For mobile devices, you can set them to forget Wi-Fi passcodes so your children can not go online without you knowing. You can also try to make an agreement that there are no tablets, laptops or gaming in bedrooms.

For younger children, you might also consider checking browser histories after your child has been online to see what sites they are visiting. This approach obviously gets harder as children grow older and work out how to clear histories – which is more reason to open the lines of communication about internet use at an early age.

**3. Know your parental controls**
Innocent searches online can lead to not-so-innocent results, so it's wise to know how to use the parental controls/search restrictions offered by web browsers, internet service provider and devices. For example, the SafeSearch Filters feature on Google will block sites with explicit sexual material. To turn it on, go to Settings/SafeSearch Filters. Although not completely accurate, parental controls can help prevent your child from seeing and accessing most violent or sexual material. Paid for security tools and features will offer extra protection and control. See (https://www.internetmatters.org/parental-controls/).

**4. Know who your children's online friends are**
As adults, we know that some people online aren't who they say they

are, but children and young people can be alarming naïve about who they are chatting with if they are not taught to be cyber wise from an early age.

Make sure you become friends and contacts within your child's social media circles and ensure you monitor posts. Your children may resist but tell them that is one of the conditions for you to allow them access.

**5. Be 'share aware' to protect your privacy**

If your child is a regular user of social networks, they must be aware of the risk of personal information or images being made public once they post it. While they won't fully understand the consequences of revealing personal information online, you should teach them to be cautious and thoughtful about what they post and share. Encourage your children to ask themselves before posting anything if the information (i.e. name, phone number, home address, email, name of school) or photo is something they would give a stranger. If the answer is no, don't post it.

If your child is sharing photos or posts online ask your child to let you see what they are sharing or ask an older sibling to check any photos before they're shared.

**6. Keep control of your family's digital footprint**

Every picture and personal detail that is posted and shared on social media and the internet contributes to someone's digital footprint. The big risk with this is that once information is shared publicly, it can be used in ways you may not expect and cannot control. You should also assume that anything that is put online is permanent (it can sometimes be deleted but not always before others have seen it and saved it). For this reason, children and young people need to be smart about protecting their images and information. The same goes for parents who regularly post pictures of their children's online.

Teach your child to stay in control of their digital footprint, by only sharing with people who they know and trust. Rather than posting to all their friends on social media, encourage them to be selective and use the privacy settings on the social media platforms they use.

**7. Teach your children to keep their location private**

Most apps, networks and devices have geo-tagging features which make

your whereabouts public and can lead someone directly to you. These features should be turned off for obvious privacy and safety reasons. Digital photos also contain metadata (information about the time, date and GPS coordinates) which may reveal more then you want to. Some social media platforms automatically hide or remove this data, but not all, so do your homework and know how much info you're sharing.

**8. Keep track of online time**

The Australian Physical Activity and Sedentary Behaviour Guidelines recommend children between the age of five and 17 should have no more than two hours of screen time a day. So, it's important to monitor your child's online time, particularly younger children, to ensure they do not develop bad habits. Get your children to agree on a period of time, say 30 minutes per session, and set a timer to go off – don't forget to make this a non-negotiable finish time. You should also switch off the home Wi-Fi at a set time each night (ideally before bedtime) so everyone has some 'time-out' from the internet. You can also try making some days 'screen-free' in your home to encourage everyone to pursue other more active and/or less technology-driven ways to entertain themselves.

**9. Be #SocialNetworkSavvy**

Educate yourself on ways to be safe on social networks so that you can give the best advice to your children. Sign up to the social networks and apps your children are using and find out how to use the privacy settings and reporting mechanisms. Talk about how they can stay safe on social networks, including talking to a trusted person when they are worried, and being aware of what constitutes online bullying – both as a perpetrator and a victim.

If your child uses social networks, be sure they know how to:

- Report inappropriate and/or offensive posts.
- Block someone.
- Keep information private.

**10. Lead by example**

Lead by example and always model the kind of positive online behaviour you would like your children to use. If they see you being cautious and respectable when you are online, they are more likely to follow in your

footsteps. And, yes, this includes limiting your own screen time.

Ultimately, you don't want to instil fear in your child or prevent them from experiencing the many educational, entertainment, social and other benefits of the internet, but rather give them the skills and knowledge they need to know how to make the most of it and avoid the dangers.

## Lesson 4 Summary

Teach kids how to protect themselves and how to identify dangerous situations. When talking to children, it is best to share and educate instead of just banning access. Also important is to review how we interact with the internet, as our children will copy our behavior. Learn what your kids are accessing and take a look at what happens in those sites and gaming apps.

*****Notes to Trainers**
Here is another set of quiz that you can use to help children understand better: https://www.nspcc.org.uk/globalassets/documents/fundraising/number-day/number-day-resources-2018/online-safety-quiz-ks3.pdf

Other helpful links:
https://www.esafety.gov.au/
https://kidshelpline.com.au/kids/get-help/webchat-counselling/

**Something to think about:**

- Predators are out there to get to our kids. Protect them.

**Something to remember:**

- Teach our kids how to identify threats online.

## Summary of Module 3

In Module 3, we covered the following topics that help us think like hackers so we understand how to protect ourselves:

- How to identify a scam where we looked at ways that scammers find a loophole to gain our trust and also the top 10 scams happening now.
- How to protect your email account by adding authentication. We also looked at malware and how to protect ourselves.
- How to protect your social media account. We also looked at how to know that your account has malware and how to protect ourselves from an attack.
- How to protect your kids online with these ten tips.

# COURSE WRAP UP

## Intermediate Activities

- Identify best practices in collecting customer data
    - All organizations will have to build their own processes when it comes to collecting data and keeping data safe. Invest in technology and get your employees trained to think safety first by equipping them with the right knowledge and mindset.
- Strengthen your website and social media accounts
    - Invest in firewalls and antivirus software to protect your website. Practice safe behaviours to manage organizations social media accounts.
- Standard operating processes (SOPs) for employees
    - Ensure that you have SOPs in place since one of the common sources for data to go missing is within the organization itself. Make sure you have safety and control measures on who gets to access the data of your organization.

## Long Term Activities

- Audit security of your server and applications – this is best done by hiring an expert to do penetration test and audit report.
- How to think like a hacker so that you build an internal awareness on how your SOPs and guidelines look to a hacker.

## Assesment Guide

The following are questions to assess readiness:

- Do you use online methods to promote your business? Please tick which ones.
    1. Website
    2. Email
    3. E-Commerce Store (own site)
    4. E-Commerce Store (merchant on Lazada, Shopee, etc.)
    5. Social media (Facebook, Instagram, Tik Tok etc.)
    6. Chat tools (Whatsapp, Telegram etc.)

- Do you ask customers to register with you?
    1. If yes, what kind of information do you ask for?
    2. Personal identification number
    3. Phone number
    4. Email
    5. Address
    6. If no, are you planning to keep details about your customer in the future?

- Do you keep the following information about a customer's payment details?
    1. Credit card number
    2. Bank account number

## Assessment Method

- Pop quiz based on scenarios
    - Are participants able to choose the right answers? This is also an opportunity to reinforce the learnings.
- Action items for personal and business protection
    - This allows the participants to assess their personal and business needs moving forward.

# COURSE REFERENCES

Kaspersky. (2020). Top 10 Internet Safety Rules & What Not to Do Online. Kaspersky.com. https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online

Kaspersky. (2019). What Is Cyber Security? Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Meshesha, Y., & Antonelli, D. (2024, April 11). How to Protect Your Email Account from Hackers. Wikihow.com. https://www.wikihow.com/Protect-Your-Email-Account-from-Hackers

Facebook. (n.d.). Keep your Facebook account secure | Facebook Help Center. Facebook.com. https://www.facebook.com/help/213481848684090

Money Helper. (n.d.). A beginner's guide to scams. MaPS. https://www.moneyhelper.org.uk/en/money-troubles/scams/a-beginners-guide-to-scams

Federal Trade Commission. (2020, November 9). How To Avoid a Scam. Consumer Information. https://consumer.ftc.gov/articles/how-avoid-scam

How to spot and avoid romance scams | Equifax UK. (n.d.). equifax.co.uk. https://www.equifax.co.uk/resources/identity-protection/how-to-spot-and-avoid-romance-scams.html

Mathis, S. (2022, July 12). How Do Companies Protect Customer data? TechTarget. https://www.techtarget.com/searchcustomerexperience/answer/How-do-companies-protect-customer-data

Edwards, R. (2019, December 23). 10 Safety Tips to Protect Yourself Shopping Online. SafeWise. https://www.safewise.com/blog/10-cybersecurity-tips-for-online-shopping/

Easterbrook, L. (2017). 10 things every parent can do to keep their kids safe online. [online] Children's Health Queensland. Available at: https://

www.childrens.health.qld.gov.au/about-us/news/feature-articles/10-things-every-parent-can-do-to-keep-their-kids-safe-online.

How do you protect your customers' data and privacy when using Payment Systems? (n.d.). linkedin.com. https://www.linkedin.com/advice/3/how-do-you-protect-your-customers-data-privacy

Online safety quiz. (n.d.). NSPCC. https://www.nspcc.org.uk/globalassets/documents/fundraising/number-day/number-day-resources-2018/online-safety-quiz-ks3.pdf

Kumar, G.V., Sum, T.W., Lynn, E.C.W. and Lung, C. (n.d.). Recent Personal Data Protection Law Updates Within the ASEAN Region . [online] LH AG Advocates and Solicitors. Available at: https://lh-ag.com/wp-content/uploads/2022/11/Recent-Personal-Data-Protection-Law-Updates-Within-the-ASEAN-Region_LHAG-Insights-20210512.pdf.

Northern Territory Government. (2015, June 11). Scams. Nt.gov.au. https://nt.gov.au/law/crime/scams/ten-most-common-types-of-scams

Federal Trade Commission (2020). How To Avoid a Scam. [online] Consumer Information. Available at: https://consumer.ftc.gov/articles/how-avoid-scam.

Southeast Asia digital, social and mobile 2019 - ASEAN UP. (2019, July 31). ASEAN UP. https://aseanup.com/southeast-asia-digital-social-mobile/


**APCICT**

Asian and Pacific Training Centre
for Information and Communication
Technology for Development