Security Threats at a Glance

Any actions that put our resources and information at risk is considered an incident or a security threat; that's why we have you as our last line of defence against such threats. You can stop or prevent those incidents or security threat by remaining vigilant against malicious attempts or theft to our information and above all, by following our security policies and procedures.

There are many forms of security threats of which, the most common incidents and easy to prevent are the theft, cybercrime and loss.

You are our best security protection against cyber threats or incidents. A security threat or incident is any action that puts our information or resources at risk. Such incidents may result from malicious attempts to steal information or from simple inattention to security policies or procedures. Either way, you have the power to stop most security threats.

Although the number of security threats is endless, the most common categories are loss, theft and cybercrime. Your attention to our security policies and procedures is critical to tipping the scales in our favour to prevent security breaches.

To explore security threats, click L**OSS, THEFT, a**nd C**YBERCRIME. W**hen you are finished, go to the next slide by clicking the N**AVIGATION ARROW (>>).**

THEFT

Theft can occur as a result of inattention to security procedures. For example, theft of confidential information can occur as a result of:

- Leaving laptops unlocked in the office, in cars, unattended in public places, or checked as luggage.
- Leaving unsecured USB in briefcases, handbags, clothes pockets, or on a desk in the office.
- Leaving documents containing sensitive information in plain view on an office desk.
- Giving building access to people posing as employees or contractors.

Theft can also occur when you discuss sensitive information in public places or allow strangers to look over your shoulder at the information on your computer.

CYBERCRIME

Cybercrime is any crime that involves a computer and a network. It can occur as a result of:

- Connecting to an unsecured public Wi-Fi hotspot .
- Neglecting to keep security software up-to-date, allowing malware to infect the computer.
- Clicking a link in an e-mail without verifying who the sender is.
- Sending sensitive or confidential information in an unencrypted e-mail.
- Opening e-mail attachments from unknown sources.
- Posting sensitive or confidential information to social networking sites.

LOSS

Information is transported using many forms of media and, because it is transportable, it can easily be lost. Security breaches can occur as a result of losing:

- USB drives
- Laptops
- Documents
- Security passes

- Briefcases or handbags
- Tablets
- Mobile phones

Physical Security

You are one of the most important defenders of the physical security of our information and property.

Your actions help protect our personnel, resources, and facilities from loss or damage from events such as theft, vandalism, fires, and natural disasters.

Take a few moments to learn about some best practices for protecting us.

To learn more about physical security best practices, click each **IMAGE.** When you are finished, go to the next slide by clicking the **NAVIGATION ARROW (>>).**

WORKING IN PUBLIC PLACES
When you do business in public places, be alert to the threats posed by:
S**houlder Surfing: R**efers to looking over someone's shoulder to obtain information. It commonly occurs in busy environments, such as office, or hotel lobby.

- E**avesdropping: O**ccurs when someone secretly listens in on a conversation.

- U**nsecured Mobile Devices: M**obile devices such as laptops, mobile phones, and USB flash drives are vulnerable to theft and unauthorised access if they are left unattended and unsecured.

SECURING WORK AREAS

To protect the information in the workplace:

- **Don't leave sensitive information in plain view**
A cluttered workspace often leaves sensitive information in plain view, You don't want a visiting client to see contracts sitting out in the open.

- **Don't throw away sensitive information in an unsecured place**
Thieves look for information in our trash, and the loss of information can compromise us as well as customer trust.

- **Don't delay in retrieving sensitive information**
Promptly retrieve documents from printers or photocopiers and clean whiteboards after meetings.

ACCESS CONTROLS
To prevent intruders from entering our facilities:
- Never let anyone –even someone you recognise- follow you into a secured area without scanning their badge.

- Never propone a door to a secured area. Doing so defeats the purpose of our access controls for preventing unauthorised entry.
-
- Never assume you know the access privileges for others. Visitors or even your co-workers may not be authorised to access the same areas as you. All guests need to receive their access credentials in accordance with our organisation's policies.

Safe Computing

We face a rising number of computer-related threats that compromise the security of information and resources. We've developed safe computing practices to help combat electronic threats, protect against social engineering, create strong and secure passwords, safeguard your computer and network, and communicate securely. When you follow our safe computing practices, you play an important role in preventing costly security breaches.

To explore safe computing practices, click each **IMAGE**. When you are finished, click the **NAVIGATION ARROW (>>)**.

ELECTRONIC THREATS
Most electronic threats involve malicious software or malware. Any time you work online or download/share files, you expose our organisation's computers and network to the risk of malware infection.
Be aware of warning signs of malware infection, including failed web searches, a sluggish computer, firewall malfunction, and unexpected browser activities such as excessive pop-ups. If you believe you are impacted by malware, follow our policies for reporting incidents.

SOCIAL ENGINEERING
Social engineering is the clever manipulation of people in order to gain privileged information. Social engineers may attempt to gain access to buildings or try to elicit passwords or other sensitive information from you in person, on the telephone, or online.
If you receive a suspicious request, always verify the identification of the person before acting and contact the appropriate person within our organisation for assistance.

PASSWORD GUIDELINES
Password security is critical to keeping our organisation's information secure. A strong password consists of a combination of normal characters (such as upper and lowercase letters and numbers) and possibly special characters (such as the pound sign or the dollar symbol).
To make your password more secure, change it frequently and protect it by not sharing it with others or leaving a written record of it on your desk.

ELECTRONIC SAFEGUARDS
The simple actions you take to protect your computer and other electronic devices are critical to our information security. Always remember to:
Follow our policies for keeping system security software running and up-to-date.
Never download or install unauthorised software or files.
Always turn on a password-protected screensaver when leaving your computer unattended.
Log off the network at the end of the day.
Secure laptops left at work in a locked drawer or with a locking cable.

ELECTRONIC COMMUNICATIONS GUIDELINES

- Electronic communications, including e-mail, instant messaging, texting, and social networking (such as Facebook, Twitter, and LinkedIn) make it easy to communicate but also increase the risk of a security breach.
  Follow these guidelines to secure information online:
  Always encrypt e-mails that contain personal or sensitive information.
  Be cautious when handling attachments or downloads, even if you know the sender.
  Never assume that information you want to share is public knowledge. Do not send or post any sensitive, personal, or proprietary organisational information on social networking sites or via e-mail.

Safe Remote and Mobile Computing

Mobile devices provide fast access to information and enable you to stay connected when away from the office. However, the use of mobile devices may also increase the risk of loss or theft of our assets if not properly protected.

When working away from the office or using mobile devices, you have a responsibility to know and applying guidelines to safeguard our network, information, and computing resources from unauthorised access.

Take a moment to learn more about some of the guidelines for safe remote and mobile computing.

To explore remote and mobile computing guidelines, click each **IMAGE.** When you are finished, click the **NAVIGATION ARROW (>>).**

- **SAFE COMPUTING AWAY FROM THE OFFICE**
  Whenever you use your mobile phone, laptop, or USB device when away from the office, be sure to follow our organisation's policies to safeguard your devices and the information stored on them.
  These policies include guidelines for:
  Using mobile devices on public transportation.
  Preventing unauthorised access to your home network.
  Travelling with and using mobile devices in airports.
  Securing mobile devices when staying in hotels.
  - **CONNECTING SECURELY TO NETWORKS**
    There are several security policies you must follow to ensure information is protected when connecting to our organisation's network outside of the office, whether with an Ethernet cable, wirelessly, or through a virtual private network (VPN).
    These policies include practices such as:
    Ensuring your network settings comply with our organisation's policies.
    Preventing others from using your mobile device when connected to our organisation's network.
    Choosing only secured wireless networks that comply with our security protocols.
    Using secure passwords and screensavers to prevent unauthorised access.

- **PROTECTING DATA ON MOBILE DEVICES**
  You can minimise the risk of information loss and theft by storing sensitive information on your mobile device securely and only when absolutely necessary. Always follow our organisation's policies for protecting data when using mobile devices.
  This includes:
  Taking extra security precautions when storing business e-mails and contact information.
  Only downloading approved software and applications.

Ensuring that any sensitive information stored on your device is encrypted.
Securing your device with strong passwords to prevent unauthorised access.

Protecting and Handling Data

We have established data storage and handling policies and procedures to protect sensitive information from unauthorised access, loss, and theft. Everyone is responsible for knowing and fulfilling their data security responsibilities to ensure our information and resources remain secure.

Take a moment to learn more about protecting and handling data.

To learn more about protecting and handling data, click each **BUTTON.** When you are finished, click the **NAVIGATION ARROW (>>).**

DATA TRANSMISSION

Data transmission guidelines are designed to prevent unauthorised parties from accessing sensitive information.

These guidelines provide direction for following our organisation's policies when:

T**ra**nsmitting data electronically.

Using FTP or other client share sites.

DATA CLASSIFICATION

Our organisation classifies data into various categories to help you understand what needs to be protected and what is available for public disclosure.

At a high level, data should be protected and handled according to our organisation's policies and procedures, established for each data classification:

Public

Internal

Restricted

SYSTEM BACKUP

Data loss can be reduced, if not eliminated, by performing system backups as necessary.

Always follow our organisation's policies and procedures for backing up data.

DATA STORAGE, RETENTION, AND DESTRUCTION

To properly protect data, it is important that you know how to store data, how long to retain it, and how and when to destroy it.

Our organisation has established guidelines depending on the type (i.e., electronic versus physical) and classification of data.

Reporting an Incident

Just as you take steps to protect our information, you must also report any incident involving threats to our information. If you witness an incident or even if a situation that doesn't seem quite right, you must act immediately and contact the appropriate person to investigate the incident.

Remember, we rely on you to be mindful and trustworthy, and to follow our incident reporting procedures.

Take a moment to see how well you would protect our information.

Click **START** to begin. Read each incident, and click **REPORT** or **DO NOT REPORT**. Be careful, three wrong answers, and you'll need to start over. To view examples of incidents, click **HINT**. When you are finished, go to the next slide by clicking the **NAVIGATION ARROW (>>).**

A mobile device is remotely wiped immediately after it's been misplaced.

Correct

This is not an incident and does not need to be reported.

Incorrect

This is not an incident and does not need to be reported.

Confidential papers are left in the copy room.

Correct

This is an incident and should be reported to the appropriate person immediately.

Incorrect

This is an incident and should be reported to the appropriate person immediately.

Passwords are left in plain sight.

Correct

This is an incident and should be reported to the appropriate person immediately.

Incorrect

This is an incident and should be reported to the appropriate person immediately.

TRY AGAIN

Uh oh, that's too many wrong answers. Click the R**ETRY** button to try again.

A document containing sensitive information is sent to the wrong recipient.

Correct

This is an incident and should be reported to the appropriate person immediately.

Incorrect

This is an incident and should be reported to the appropriate person immediately.

TRY AGAIN

Uh oh, that's too many wrong answers. Click the R**ETRY** button to try again.

Computer antivirus software is up-to-date.

Correct

This is not an incident and does not need to be reported.

TRY AGAIN

Uh oh, that's too many wrong answers. Click the R**ETRY b**utton to try again.

YOU'RE AWESOME!

You did a great job of recognising and reporting incidents.

To continue, click the N**AVIGATION ARROW (>>).**