Information Security and UST

An induction training program on protecting valuable business and personal information

May 2024

Version History

Date	Ver	Description	Author	Reviewer	Approver
28-Jun-22	1.0	Baseline Document	Greeshma Raveendran	Krishnakumar	Adarsh Nair
11-Aug-23	2.0	Reducing the slide count as the induction time slot has been reduced	Akhil Asokakumar	Krishnakumar	Adarsh Nair
11-Sep-23	2.1	Updated the UST certification details	Akhil Asokakumar	Krishnakumar	Adarsh Nair
20-Nov-23	2.2	Updated as per new branding template	Sathyush S	Satish	Adarsh Nair
28-Feb-2024	2.3	Updated the Template to latest version	Simi Kalathoor	Ranjana Vettath	Adarsh Nair
13-May-2024	2.4	Updated UST Certification details to include PIMS	Anaya Solomon	Ranjana Vettath	Adarsh Nair

Objective of the program

To give you an overview of;

- Information Security, Data Privacy, Business Continuity
- Data Privacy policies and practices at UST
- Your Information Security responsibilities as a USsociate

UST Information Security policy

> *It is the policy of UST that information must be protected in all its forms, on all media, during all phases of its lifecycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction*

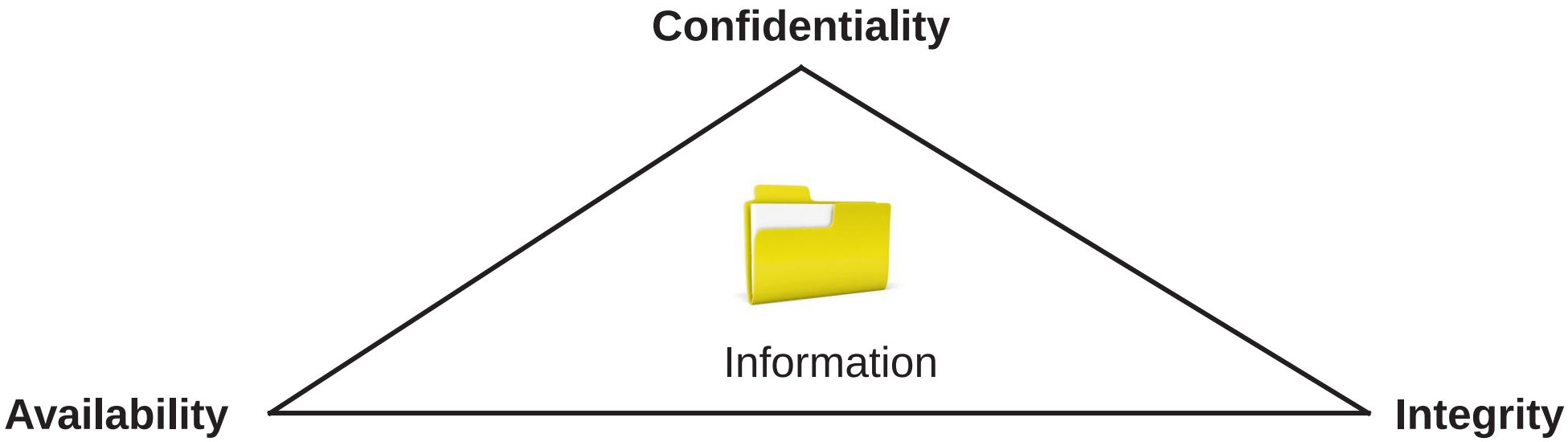
Privacy vision statement

To build an environment in which privacy and data protection mandates are effectively fulfilled, thereby increasing the confidence that our employees, customers and other stakeholders have in UST while handling personal data

What is Information Security?

Information Security focuses on protection of **Confidentiality**, **Integrity** and **Availability** of information

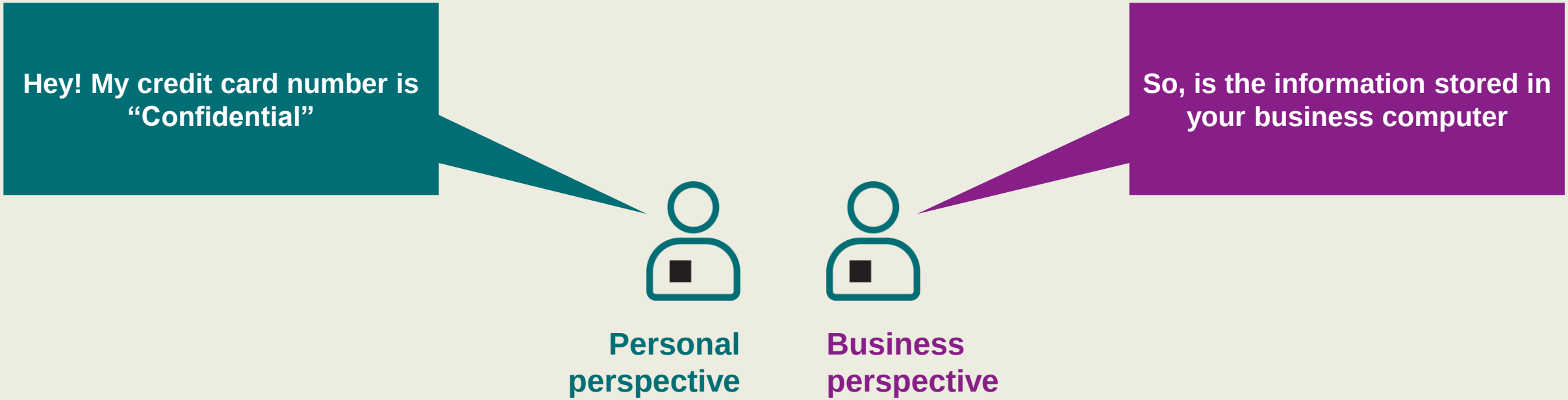
That's **CIA,** simple, isn't it?



What is Confidentiality?

Making sure only those people who are supposed to see the information, see it.

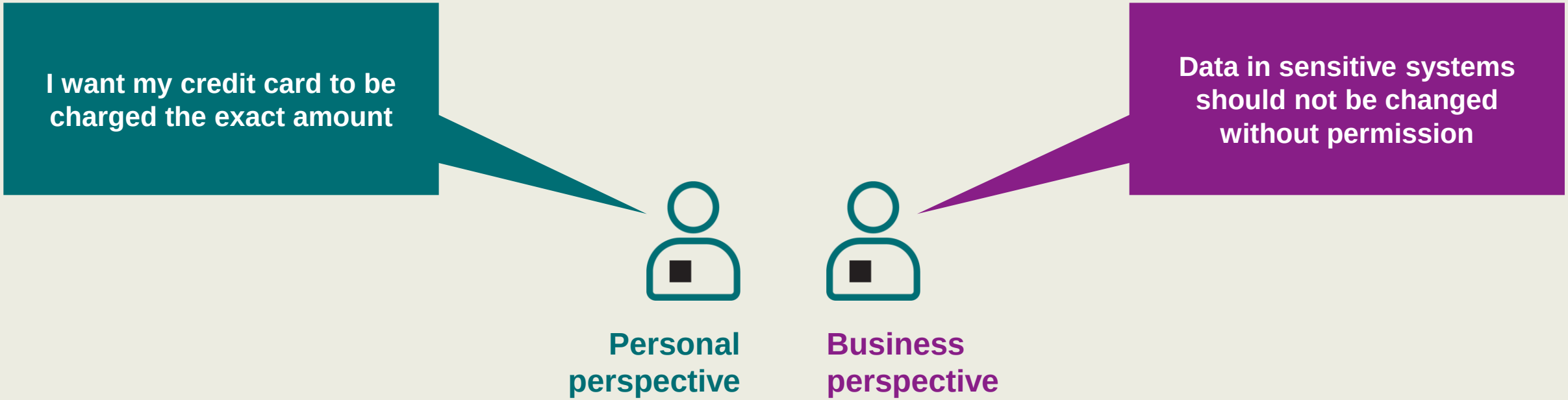
Example: A password or PIN number enforces Confidentiality



What is Integrity?

Making sure only those people who are supposed to change (edit) the information, can change it.

Example: File permissions enforce Integrity



What is Availability?

Making sure that the information is available when the authorized people need it.

Example: Backups ensure Availability

I keep backup of my credit card statements in case disputes arise

Personal perspective

Business perspective

Keeping a backup of business data to ensure availability during situations like equipment failure.

Information Security Management System (ISMS) & its objective

We handle different types of sensitive information such as client data, UST's own information and employee data and these are essential for executing business processes, satisfying client requirements and adhering to the laws of the land.

ISMS helps us to:

- Centrally manage and co-ordinate security efforts effectively
- Continuously assess and improve our security posture
- Integrate clients and regulatory requirements into the information security policies and practices
- Investigate incidents and take appropriate actions

U ▪
S T

‘’Human brain hold around more data compared to electronic/paper media. So most information security leaks happen via human beings …i.e., you and me!”

Information Security responsibilities

- Our primary information security responsibility is to protect the “Confidentiality, Integrity and Availability” of Information
- Information here means, information belonging to UST and information belonging to our clients

By Protecting Information

- You ensure continuous availability of information and information systems that help in the growth of the business.
- You give confidence and assurance is to our customers that their information is safe with us. This drives more business.
- You are on the right side of information protection laws in various geographies that we operate in.

U ▪
S T

Physical Security and Visitor Access Control

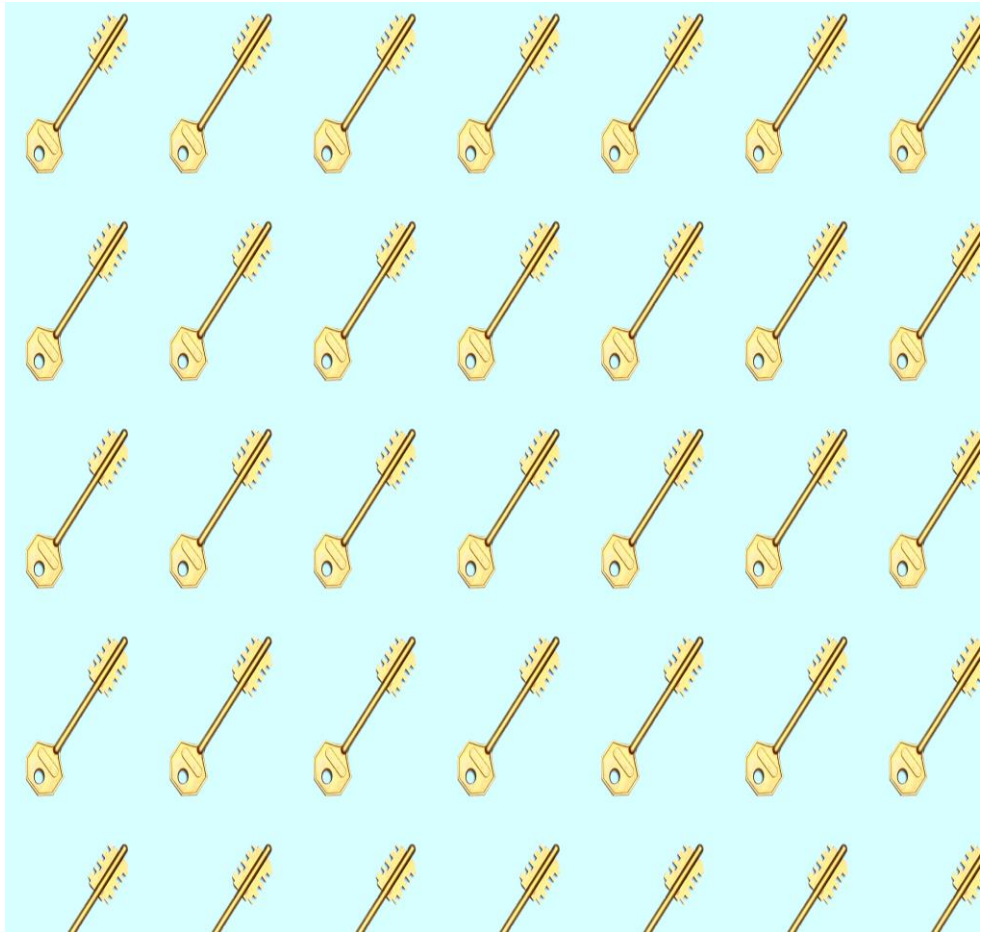
What does it mean?

- Ensure that only authorized users enter UST facilities
- Ensure that access to sensitive information for external parties is provided only after authorization

How to practice it?

- Use your access card to enter the facility.
- Do not tailgate or encourage tailgating .
- Register visitors and declare their computing devices.
- Visitors should be always escorted.

Computers and Applications Access Control



What does it mean?

- Access to sensitive systems and applications is a privilege. Treat it with respect.

How to practice it?

- Never share your passwords or access cards with anyone
- Use strong passwords as directed by the password management policies set by the organization

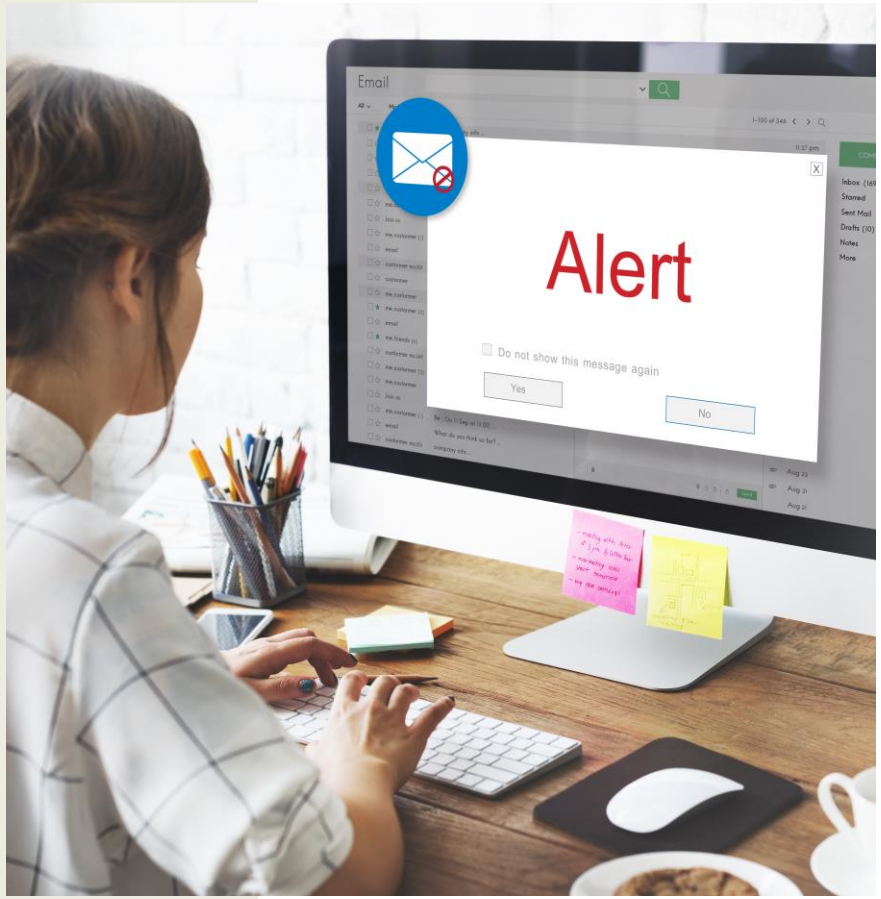
Email security

What does it mean?

- Avoid information leakage through email
- Be careful of worms and viruses in email attachments

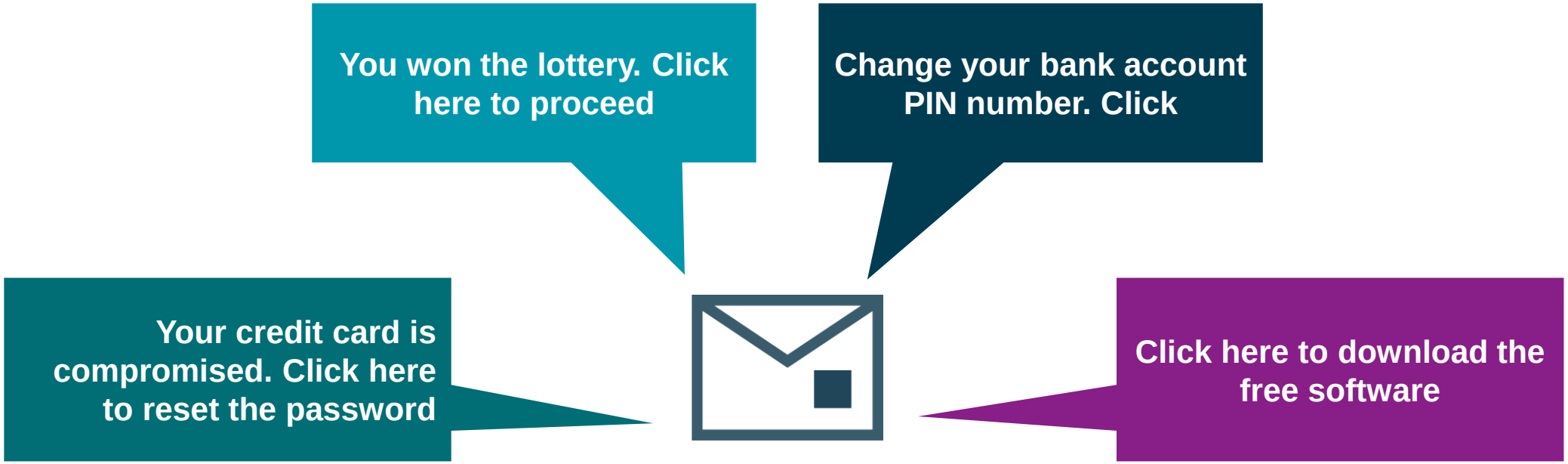
How to practice it?

- Use official emails only for official purposes
- Do not open suspicious attachments
- Do not forward inappropriate emails to official email ID’s



U ▪
S T

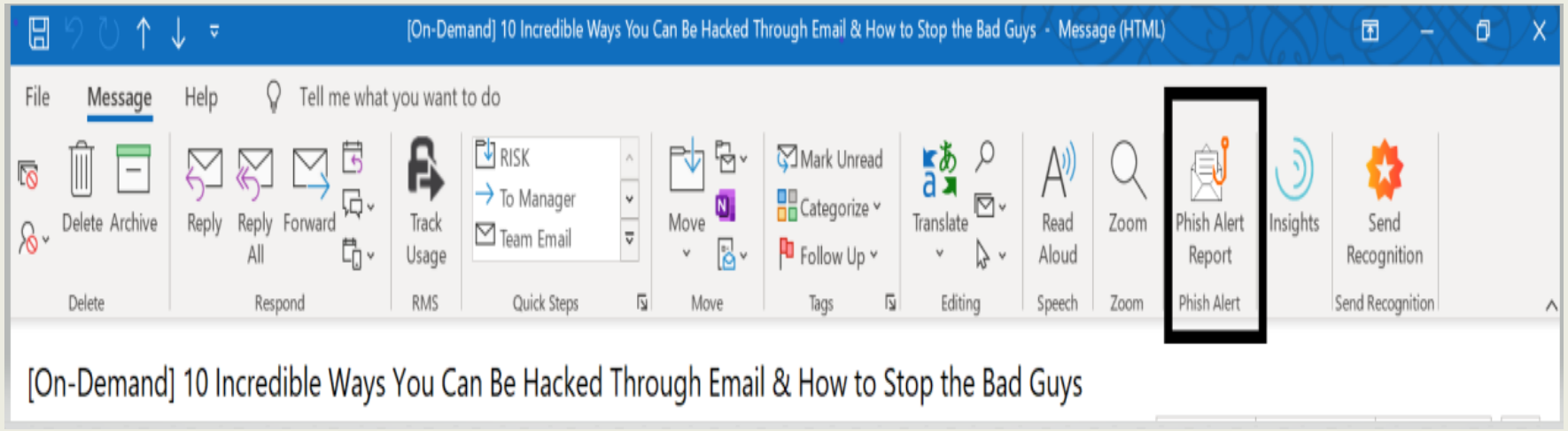
Example: Email security threats: Phishing

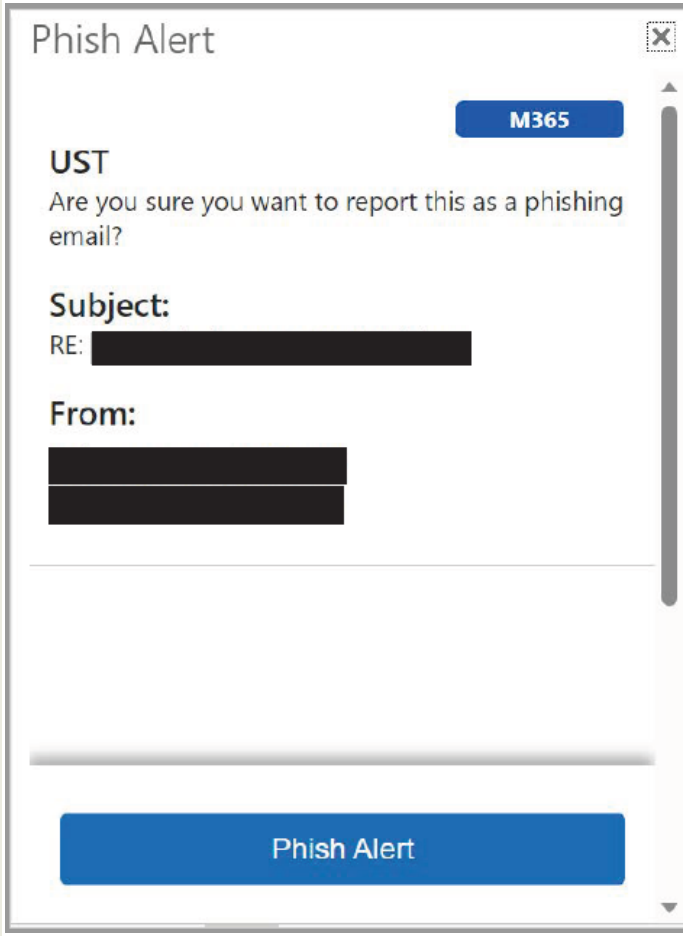


Beware of Phishing mails

- Criminals use techniques such as “phishing emails” to entice you into, revealing sensitive information such as bank account numbers, PIN and credit card details. They may also entice you into installing malicious software
- Stay safe by avoiding emails or SMS messages that ask you for sensitive information. Stay alert!

Phish Alert Button





The perfect solution to phishing is to report the suspicious emails using the '**Phish Alert Report button**'. It is a safe and easy way to tackle any suspicious email as this feature sends the phishing email to the security department or an in-depth analysis of the threat - all at just one click!

AC

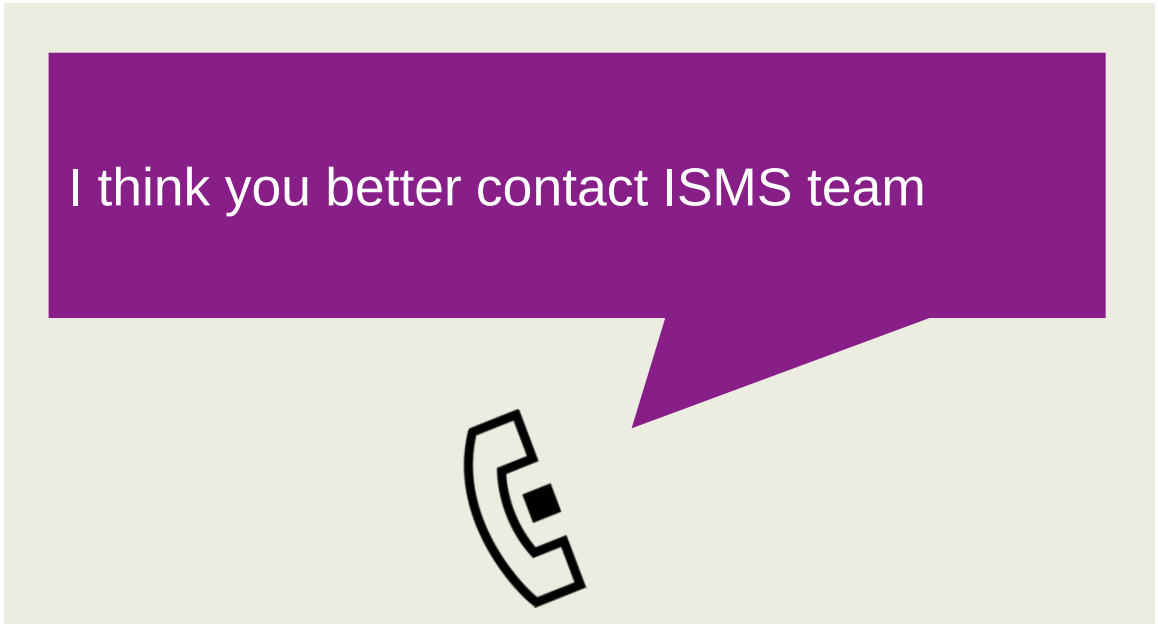
NB: If the Phish Alert report option is greyed out or not visible , kindly drop an email to **securitylearning@ust.com**

U ▪
S T

Information disclosure and social engineering

Social engineering: Is a technique through which attackers steal information from human beings (through telephones, email, direct contact etc.)

Refer all request for UST business information immediately to the email id - isms@ust.com



Clear desk/Clear screen

What does it mean?

- Reduce possibilities of information being openly visible and accessible to unauthorized people

How to practice it?

- Lock workstations while leaving the work desk
- Avoid having a cluttered work desk
- Lock sensitive documents in the cabinet after use
- Wipe white boards after meetings are over
- Pick printouts immediately after printing

Secure information disposal

What does it mean?

- To ensure that sensitive information, after usage, does not fall into the wrong hands

How to practice it?

- Destroy sensitive information or information devices after usage
- For paper documents, use the shredder

Internet security (general, social networking/blogging)

What does it mean?

- Avoid information leakage through Internet
- The Internet should be used only for UST business
- Be careful of what you browse. Your Internet activity is monitored.

How to practice it?

- Do not download and install unauthorized software
- Do not post sensitive UST information on publicly accessible sites
- Do not use the Internet to defraud, harass or defame others
- Do not violate any company policy; or any applicable law, ordinance or regulation

Mobile phone and portable media usage

What does it mean?

- Avoid information leakage through portable media devices
- Avoid using unauthorized apps for communication (like WhatsApp) for official use

How to practice it?

- Portable storage media such as USB drives/external hard drives are not allowed inside the office

Portable computing devices (Laptops)

What does it mean?

- Protect portable computing devices such as laptops from theft and accidental loss.

How to practice it?

- Always carry these devices with you.
- Never put laptops in check-in luggage while flying.
- Never leave laptops unattended in cars and at public places.

Insider Threat

An insider threat refers to a cyber security risk that originates from within an organization. It typically occurs when a current or former employee, contractor, vendor, or partner with authorized access misuses that access to negatively impact the organization's critical information or systems. An insider threat may be executed intentionally or unintentionally. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems.

Key Points to be noted:

- Monitor and review access rights granted to the associates on a regular basis.
- Be cautious while sending emails – ensure the recipient address and email content is correct.
- Follow organizational policies without fail.
- If you find or suspect something suspicious, report it.

Information Security Incident Reporting

What does it mean?

To prevent incidents from becoming catastrophes, report it.

To report a security incident, send a mail explaining about the violation to

SecurityIncidentReporting@ust.com

Or

Ishelpdesk@ust.com

And can report the Security Incident through **ServiceNow** under IT section

Examples of Information Security Incidents

- A misbehaving computer. It could be a virus or worm. Report it before it becomes serious
- A missing file or document
- A stolen laptop
- A stranger without valid identification inside the facility
- An unattended laptop or information device
- Someone taking photos inside the facility or using a portable storage media
- Someone sharing passwords
- UST information posted publicly on the Internet
- An empty meeting room with sensitive information on the whiteboard
- Anything else that is against UST Information Security policies

What is Personally Identifiable Information (PII) ?

PII (Personally Identifiable Information) is any information about an individual that can be used to distinguish or trance an individual's identity or can be linked to an individual

Examples of PII

- Name
- Date of Birth
- Mother's maiden name
- Social Security number
- Financial records
- Email address
- Health Information
- Passport number
- Driver's license number, etc.

Do’s and Don’ts for Data Privacy

Do’s

- Strictly follow the information security practices.
- Hold personal data about people only when necessary.
- Ensure personal data is kept accurate and up to date.
- Ensure all personal data is disposed of as confidential waste.
- Report immediately, any accidental or deliberate release of personal information to:

ISMS@ust.com

or

SecurityIncidentReporting@ust.com

Don’ts

- Never disclose PII information to anyone in the organization or to an external organization.
- Don’t Disclose any personal data over the telephone.
- Leave personal data insecure in any way, whether it is physical files or information held electronically.
- Use personal data, held for one purpose, for a different purpose without permission from the data subject.
- Put personal data about an individual on the Internet or in social media without their permission.

The need to protect PII

- Regardless of how the data is lost, the cost of a data breach can be huge. Fines are one of the most widely-known consequences of losing personal data, and they can be very expensive (e.g., up to $1.5 million per year in the case of a breach of healthcare records in violation of the Health Insurance Portability and Accountability Act [HIPAA] regulation or up to £500,000 from the UK Information Commissioner).
- However, the consequences extend much further and include reputation damage, loss of customer trust, employee dissatisfaction and attrition, and clean-up costs following the breach.

Business Continuity Planning (BCP)

"UST is committed to developing & implementing a Business Continuity Plan, to reduce the threat to critical business functions; to protect its employees & assets, to recover & resume its critical business functions to operate within business acceptable time frame following a crisis or a disaster"

Defining Business Continuity Plan

The process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change.

UST practice

- Management level continuity plan
- Account level continuity plan
- Function level continuity Plan
- Service level continuity Plan
- UST has mainly Account, Functional and Service level continuity plan which is monitored at the management level

ISMS awareness trainings

- ISMS quarterly trainings are mandatory and should be completed within the given due date **as it is part of UST's ISMS policy.**
- Trainings will be rolled out via ISMS training platform – **KnowBe4**
- The link to the training and the due date will be mentioned in the notification email.

If you face any issues in accessing the link please contact:

Security Learning at securitylearning@ust.com

Certifications

UST has the following accreditations and certificatio

- ISO 27001 Information Security Management System
- ISO 22301 Business Continuity Management System
- PCI-DSS for specific customer
- HITRUST accredited
- SOC2 Type II Compliant
- ISO 27701:2019 Privacy Information Management System

U ▪
S T

“Good Information Security practices make us a winner”

Practice It

- Information Security focuses on protecting the C, I and A of information
- Information security helps the business to grow by gaining the confidence of customers and by helping to be on the right side of the law
- Each of us must exercise our information security responsibilities by applying the safe security practices at work
- For more information, connect with us at isms@ust.com

Thank you

Copyright and confidentiality notice

UST
5 Polaris Way
Aliso Viejo, CA 92656

T +1 949 716 8757
F +1 949 716 8396

ust.com