



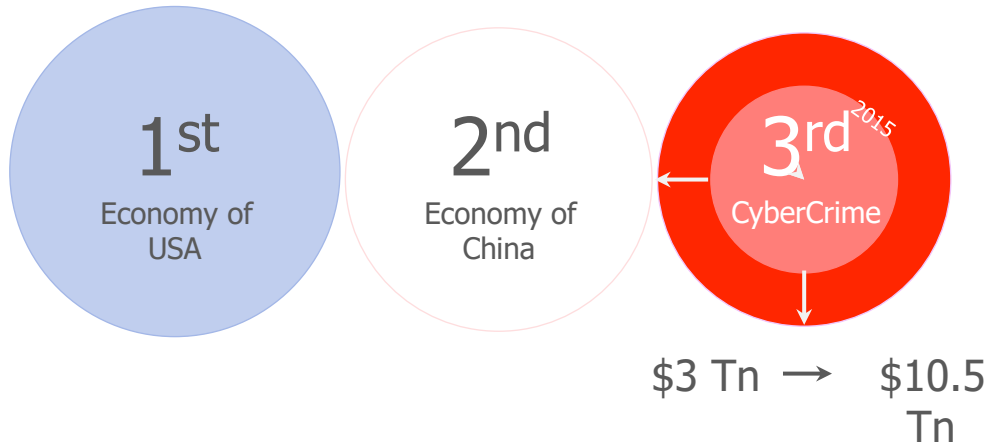
Information Security Awareness Training



The Cyber Threat Wave

Cybercrime is projected to cost the world **\$10.5 trillion USD by 2025**, according to Cybersecurity Ventures. If it were measured as a country, cybercrime would rank as the world's **third-largest** economy after the U.S. and China, growing over **20% annually**.

\$330,000 / second



11 seconds

that's how often a business is hit by a ransomware attack in 2024, according to Cybersecurity Ventures.

\$30 billion annually

cryptocrime is projected to reach this figure by 2025, almost twice the losses seen in 2021.

74%

of organizations faced a significant cyber attack in the past year, according to the World Economic Forum's Global Cybersecurity Outlook 2024.

4X

increase in extreme cyber losses—now reaching \$2.5 billion—threatens company solvency, per the Global Financial Stability Report.

Agenda

1. Information Security
2. Impact of Security Breaches on Business
3. Data Classification
4. Information Security Model
5. Information and Information Assets
6. Threats and Vulnerabilities to Information
7. Information Security Policy
8. Importance of conforming to information security policy and objectives
9. Information Security Best Practices

Agenda

- 10. Clear Desk and Clear Screen
- 11. Password Management
- 12. Email Security
- 13. Malware
- 14. Common Malwares
- 15. Phishing Attacks
- 16. Software Development Life Cycle
- 17. Takeaway Do's and Don'ts

INFORMATION SECURITY

Information Security refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction and inspection.

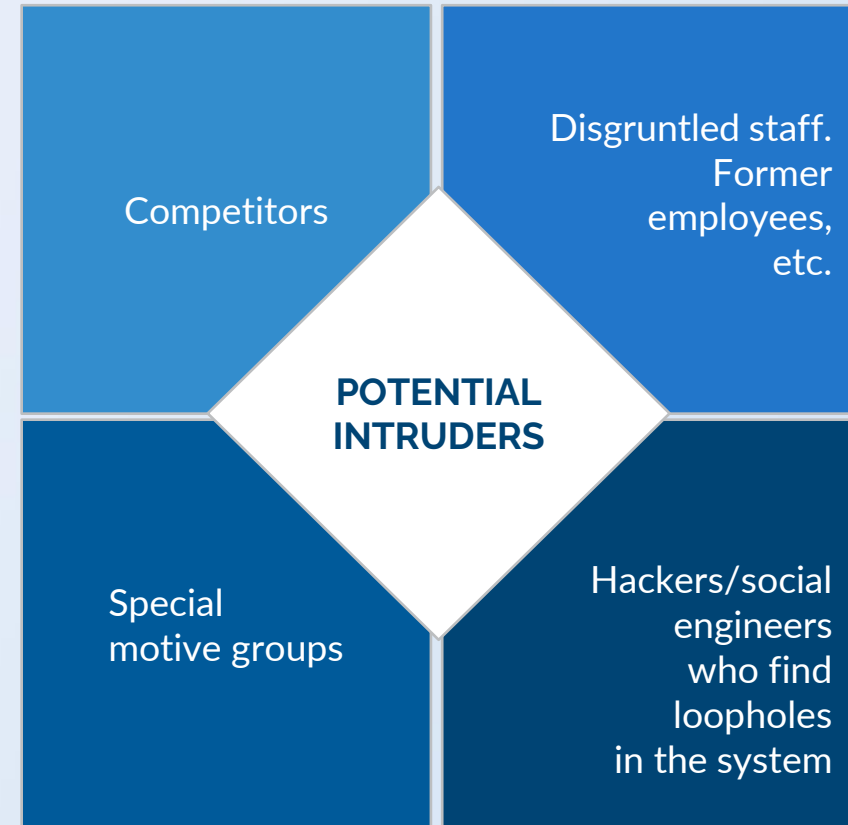
Good Information Security practices helps in

- ☐ Minimizing Threats
- ☐ Reduces Risks
- ☐ Ensure Business Continuity



IMPACT OF SECURITY BREACHES ON BUSINESS

- ❑ Damage to reputation
- ❑ Loss of market and customer confidence
- ❑ Disruption in business
- ❑ Financial loss
- ❑ Competitive edge in the industry jeopardized



DATA CLASSIFICATION

Restricted

Highly- Sensitive information

Confidential

Sensitive information

Internal

Non- sensitive information that is not released to public

Public

Information has been approved for public access

DATA CLASSIFICATION

RESTRICTED

This information is usually described as 'non-public information' about people or critical business or research operations under the purview of the Owner/Data Custodian

CONFIDENTIALITY

Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know.

INTERNAL

Intended for use within the EFR and authorized third parties only.

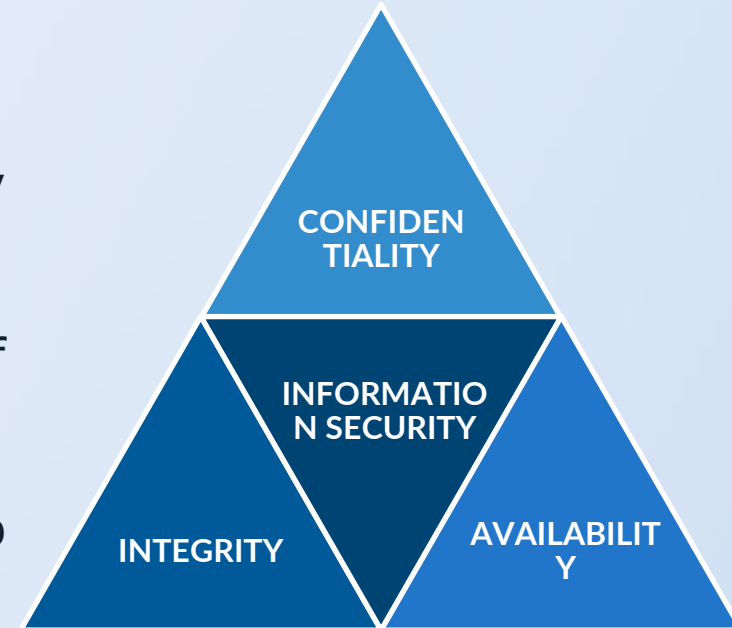
PUBLIC

Information that may or must be open to the public.

INFORMATION SECURITY MODEL

Information Security helps in protecting

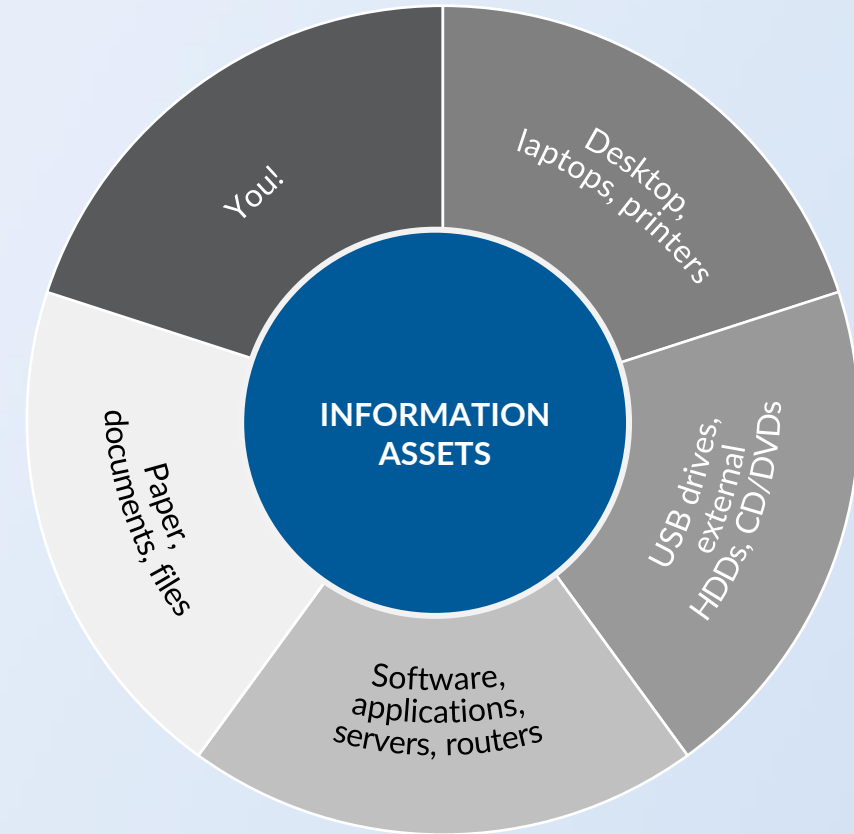
- ❑ **CONFIDENTIALITY** : Confirming that information is accessed by only those who have authorization to have access to it.
- ❑ **INTEGRITY** : Safeguarding the accuracy and completeness of information and its processing methods.
- ❑ **AVAILABILITY**: Confirming that authorized users have access to information whenever required by them.



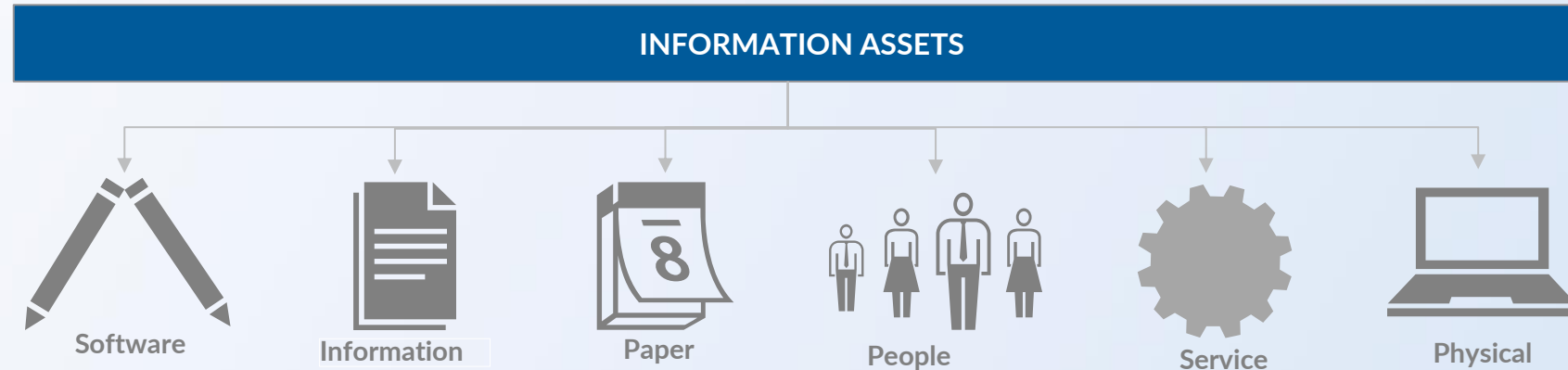
INFORMATION & INFORMATION ASSETS

INFORMATION MAY EXIST IN MANY FORMS

- ☐ Printed or written on paper
- ☐ Stored electronically
- ☐ Transmitted by electronic means
- ☐ Shown in corporate videos
- ☐ Verbal



THREATS & VULNERABILITIES TO INFORMATION



Vulnerabilities are weaknesses associated with information assets, which could be exploited by threats.

Information security controls provide a layer of protection between the threats and the information assets.



Threats are anything that could cause damage/harm/loss to assets.

INFORMATION SECURITY POLICY

- ❑ It is the policy defining about its information assets that shall be protected from all threats identified, whether internal or external, deliberate or accidental, such that:
 - Confidentiality of customer information is maintained.
 - Integrity of customer information can be relied upon.
 - Availability of customer information is maintained.
- ❑ All legal, regulatory, statutory, and contractual obligations are met.
- ❑ The brand image is protected.
- ❑ To identify the information assets, and to understand their vulnerabilities and the threats that may expose them to risk, a risk assessment is performed by EFR management.
- ❑ To manage the identified risks to an acceptable level, shall design, implement, operate, and improve a formal Information Security Management System (ISMS).

IMPORTANCE OF CONFIRMING THE INFORMATION SECURITY POLICY AND OBJECTIVES

- ☐ Help bring into compliance with legal, regulatory, and statutory requirements
- ☐ Minimize internal and external risks to customer information and our business
- ☐ Limit the risk of security and privacy breaches
- ☐ Provide continuous protection that allows for a flexible, effective, and defensible approach to security and privacy
- ☐ Reduce operational risk where threats are assessed, and vulnerabilities are mitigated
- ☐ Increase overall organizational efficiency and operational performance
- ☐ Enhance our reputation and potentially gain a competitive advantage



INFORMATION SECURITY PRACTICES

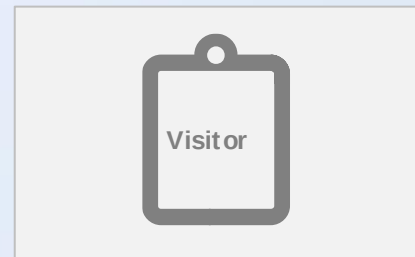
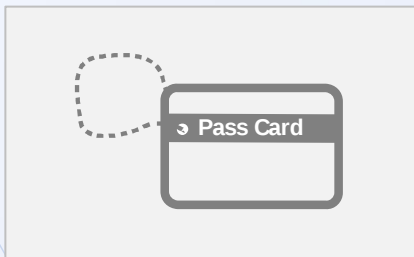
- ☐ PHYSICAL SECURITY
- ☐ CLEAR DESK AND CLEAR SCREEN
- ☐ PASSWORD MANAGEMENT
- ☐ PROTECTING INFORMATION AND WORKING OFF-SITE
- ☐ EMAIL SECURITY
- ☐ INTERNET USAGE AND MALWARE PROTECTION



INFORMATION SECURITY PRACTICES

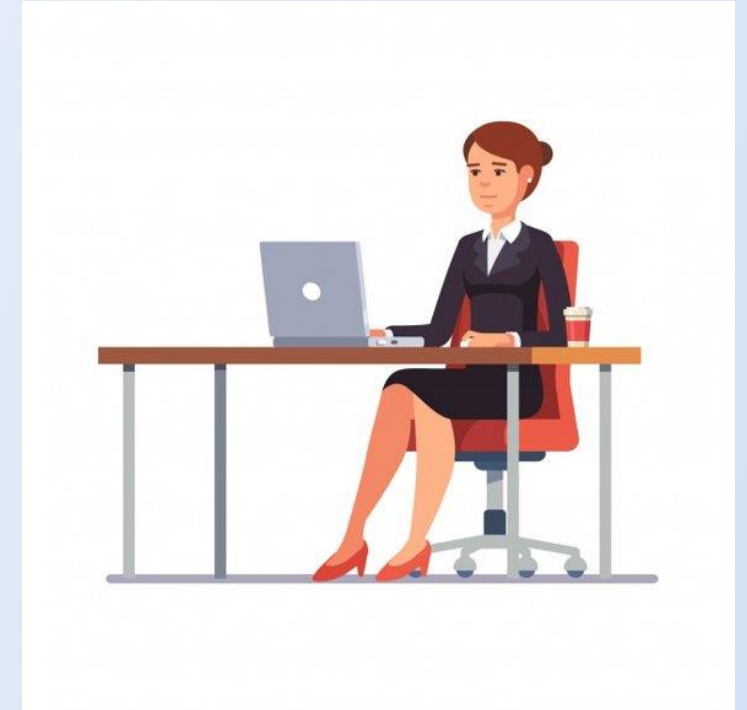
PHYSICAL SECURITY

- ☐ Use only your biometric / access card to enter/leave the premises. Do not tailgate.
- ☐ All visitors (including former employees) should be accompanied by an employee during their visit.
- ☐ Never lend your access badge to anyone. Challenge a person not carrying access badge and ask for their identification.
- ☐ In case of loss or theft of your access badge, immediately report the same.
- ☐ Raise an incident through your manager about unattended and unprotected equipment within your work area.
- ☐ Familiarize yourself with the security layout and contingency plans in place in case of an incident.
- ☐ Do not try to enter restricted premises with business reason and authorization.



CLEAR DESK AND CLEAR SCREEN

- ☐ Confirm that your screen is locked, whenever you leave your workstation by using '**Ctrl**' + '**Cmd**' + '**Q**' or **Windows + L**
- ☐ Clear your desks before leaving. Keep confidential information in secure storage. Keep filing cabinets shut and locked, when unattended.
- ☐ Information should never be left lying around or unattended on printers or fax machines. Empty in-trays and clear your work area before leaving it.
- ☐ In case documents containing sensitive information are no longer required, they should be shredded before disposal.



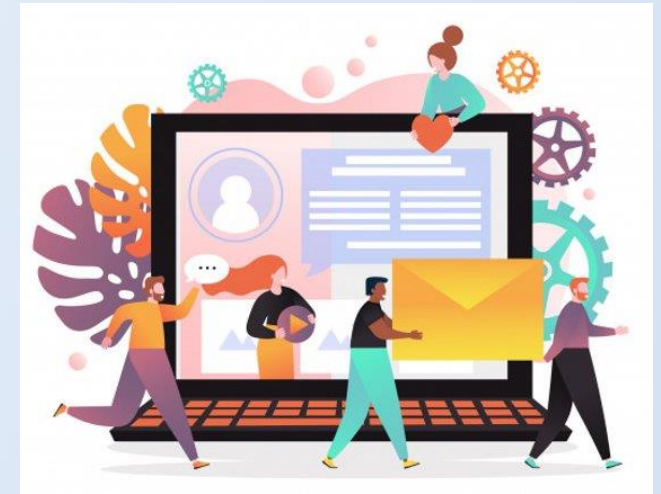
PASSWORD MANAGEMENT

- ☐ Rotate passwords on a regular basis.
- ☐ Never share or divulge your passwords, even when receiving technical assistance.
- ☐ Do not use any “password saving” features in any application or software, which would defeat the purpose of requiring a password.
- ☐ Never write down or store passwords in a readable format.
- ☐ Choose a password that satisfies the password policy:
 - ☐ Minimum 12-14 characters
 - ☐ Contains upper case, lower case, digits, punctuation, non-alphabetic
 - (not a recognizable word)



E-MAIL SECURITY

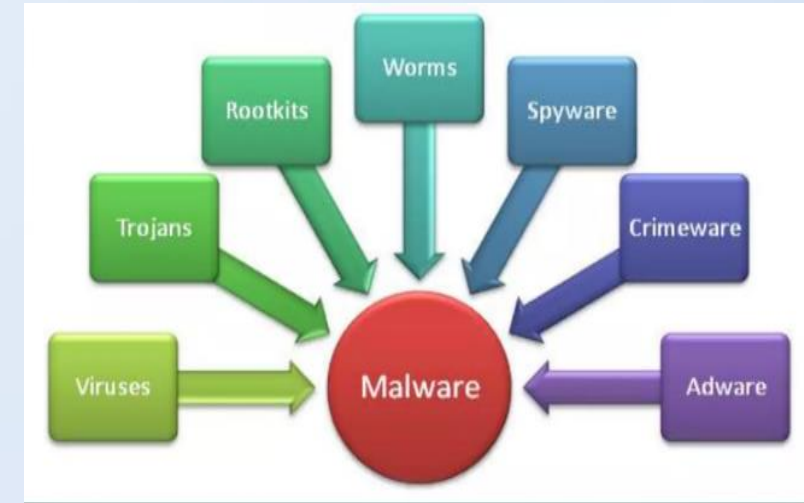
- ☐ Corporate e-mail is meant for business purposes. Do not use personal e-mails for official communications.
- ☐ Do not auto forward emails to external email addresses.
- ☐ Do not send IP, IDs and passwords or other sensitive data in an unencrypted email messages.
- ☐ Report all SPAM or phishing messages (messages from an unauthorized sender requesting personal or corporate information) as an incident.
- ☐ Emails from unauthorized senders containing attachments and links should be permanently deleted and reported as an incident.
- ☐ Employees using e-mail resources are subject to having their activities monitored by system or security personnel without any specific notice.
- ☐ Do not open emails from unknown senders



MALWARES

WHAT IS MALWARE?

- ❑ Made up of two words “Malicious” + “Software”
- ❑ **Malware** is an umbrella term used to refer a variety of malicious software variants, including viruses, ransomware and spyware.
- ❑ Malware typically consists of code developed by cyber attackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network.
- ❑ Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or to open the file to execute the malware.



COMMON MALWARE

RANSOMWARE



A type of malware that encrypts files or systems until a ransom is paid to decrypt and restore access

TROJAN



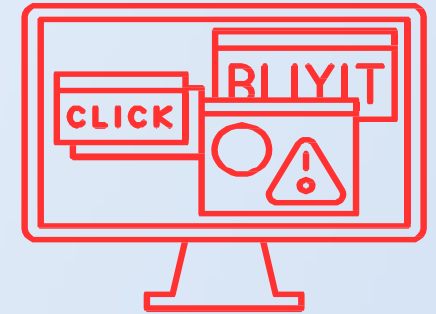
Malicious programs that are disguised as legitimate software to trick users into installing and executing an attack payload on their systems.

VIRUS



Viruses are malicious code that spread by copying themselves to infect files, programs or boot sectors to alter system function.

ADWARE



Adware is software that automatically displays or downloads advertising material such as banners or pop-ups when a user is online.

COMMON MALWARE

SPYWARE



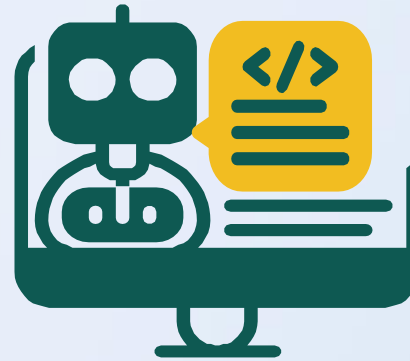
Spyware is malicious software that secretly monitors and collects data on a user's online activities, data and communications without consent.

WORM



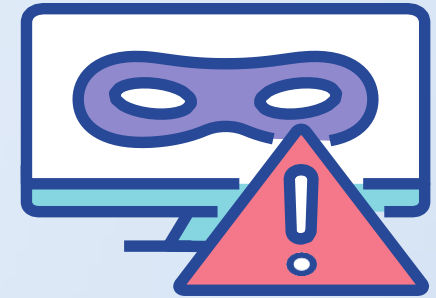
A computer worm maliciously self-replicates across networks by exploiting vulnerabilities.

BOTS



Bots are automated programs scripted to perform online tasks like crawling content, querying data, or interacting with users.

ROOTKITS



Rootkits stealthily gain system access by hiding malicious components from detection.

MALWARES

RANSOMWARE ATTACK, AKIRA 2023

•**Description:** Akira ransomware appeared early in 2023 to attack small to medium-sized businesses across several industries. Akira encrypted files with the “.akira” extension and demanded Bitcoin payments, applying double extortion by pressuring victims through data leaks. This was a simple yet effective ransomware attack that has breached many SMBs.

•**Impact:** In January 2024, Akira ransomware had compromised more than 250 organizations and claimed approximately \$42 million in ransomware proceeds. The attacks exposed vulnerabilities among SMBs, as generally, the lack of resources makes it impossible to defend against advanced ransomware threats and reduce financial impact.

PHISHING ATTACKS

Phishing is a social engineering scam whereby intruders seek access to your personal information or passwords by posing as a real business or organization with a legitimate reason to request information.

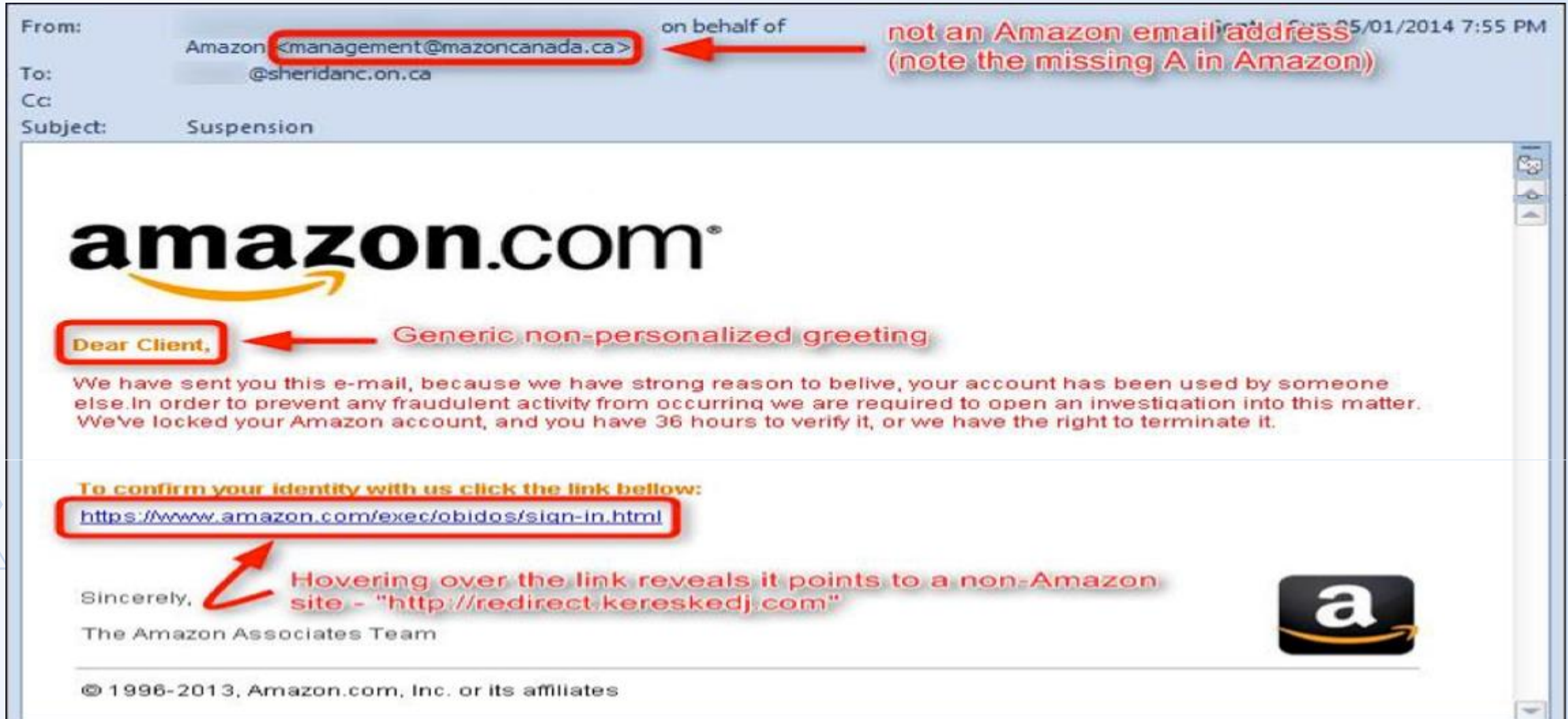
Example of Phishing email :

Phishing emails (or texts) quite often alert you to a problem with your account and asks you to click on a link and provide information to correct the situation. These emails look real and often contain the organization's logo and trademark. The URL in the email resembles the authentic web address.

For example, **"Amazons.com"**



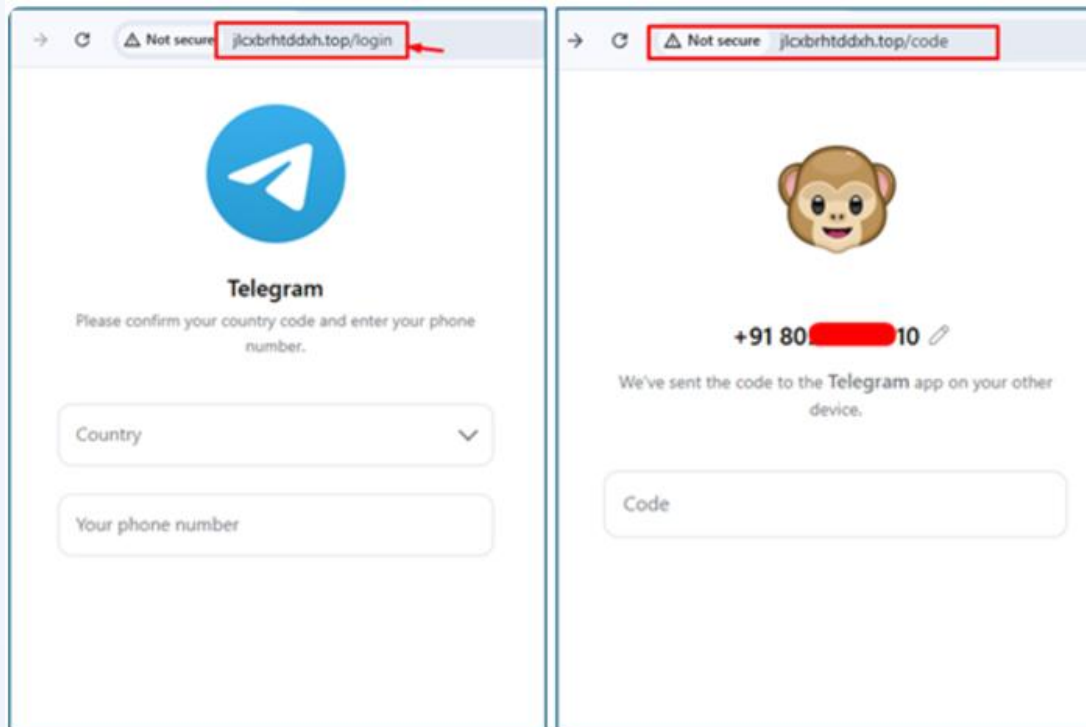
PHISHING ATTACKS



PHISHING ATTACKS

Description: This attack involved the use of phishing links disguised as Telegram login pages, aimed at harvesting user credentials such as mobile number, OTP, and 2FA passwords.

Mass Telegram account hijacking
via supply-chain phishing campaign



PHISHING ATTACKS

1. Phishing Link Distribution:

- The attacker sends an initial phishing message with a link, appearing to be from Telegram to the victim. The message may say, "There are your photos and videos in it: <http://lbvamvemkxfi.top/login>".
- The link directs the victim to a fake Telegram login page designed to steal credentials, OTPs, and passwords.



2. Credential Harvesting:

- Once the victim enters their credentials, they are harvested by the attacker in real time.
- The attacker immediately uses the stolen credentials to hijack the victim's Telegram account and then sends a similar phishing message from the compromised account to the victim's entire contact list.

Software Development Life Cycle

- ❑ A framework that describes the activities performed at each stage of a software development project.
- ❑ SDLC process is used by the software industry to design, develop and test high quality software. It aims to produce the quality that meets, is secure and meets customer expectations.

Software Development Life Cycle (SDLC) Phases

- ☐ Planning and Requirements Analysis
- ☐ Defining Requirements
- ☐ Designing the Software
- ☐ Building or Developing the Software
- ☐ Testing the Software
- ☐ Deployment and Maintenance

Secure SDLC

Usual Mistakes:

1. Not Integrating Security into the SDLC:

- Failing to incorporate security measures throughout the development lifecycle can leave applications vulnerable to attacks.

2. Ignoring Threat Modeling:

- Overlooking threat modeling can result in unaddressed security risks and potential vulnerabilities in the application.



Secure SDLC

How to Avoid:

1. Integrate Security at Every Phase:

- Ensure that security is a fundamental part of every phase of the SDLC, from planning and design to implementation, testing, and maintenance.

2. Conduct Threat Modeling and Risk Assessments:

- Regularly perform threat modeling and risk assessments to identify and mitigate potential security threats early in the development process.

3. Implement Continuous Security Testing:

- Use continuous security testing practices, such as static and dynamic analysis, to detect and address vulnerabilities throughout the development lifecycle.



Secure SDLC

SolarWinds Supply Chain Attack in 2020

Incident: In 2020, the SolarWinds supply chain attack highlighted significant vulnerabilities in the SDLC, where attackers inserted malicious code into the Orion software updates.

Sequence of Events:

- **Supply Chain Compromise:** Attackers gained access to SolarWinds' build system and injected malicious code into the Orion software updates, which were then distributed to thousands of customers.
- **Widespread Impact:** The compromised updates were installed by numerous organizations, including government agencies and large enterprises, leading to widespread data breaches and unauthorized access.

Secure SDLC

SolarWinds Supply Chain Attack in 2020

Impact:

- **Data Exposed:** The breach exposed sensitive information from numerous organizations, leading to potential data misuse and security risks.
- **Financial and Reputational Damage:** SolarWinds and its affected customers faced significant financial and reputational damage, including loss of client trust and potential regulatory scrutiny.

TAKEAWAYS: DO'S

- ☐ Lock your computer and documents every time you leave your desk
- ☐ Always carry your access badge and use it to enter the office premises
- ☐ Choose a password that is easy for you to remember but difficult for someone else to guess
- ☐ Be vigilant and report incidents
- ☐ Read information security related emails and guidelines
- ☐ Know whom to call in an emergency
- ☐ Be aware of employee safety measures
- ☐ During a crisis, give priority to personnel safety and evacuate the building

TAKEAWAYS: DONT'S

- ☐ Publish any sensitive (confidential or private) information on the Internet
- ☐ Talk to media during a crisis. If asked, simply say "No comment"
- ☐ Be negligent in your role in implementing an effective ISMS at EFR.
- ☐ Leave your laptop or cell phone unattended in your car or elsewhere
- ☐ Spread rumors or trust any information from unreliable sources

RESPONSIBILITY AGREEMENT

INFORMATION SECURITY AND COMPLIANCE RESPONSIBILITY AGREEMENT STATEMENT OF ACKNOWLEDGMENT

I have completed EFR Information Security awareness training, including reviewing the Policy governing the Services provided by EFR. I understand it is my responsibility to read and become familiar with the EFR policies and related procedures.

I acknowledge that it is my duty to follow all the security access procedures related to information and data associated with EFR and its clients. I agree that physical security and information security begin with me.

I understand that violation of the security & compliance responsibility agreement may result in disciplinary action up to and including termination of my employment.

Note : By reading and understanding this course as complete, you are accepting this Statement of Acknowledgment.

Thank You!