**Information Security Awareness**

**By:** Oluwabunmi Olanrewaju

COMP 249-001 – Information Security, Privacy and Ethic

Table of Contents

[General Overview: 3](#_Toc5618622)

[Key Definitions: 3](#_Toc5618623)

[Information security 3](#_Toc5618624)

[Information Security Awareness 4](#_Toc5618625)

[Information Security Policies (ISP) 4](#_Toc5618626)

[Important of Information Security Awareness 5](#_Toc5618627)

[Types of Security Threats 5](#_Toc5618628)

[ Natural 5](#_Toc5618629)

[ Unintentional 5](#_Toc5618630)

[ Intentional 5](#_Toc5618631)

[Threat Analysis Base on 2018 Data Breach 7](#_Toc5618632)

[Notable incidents 8](#_Toc5618633)

[Best Practices in Securing Information 10](#_Toc5618634)

[Safe email practice 10](#_Toc5618635)

[Physical Security 10](#_Toc5618636)

[Securing your computer 10](#_Toc5618637)

[Passwords 10](#_Toc5618638)

[Protecting Verbal Communication 11](#_Toc5618639)

[Safe Internet and Social Networking Usage 11](#_Toc5618640)

[Incident Response 11](#_Toc5618641)

[Consequences of Security Violations on the part of the user 12](#_Toc5618642)

[Standards and regulations requirements 12](#_Toc5618643)

[Summary 12](#_Toc5618644)

# **General Overview:**

Statistics base on percentage of security incidents generated from inside an organization suggest that internal users are responsible for at least around 70 per cent, and that most of these incidents are the result of user error, mishap and ignorance. The statistics have remained reasonably consistent over a number of years. Many of these incidents could have been prevented by improved understanding and by changes in attitude to information security.

Bill Gardner and Valerie Thomas also stated that the most vulnerable part of your network is the people who use it. No matter how much money and effort you’ve expended implementing technology-based defences, one ill-judged click can be your undoing (4).

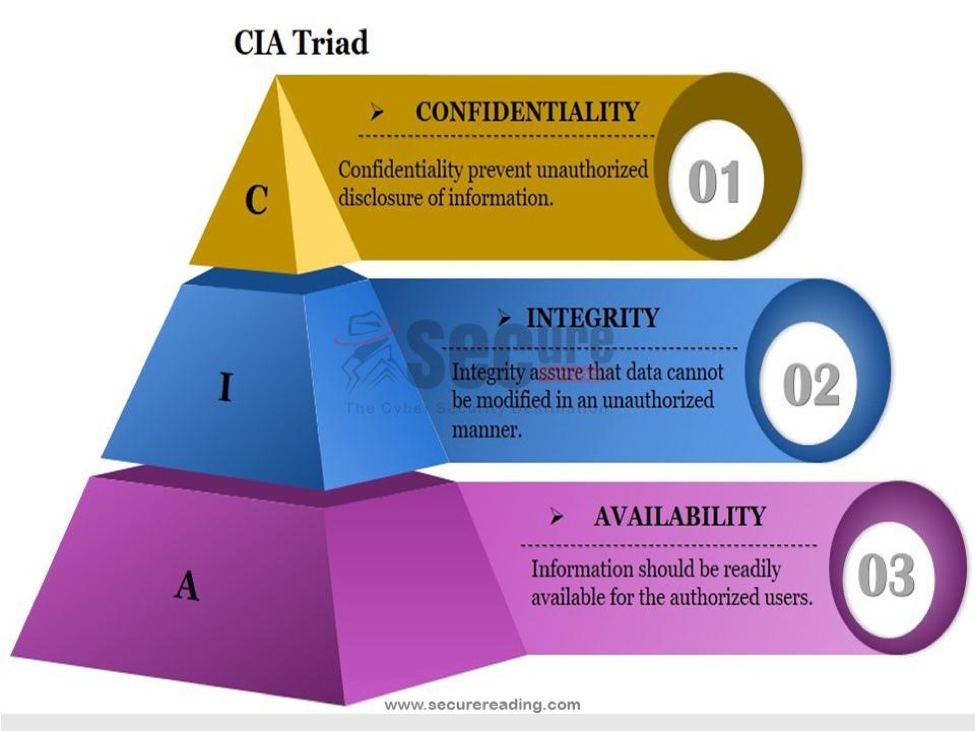
Security apathy and ignorance are the biggest threats to information networks and the best way to achieve a significant and lasting improvement in computer security is not only by throwing more technical solutions at the problem but it’s by raising awareness and training and educating all computer users in the basics of computer security (Mcllwraith).

# **Key Definitions:**

## **Information security**

Information Security is the protection of information and systems from unauthorized access, modification, disclosure, disruption or destruction. Major objectives of Information security include:

* **Confidentiality**
* **Integrity**
* **Availability**



## **Information Security Awareness**

Information security awareness is a fundamental part of effective security management, it is a formal process of training and educating users about information protection. Information security awareness involves:

* Programs to educate all users about potential threats to an organization's information and taking reasonable steps to guard against such threats.
* Individual responsibility for company security policies.
* Measures to audit these efforts.

**Who are the Users?**

* Management
* Shareholders/ Owners
* Employees
* Business partners
* Contractors
* Customers / Clients
* Regulators etc.

## **Information Security Policies (ISP)**

The information security policy defines the management, personnel and technology structure of the information security awareness program. The main purpose of ISP is to provide a set of rules for all users / networks of the IT structure within the organization’s domain to abide by. ISP covers areas such as system access control, information access, passwords policies etc.

# **Important of Information Security Awareness**

* Regulatory Requirements Compliance
* Due Diligence
* Ensure Accountability
* Corporate Reputation

# **Types of Security Threats**

Threats can be object, person or other entity that represents constant danger to information asset and there are there categories namely:

* Natural (such as fire, flood, lightening, Tornado, Power failures)
* Unintentional: actions that occur due to lack of knowledge or carelessness
* Intentional: Threats that are deliberately designed to harm or manipulate an information system, its software and/or data.

Some threats an attacker can use to infiltrate a company network include:

**Malware**

Short for Malicious Software, malware is any code that can be used to steal data, bypass access controls, or cause harm to, or compromise a system.



* **Virus** is a computer program than can copy itself by modifying other computer programs and inserting its own code.
* **Worms** are malicious codes that replicate themselves by independently exploiting vulnerabilities in networks. virus requires a host program to run, worms can run by themselves.
* **Spyware –** This malware is design to track and spy on the user. Spyware often includes activity trackers, keystroke collection, and data capture. Example is a keylogger.
* **Adware –** Advertising supported software is designed to automatically deliver advertisements such as miracle weight loss programs, offers for get-rich-quick secrets, and bogus virus warnings that invite your click. Also, you might experience new tabs opening, a change in your home page, findings from a search engine you never heard of.
* **Rootkit –** This malware is designed to modify the operating system to create a backdoor. Attackers then use the backdoor to access the computer remotely. Most rootkits take advantage of software vulnerabilities to perform privilege escalation and modify system files. It is also common for rootkits to modify system forensics and monitoring tools, making them very hard to detect.
* **Trojan horse -**A Trojan horse is malware that carries out malicious operations under the guise of a desired operation. This malicious code exploits the privileges of the user that runs it. A Trojan horse differs from a virus because it binds itself to non-executable files.

**Symptoms of Malware**

Regardless of the type of malware a system has been infected with, these are common malware symptoms:

* There is an increase in CPU usage.
* There is a decrease in computer speed or computer freezes or crashes often.
* There is a decrease in Web browsing speed.
* There are unexplainable problems with network connections.
* Files are modified or deleted
* There is a presence of unknown files, programs, or desktop icons.
* There are unknown processes running.
* Programs are turning off or reconfiguring themselves.
* Email is being sent without the user’s knowledge or consent.

**Social Engineering**

Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information.

**Types of social engineering attacks:**

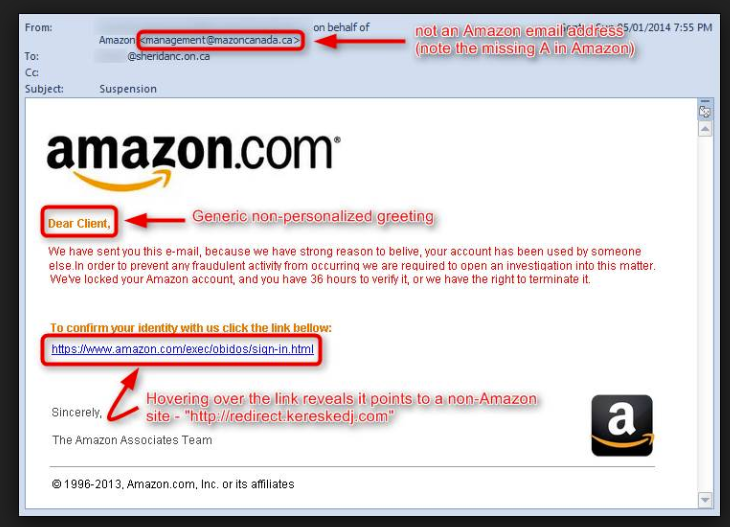
**Pretexting -** This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data. An example involves an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

**Tailgating** - This is when an attacker quickly follows an authorized person into a secure location

**Something for Something -** This is when an attacker requests personal information from An individual in exchange for something, like a free gift.

**Phishing**

Phishing is when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source. The message intent is to trick the recipient into installing malware on their device, or into sharing personal or financial information. An example of phishing is an email forged to look like it was sent by a retail store asking the user to click a link to claim a prize. The link may go to a fake site asking for personal information, or it may install a virus.



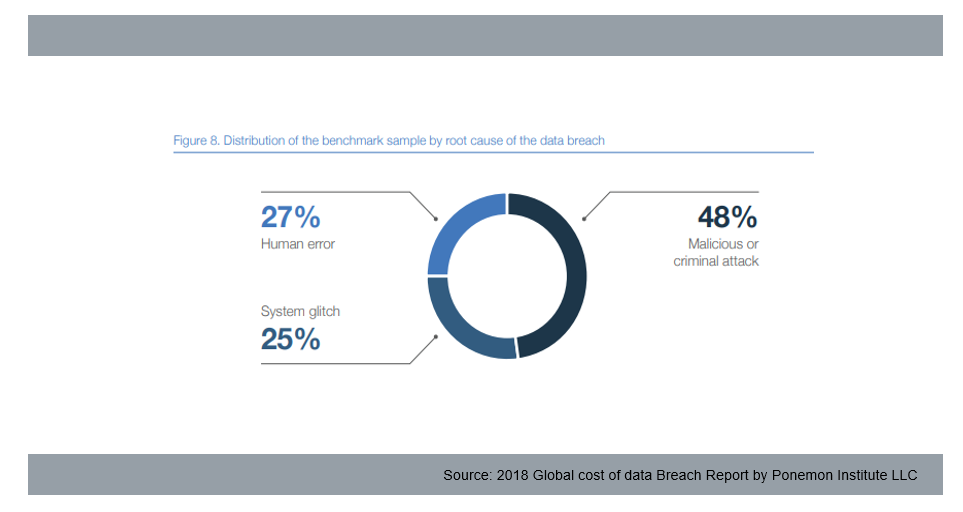
**Hacking**

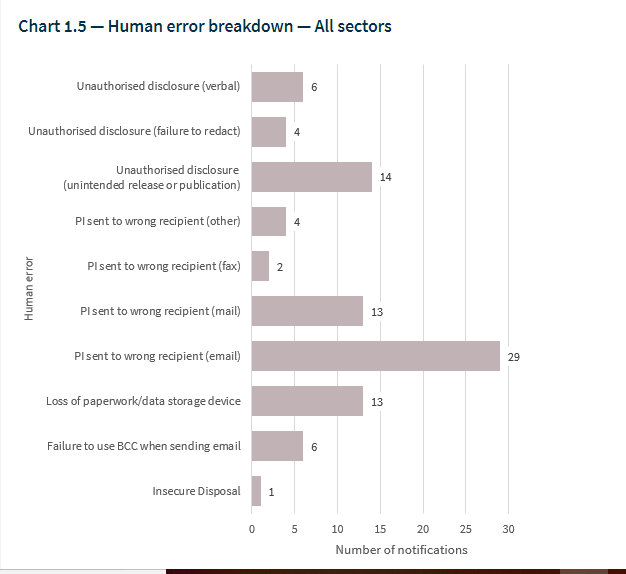
It is a term used to describe actions taken by someone to gain unauthorized access to a computer.

**Spam**

It is the use of messaging systems to send an unsolicited message, especially advertising.

**Threat Analysis Base on 2018 Data Breach**





## **Notable incidents**

1. **US Universities:** In March 2018, Department of Justice indicted nine Iranian hackers that infiltrated 144 US universities, 176 universities in 21 other countries, 47 private companies, and other targets like the United Nations, the US Federal Energy Regulatory Commission, and the states of Hawaii and Indiana. The attacks used carefully crafted spear phishing emails to trick professors and other university affiliates into clicking on malicious links and entering their network login credentials.
2. **eBay:** in 2014, a group of attackers leveraged phishing attacks to steal the credentials of as many as 100 eBay employees. They used that information to gain access to eBay's internal network.
3. **BlackRock Inc.:** earlier in the year, a user at BlackRock accidentally posted spreadsheets of sales information to a public part of the website.

# **Best Practices in Securing Information**

## **Safe email practice**

* Do not open email attachment unless you are sure what they are
* Delete spam or suspicious emails, do not open, forward or reply them
* Be mindful of phishing emails asking for personal or sensitive information

## **Physical Security**

* Physically secure all mobile devices at all times: lock them up securely before you step away
* In shared printer areas, immediately remove all sensitive documents from equipment.
* Use a paper shredder or secure shred bin when throwing out personal or sensitive information.
* Clear desk of papers including sticky notes and papers that contain sensitive information.
* Set up your workstation so that unauthorized people and passers-by cannot see sensitive information on your monitor.
* Securely delete all contents of computers and mobile devices, before discarding, exchanging, selling or donating them.

## **Securing your computer**

* Enable automatic software updates where available
* Install and update antivirus software
* Install and configure firewall software
* Do not automatically connect to public wireless networks
* Disconnect your computer from the wireless network when it is not in use
* Use caution when downloading and installing software
* Lock your computer when it is unattended

## **Passwords**

* Do not reveal your passwords to anyone
* Avoid writing your passwords down.
* Change default passwords the first time you log in.
* Avoid using the same password for all devices.
* Change password immediately if you discover someone's aware of it.
* Use strong, unique passwords using the following guidelines:
  + Use passwords that are more than 8 characters in length.
  + Use a combination of upper and lowercase letters, numbers, and special characters in passwords.
  + Avoid using common words such as password or administrator, or know facts such as pet names or date of birth etc.

## **Protecting Verbal Communication**

* Be mindful of your surroundings when discussing Restricted data
* Do not discuss Restricted data with individuals who do not have a need to know

## **Safe Internet and Social Networking Usage**

* Do not reveal personal details or confidential information online.
* If any web or Social Media content looks suspicious in any way, close your browser and do not return to that page.
* Avoid using the same passwords for web sites that you use to access company system.
* Do not click on links in pop-up ads/windows; Use your web browser’s pop-up blocker, if it has one, to help prevent these ads from getting through.
* When visiting a website, look for the lock in the browser address to ensure that the site is SSL (Secure Sockets Layer) encrypted

## **Incident Response**

An Information Security Incident is an adverse event in an information system that poses a threat to computer or network security in respect of availability, integrity and confidentiality. Example include:

* Direct loss or theft of Classified Information (e.g. papers taken from car, post intercepted, unauthorized download)
* Loss or theft of equipment used to store Classified Information (e.g. laptop, smartphone, USB stick)
* Corruption or unauthorized modification of vital records (e.g. alteration of master records)
* Computer system or equipment compromise (e.g. virus, malware, denial of service attack)
* Compromised IT user account (e.g. spoofing, hacking, shared password)
* Break in at a location holding critical information processing equipment such as servers

Promptly notify the appropriate staff if you become aware of a possible security incident

# **Consequences of Security Violations on the part of the user**

* Loss of personal and confidential information
* Loss of trust in the user and sometimes can leads to embarrassment of bad reputation
* In a situation of compromise of sensitive information, it can lead to bad reporting
* Disciplinary action which might include penalties, termination of employment or lawsuits

# **Standards and regulations requirements**

* **ISO/IEC 27001 and 27002**

8.2.2: All employees of the organization and, where relevant, contractors and third-party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

* **PCI DSS 12.6:**
* Make all employees aware of the importance of cardholder information security.
* Educate employees (for example, through posters, letters, memos, meetings, and promotions).
* Require employees to acknowledge in writing that they have read and understand the company’s security policy and procedures. In a situation of compromise of sensitive information, it can lead to bad reporting
* **CobiT**

PO7.4 Personnel Training: Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls, and security awareness at the level required to achieve organizational goals.

# **Summary**

Nowadays, attackers are now turning to more targeted attacks focused on tricking users into clicking links or opening attachments in order to gain access to company’s network, so it is necessary that all users are educated on best practices in ensuring information security so that they are not the weak link.

Articles:

* Building an Information Security Awareness (1st Edition) by Bill Gardner and Valerie Thomas. Published by Syngress.
* Information Security and Employee Behaviour How to Reduce Risk Through Employee Education, Training and Awareness by ANGUS McILWRAITH
* [https://resources.infosecinstitute.com](https://resources.infosecinstitute.com/)
* CISCO Networking Academy
* <https://www.wired.com/story/2018-worst-hacks-so-far/>
* <https://www.farmprogress.com/technology/3-ways-prevent-russian-hacking>
* <https://www.augustadatastorage.com/know-cost-data-breach-2018/>
* <https://www.powershow.com/view0/786844-YjAwY/Employee_Information_Security_Awareness_Training_powerpoint_ppt_presentation>
* <https://www.slideserve.com/gaetan/it-security-awareness-information-security-is-everyone-s-business>
* <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/notifiable-data-breaches-quarterly-statistics-report-1-july-30-september-2018>