**BUSINESS CONTINUITY PLAN (BCP) AND DISASTER RECOVERY**

**PLAN (DRP)**

**To 10 Domains of the Information Security CBK**

1. Physical Security
2. Access Control
3. Operations Control
4. **Business Continuity and Disaster Recovery Planning Domain**
5. **Information Security Governance and Risk Management**
6. Cryptography
7. Security Architecture and Design
8. Telecommunications and Network Security
9. Software Development Security
10. Legal, Regulation, Investigations, and Compliance

**Disaster -** is an **event**, often **unexpected**, that **seriously disrupts your usual operations or processes** and can have a **long-term impact** on your

the normal way of life or that of your

**organization.**

**Events that will disrupt your IT operations:**

**Natural –** fire, earthquake, flood, tsunami, cyclone, lightning, etc.

• Man-made

*–Non-intentional:* negligence, human error

*– Intentional:* hacking, phishing, theft, DDOS, strikes, work stoppages, sabotage, burglary

**• Environmental –** power failure/ disruption, water leaks, high heat and humidity

**Types of Incidents**

* **Negligible** – short power/ Internet outage
* **Minor -** brownout
* **Major** – frequent/long brownouts, damaged laptop
* **Crisis –** theft, unrepairable laptop, head crash, floods



**The Business Continuity Plan (BCP)**

deals with **business management concerns,** which include:

– How to **prepare** for an **event/ disaster/ emergency/ calamity?**

– How to **respond** and continue **operations?**

• It *describes* the **critical processes, procedures**, and **personnel** that must be **protected**

• it *outlines* **the potential impact of disaster** situations to business operations or **Business Impact Analysis (BIA)**

• It ***creates*** policies that respond to various situations to **ensure a business** is able to **recover quickly** after a crisis.

**Goal: To protect people, property and assets.**

**Importance of the BCP**

• **Reduce the risk** to the business

• **Save time, money,** and stress

• **Maintain** a steady flow of **income**

• **Protect lives**

• **Minimize** disruptions

• **Avoid legal problem**s **– business responsibilities** are *not limited within the organization*, they are also liable to their investors, government agencies, and other stakeholders

• **Damage** to market share, **reputation** or brand (“It takes

many good deeds to build a good reputation, and only one bad one to lose it” – Benjamin Franklin)

• Failure to **protect the company assets** including intellectual properties and personnel

**The BCP Process**

• **Identify the scope** and **boundaries** of the BCP

* **Communicate** the plan
* **identify the critical aspects** that should be included in the plan
* **Audit analysis of the assets** (e.g. people, facilities, applications, IT systems)
* **Conduct risk analysis** that identifies the **type of threats**, both man-made, natural, and environmental

• **Prioritize the processes** and assign a value to each

* **IT facilities/ services** at the ICU in the hospital
* Identify **which services should be restored** withinan hour, day, week

• **Create a Business Impact Assessment (BIA)**

* Measures the operating and financial loss
* Determine the cost of continuous operation and value to each service

• Get the **Management Approval & Support (financial)**

**– Define the roles** of engagement

**– Identify** roles and **responsibilities** of the team

– Establish means of **communication and the mechanism** for **tracking progress**

• Awareness

– Train each **department to understand** its role in the plan and support and maintain it

• Plan Implementation

– **Training, testing**, and **review and support**

**The Business Impact Analysis (BIA)**

* **Identify the risks** that specific threats may cause to the business,
* **Quantify the risks**
* **Establish priorities**
  + Determine **how long each process can be down** before business continuity is seriously compromised
* **Performs Cost-Benefit-Analysis (CBA)** for countering risks
  + **Identify the resources** needed to support the critical process
  + **What equipment,** and **which people are needed**
  + **How much will it cost** to **maintain critical system?**

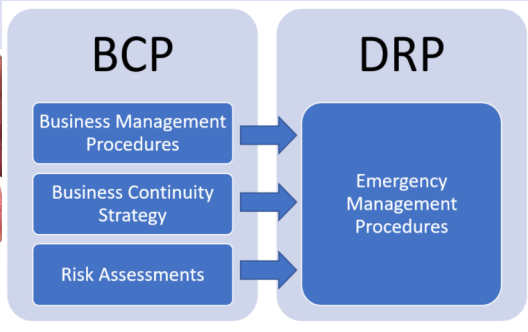
**• Critical step in developing the business continuity plan**

**Three main questions to consider during BIA phase:**

1. What are the **different business processes**?
2. What are the **critical information resources** related to an organization’s **critical business processes?**
3. What is the **critical recovery time period** for information resources in which business processing must be resumed before significant or unacceptable losses are suffered?

**The Disaster Recovery Plan (DRP)**

* describes **the exact steps** and **procedures,** that **personnel** (e.g. ITO) handling **critical operations,** must follow in order to **recover critical business** systems **in the event of a disaster**.
* Objective: To **ensure that an organization** can **respond to a disaster** or other emergency that **affects information systems** and minimize the effect on **business operations.**
* **Purpose:** To **comprehensively explain** the consistent **actions that must be taken before,** during, and after a natural or man-made **disaster** so that the entire team can take those actions

****

**Goals of the DRP**

• **Keep** the computers running

• **Meeting** **formal and informal service-level** agreements with customers and suppliers

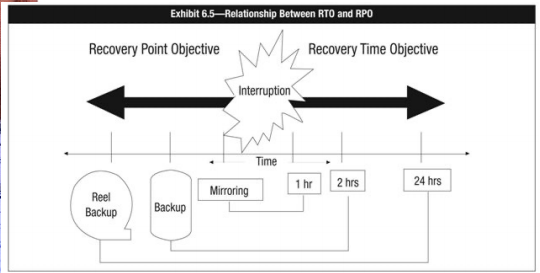
• Being proactive instead of reactive.

– DRP **should include a** **comprehensive list** of **activities** to **perform through practice runs** to **ensure** that responsible **people can respond**

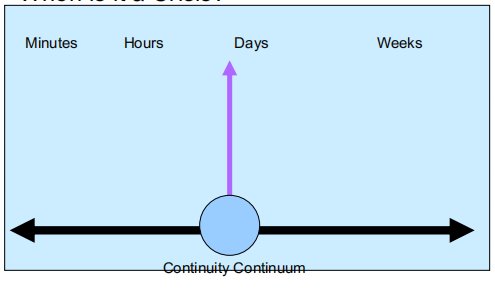
**appropriately**

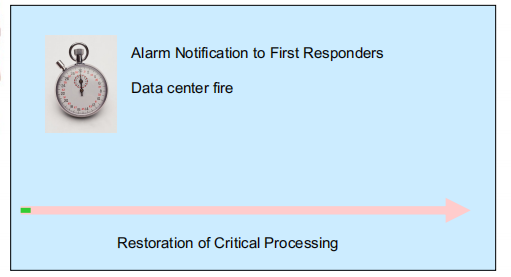
**Recovery Point Objective and Time Objective**

* **Recovery Point Objective (RPO)**
  + Based on **acceptable data loss**
  + Indicates the **earliest point in time** in which it is **acceptable to recover the data**
* **Recovery Time Objective (RTO)**
  + Based **on acceptable downtime**
  + Indicates **earliest point in time** at which the **business operations must resume** **after a disaster**

\ dd

**When is it a Crisis?**

****

**Restoration of Critical Processing**

* **Alarm Notification** to First Responders
* **Data Fire Center**
* **Activate** Emergency Operations Center
* IT decision to **move a backup facility**
* **Assemble IT recovery** at **appropriate sites**
* **Obtain backup tapes** form off – premises storage
* **Acquire** and **install back-up hardware** and **network connections**
* **Restore Operating System** and **Network**
* **Reload database** and other data
* **Restore Critical Applications**
* **Begin Critical Processing** –

(Recovery Time Objective RTO)

**Recovery Strategies**

* A **recovery strategy** is a combination of **preventive, detective, and corrective measures**
* Recovery strategy would **depend upon:**

– The **criticality of the business** process and the

**applications** supporting the processes

**– Cost**

– **Time required** to **recover**

**– Security**

**Recovery strategies** based on the **risk level identified** for **recovery** would include developing:

**• Share—agreement**

**• Hot sites**

**• Warm sites**

**• Cold sites**

**• Duplicate information processing facilities**

**• Mobile sites**

**• Reciprocal arrangements with other organizations**

**Type of backup facilities**

* **Shared-site agreement**
* **Arrangements between companies** with **similar data**
* **processing centers** (e.g. UPD & UPMin, UPMin & college)
* **Both companies (A & B)** agreed to **share resources in the event of a disaster**
  + **Compatibility** in **hardware, software and services**
  + **Less costly, faster to implement**
  + Done with **a written/ legal document**
  + **Issues:** data security, privacy protection & data synchronization

**Type of backup facilities**

* **Alternate Site**
  + The **company hires the services** of the **3rd party vendor** to **provide the backup services**

**• Categories of Alternate Sites**

**– Hot sites**

» The 3rd party

• **assumes** the **responsibility to backup the computing**

services (e.g. hosting the application and data) **of the**

**customer**

• Assumes all **responsibility for processing transactions** for the customer

• **Maintain the facility** including all **environmental controls** such as heating, cooling, power;

**• hardware (e.g. printers, servers)**

• Data backups

• Other services

**Cold Site**

**» Power, cooling, heating** (3rd party vendor)

» **hardware** or **software** (c/o customer)

**» Cheaper** than the warm site

**– Warm site**

» A **compromise** between the **warm and cold sites**

» Provides **building and environmental services** + **hardware** and **communication links**

» **Software installations** and **workstations (c/o customers)**

» **Restoration** from backup (c/o customer)

**Type of backup facilities**

* + **Additional Arrangements**
  + **Multiple centers**
  + Processing is distributed in multiple sites
  + Improves processing speed
  + Offers redundancy
  + Downside: **burdensome and costly**
    - Service bureaus
  + Provide **backup processing services** at a **remote location**
  + Perform **other services (IaaS, SaaS, PaaS)**
    - Mobile Units
  + Vendor provides a **data processing center** on wheels (**with AC and power systems)**

**Testing DRP**

* **Necessary and non-negotiable** (e.g. earthquake drill, fire drill)

Methods

* **Walk-throughs** 
  + Members of the key business units meet **to trace their steps through plan**, looking for omissions and inaccuracies
* **Simulations**
  + **Perform a dry run**
* **Checklists**
  + **Members of key units/ office check** off the tasks for which they are **responsible and report in te accuracy** of the checklist
* **Parallel Testing**
* **Full interruption**
  + **Production systems** are **stopped** as if a disaster has occurred
  + **Evaluate the performance** of the backup services

**DRP Characteristics**

* + - **It’s practical** – include **useful information**
    - It’s **understandabl**e – test **instructions** before **implementing them**
    - It’s **accessible** – give **copies** to all concerned players
    - It’s **kept current** – revise **document a**s needed

**Development of Business Continuity Plan**

**(BCP) and Disaster Recovery Plan (DRP)**

The **emergency management team** coordinates the

activities of all other recovery teams. It oversees:

• **Retrieving critical** and **vital data** from offsite storage

• I**nstalling** and **testing systems software** and **applications at the**

systems recovery

• **Identifying, purchasing, and installing** hardware at the systemrecovery site

• **Operating** from the **system recovery site**

• **Rerouting network** communications traffic

**The emergency management team coordinates the**

**activities of all other recovery teams. It oversees:**

• Reestablishing the user/system network

• **Transporting** users to the **recovery facility**

• **Reconstructing** databases

• **Supplying** necessary office goods, i.e., **special forms, check** stock, paper

• **Arranging** and **paying for employee relocation** expenses at the recovery facility

• **Coordinating systems** use and **employee work schedules**

**Other Issues in Plan Development**

* **Management** and **user involvement is vital** to

the success of BCP

**– Essential to the identification** of **critical systems**,

recovery times and resources

– **Involvement from support services, business**

operations and information processing support

• **Entire organization needs** to be **considered**

**for BCP**

**Components of a BCP**

A **business continuity plan** may consist of

**more than one plan document**

• Continuity of operations plan (COOP)

• Disaster recovery plan (DRP)

• Business resumption plan

• Continuity of support plan / IT contingency plan

• Crisis communications plan

• Incident response plan

• Transportation plan

• Occupant emergency plan (OEP)

• Key decision-making personnel

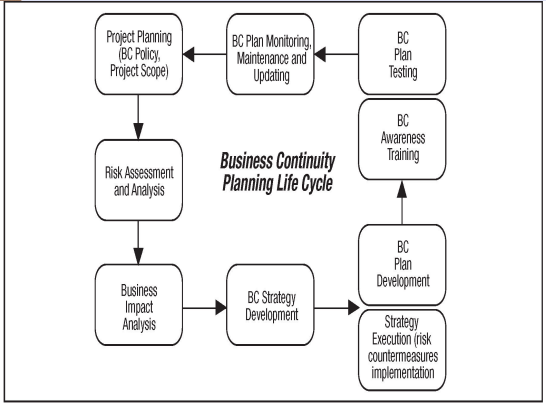
• Backup of required supplies

• Telecommunication networks disaster recovery

methods

• Redundant array of inexpensive disks (RAID)

• Insurance



**INFORMATION SECURITY GOVERNANCE AND RISK MANAGEMENT** (Common Body of Knowledge)

educause.edu:

- it is the **system** by which an organization **directs and controls IT security.**

- Governance specifies the **accountability framework** and **provides oversight** to ensure that risks are adequately mitigated, while management ensures that **controls** are implemented to mitigate risks.

- Management recommends security strategies.

- Governance ensures that **security strategies are aligned with business objectives** and consistent with regulations.

**What is information security governance?**

§ **Leadership**

§ organizational structures and processes

§ It is an enterprise matter and should be part of the **core**

**functions** and **priority areas** of any organizations

§ ensure that all the security elements are put in place to **protect your data environment** work efficiently, accomplish what is intended, and do so cost-effectively.

§ Processes to carry out what is intended by the leadership

**Importance of InfoSec Gov**

§ Provides the **ability to conduct secure business operations** in an interconnected world

§ Ensures that **security resources** are **well spent**

§ Gains **institutional respect**

§ Provides a **framework for secure business operations** in an interconnected world

§ Ensure that **IT investments and resources** are aligned with **the business objectives and goals**

**Benefits that can be gained of Infosec Governance**

§ **Fewer breaches** to deal **with/increased efficiency**

§ **More effective** use of resources

§ Secured information

§ **Clear policies**

§ Makes everyone careful in their activities

**How does it work?**

**Information Sec Governance** includes a **broad set of executive and management activities** that define an IT **security program.** A program is an ongoing

management activity that is **constantly funded and intended** for the **preservation and advancement** of the organization.

**Program-> Policies -> Standards -> Guidelines- > Procedures**

**Structure of Policy**

* Title
  + Purpose
  + Authorizing individual
  + Author/sponsor
  + Reference to other policies: Laws (Intl or National), DPA, Ecommerce
  + Scope
  + Measurement expectations
  + Exception process
  + Accountability
  + Compliance management and measurement descriptions
  + Effective/ expiration dates
  + Definitions

Four Types of Policies

**Program-level policy or Information Security Charter**

• Used for creating a **management-sponsored** computer security program

• it is like a mission statement for the IT security program

• Assign **program management responsibilities**, state an organization-wide computer security purpose and objectives, and establish a basis for policy compliance

• Defines the purpose, scope

**Program-framework policy**

• Establishes the overall **approach to computer security**

• It adds detail to the program by describing the elements and organization of the program

and **department** that will carry out the security mission

**Issue-specific policy**

• Addresses specific issues of concern to the organization

**System-specific policy**

• Focuses on policy issues that management has decided for a specific system

**Program -Level Policies**

* Purpose

• Authorizing individual

• Author/sponsor

• Reference to other policies

• Scope

• Measurement expectations

• Exception process

• Accountability

• Compliance management and measurement descriptions

• Effective/expiration dates

• Definitions

**Program -framework policy**

* Provide an **organization-wide direction** for broad areas of the program implementation

• This is to **assure** that **everyone complies with acceptable use rules** (e.g. email, Internet, etc)

• It reflects **IT management’s decisions** about **priorities for protection, resource** allocation and assignment of responsibilities

• It can be in a form of a **handbook**

• Possible program-framework policies include:

• **Business Continuity Planning (BCP) framework**

**• Physical Security Requirements Framework for Data Center**

**• Application Development Security Framework**

**Issue Specific policy**

**•** Issue statement

• Statement of the organization’s position

• Applicability

• Roles and responsibilities

• Compliance

• Points of contact and supplementary information

**System- specific policy**

* Who is **allowed to read/modify data** in the system?

• What **conditions c**an data be read/modified?

• Are users allowed to dial into the computer system from home while on travel?



**Development and Management of Security Policies**

**Security Objectives**

– **CIA** and all associated concepts like **controls,** authentication**, etc.**

- must be **specific and concrete**

- consist of a **series of statements**

**Operational Security**

• authorized and unauthorized modification:

• who (by job category, name, or organizational placement)

• can do what (modify, read, write, delete) to

• which data (fields or records) under what conditions

**Policy implementation** -- technical and management methods

**Policy Support Documents**

**Regulations**

* Federal Trade Commission
* FDA
* **Data Privacy Act RA 10173**
* General Data Protection Regulation (GDPR)
* Info Systems Audit and Control Association (ISACA)

**Standard and Baselines**

* **Reuse** what people have **found to be best** practices
* **Standard** refers to **specific security** requirements, or what is needed for a system or process to be considered secure.
* Example **is password standard –** requirements for p/w creation distribution, use, changing, revocation
* Baselines – set of **requirements for** a technology implementation
* Baseline and standards are the enforceable elements in the security program
* Auditors check if baseline and standards comply

**Guidelines**

**Guidelines,** guidance documents, or advisories provide the people who need to implement a standard or baseline with more detailed information and guidance (hints, tips, price advice, advise and so forth) to aid in compliance

**Procedures**

Detailed **step-by-step activities that are followed** to implement a prices sir configure a system for compliance to a guideline

**Suggested taxonomy**

• Asset and data classification

• Separation of duties

• Pre-employment hiring practices

• Risk analysis and management

• Education, awareness, and training

**Law, Investigations and Ethics**

**InfoSec specialists** should **keep up with the latest laws, code of ethics,** and other rules governing the use of IT because this will **enable them to respond accordingly** and **appropriately or LEGALLY.**

are duty-bound to their employers, the public/ government, and other governing bodies such as the Philippines’ **National Privacy Commission (NPC)** (e.g. in the event of a breach that causes the loss of private data).

**Philippines’ laws that are related to Information security;**

d) The reproduction and communication to the public of literary, scientific or artistic works as

part of reports of current events by means of photography, cinematography or broadcasting

to the extent necessary for the purpose; (Sec. 12, P. D. No. 49)

e) The inclusion of a work in a publication,…. if such inclusion is made by way of illustration for

teaching purposes and is compatible with fair use: Provided, That the source and of the

name of the author, if appearing in the work, are mentioned;

f) ..

g) ..

h) The use made of a work by or under the direction or control of the Government, by the

National Library or by educational, scientific or professional institutions where such use is in

the public interest and is compatible with fair use;

i) …

j) …

k) Any use made of a work for the purpose of any judicial proceedings or for the giving of

professional advice by a legal practitioner.

CHAPTER VIII. LIMITATIONS ON COPYRIGHT

Sec. 185. Fair Use of a Copyrighted Work.

185.1. The fair use of a copyrighted work for criticism, comment, news reporting,

teaching including multiple copies for classroom use, scholarship, research,

and similar purposes is not an infringement of copyright. Decompilation,

which is understood here to be the reproduction of the code and translation of the

forms of the computer program to achieve the inter-operability of an independently

created computer program with other programs may also constitute fair use.

*Factors to be considered in determining whether the use made of a work is fair use:*

1. The purpose and character of the use, including whether such use is of a

commercial nature or is for non-profit education purposes;

2. The nature of the copyrighted work;

3. The amount and substantiality of the portion used in relation to the copyrighted

work as a whole; and

4. The effect of the use upon the potential market for or value of the copyrighted

work.

CHAPTER VIII. LIMITATIONS ON COPYRIGHT

Sec. 186. Work of Architecture. - Copyright in a work of architecture shall include the

right to control the erection of any building which reproduces the whole or a substantial part

of the work either in its original form or in any form recognizably derived from the original;

Provided, That the copyright in any such work shall not include the right to control the

reconstruction or rehabilitation in the same style as the original of a building to which the

copyright relates. (n)

**Sec. 187. Reproduction of Published Work. -**

187.1. …. the private reproduction of a published work in a single copy, where the

reproduction is made by a natural person exclusively for research and private study,

shall be permitted, without the authorization of the owner of copyright in the work.

CHAPTER VIII. LIMITATIONS ON COPYRIGHT

**Sec. 187. Reproduction of Published Work.** -

187.2. The permission granted under Subsection 187.1 shall not extend to the

reproduction of:

a) ….

b) An entire book, or a substantial past thereof, or of ….;

c) A compilation of data and other materials;

d) A computer program except as provided in Section 189; and

e) Any work in cases where reproduction would unreasonably conflict with

a normal exploitation of the work or would otherwise unreasonably prejudice

the legitimate interests of the author.

**Data Privacy**

All companies engaged in e-commerce should observe:

1. Notice/awareness

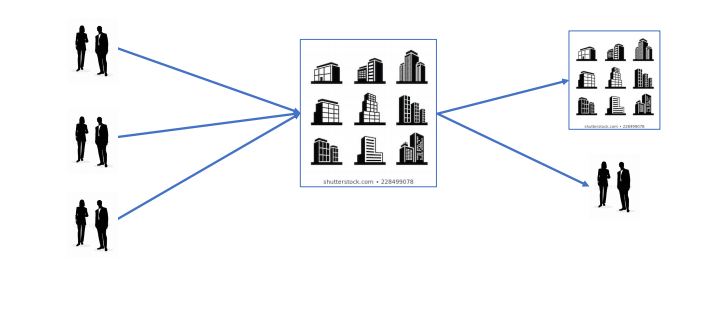
2. Choice/consent

3. Access/participation

4. Security/integrity

**Data Privacy Law (RA 10173)**

Data Privacy Principles (Sec 11). The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality



**Data Privacy Law**

Personal information must be:

a) Collected for specified and legitimate purposes … determined and declared before, or as

soon as reasonably practicable after collection, and later processed in a way compatible with such

declared, specified and legitimate purposes only;

b) Processed fairly and lawfully;

c) Accurate, relevant and, where necessary for purposes for which it is to be used the

processing of personal information, kept up to date; inaccurate or incomplete data must be

rectified, supplemented, destroyed or their further processing restricted;

d) Adequate and not excessive in relation to the purposes for which they are

collected and processed;

e) Retained only for as long as necessary for the fulfillment of the purposes for which

the data was obtained or for the establishment, exercise or defense of legal

claims, or for legitimate business purposes, or as provided by law; and

f) Kept in a form which permits identification of data subjects for no longer than is

necessary for the purposes for which the data were collected and

processed: Provided, That personal information collected for other purposes may

lie processed for historical, statistical or scientific purposes, and in cases laid

down in law may be stored for longer periods: Provided, further,That adequate

safeguards are guaranteed by said laws authorizing their processing.

g) The personal information controller must ensure implementation of personal

information processing principles set out herein.

**Ten Commandments of Computer Ethics**

1. Thou Shalt Not Use A Computer To Harm Other People.

2. Thou Shalt Not Interfere With Other People’s Computer Work.

3. Thou Shalt Not Snoop Around In Other People’s Computer Files.

4. Thou Shalt Not Use A Computer To Steal.

5. Thou Shalt Not Use A Computer To Bear False Witness.

6. Thou Shalt Not Copy Or Use Proprietary Software For Which You have Not Paid.

7. Thou Shalt Not Use Other People’s Computer Resources Without Authorization Or

Proper Compensation.

8. Thou Shalt Not Appropriate Other People’s Intellectual Output.

9. Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The

System You Are Designing.

10. Thou Shalt Always Use A Computer In Ways That Insure Consideration And Respect For

Your Fellow Human

**Social Engineering**

**Definition.** It is a technique used by cybercriminals that aim to trust or steal personal and corporate formation that can be utilized to commit further cybercrimes by employing a trick to any entity to give up their confidential information. In addition, social engineering relies on the basic human instinct of trust to steal information.

* It is “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems.
* It can happen online, in person, or via any other transactions

[What is Social Engineering? | Definition (kaspersky.com)](https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering)

Types of Social Engineering Attacks

**Phishing**

**Definition.** is a kind of social engineering assault that is frequently employed to acquire user information, such as login information and credit card details. It happens when an attacker deceives a victim into opening an email, instant message, or text message by disguising themselves as a reliable source. Next, a dangerous link is deceived into being clicked by the recipient. This can cause malware to be installed on the recipient's computer, a ransomware assault to lock it down, or the disclosure of private data.

Effects on Individuals

* unauthorized purchases
* the stealing of funds,
* identify theft.

Effects on Organizations

* severe financial losses
* declining market share,
* reputation, and
* consumer trust
* reputation

[https://www.imperva.com/learn/application-security/phishing-attack-scam/#:~:text=Phishing%20is%20a%20type%20of,instant%20message%2C%20or%20text%20message](file:///C:\Users\Lenovo\OneDrive\Documents\THIRD%20%20YEAR\CMSC%20185%20(M)%20%20-%20INFORMATION%20SECURITY%20AND%20RISK%20MANAGEMENT\Phishing.docx#:~:text=Phishing%20is%20a%20type%20of,instant%20message%2C%20or%20text%20message).

**Vishing**

**Definition.** Is a type of cybercrime where victims' phones are used to steal sensitive personal data. Cybercriminals use sophisticated social engineering techniques, sometimes known as voice phishing, to persuade victims to act, divulging personal information and access to bank accounts.

**Techniques**

**Wardialing** The cybercriminal uses software to call specific area codes, using a message that involves a local bank, business, police department, or other local organization. When answered the automated calls will suggest confirmation of victims’ confidential information.

**VoIP** makes it very easy for cybercriminals to create fake numbers and hide behind them. These numbers are tough to track and be used to create phone numbers that appear local or use a 1-800 prefix.

**Caller ID Spoofing.** Like VoIP vishing, the cyber criminal hides behind a fake phone number by spoofing the caller ID. They may list their name as Unknown or pretend to represent a legitimate caller, using an ID such as Government, Tax Department, Police, etc.

**Dumpster Diving.** Asimple and popular method of collecting valid phone numbers is to dig through dumpsters behind banks, office buildings, and random organizations.

<https://terranovasecurity.com/what-is-vishing/>

**Smishing**

**Definition.** In a phishing version, victims are tricked into providing the sensitive information to an impersonated attacker. Malware or scam websites might help with SMS phishing. It happens across a wide range of mobile text messaging platforms, including some that don't use SMS, like data-based mobile messaging apps.

**Techniques**

**Malware.** The smishing URL link might trick you into downloading malware, malicious software that installs itself on your phone.

**Malicious website** the link in the smishing message might lead to a fake site that requests you to type sensitive personal information.

<https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it>

**Whaling**

**Definition** is a type of spear-phishing attack directed at high-level executives where attackers masquerade as legitimate, known, and trusted entities and encourage a victim to share highly sensitive information or to send a wire transfer to a fraudulent account.

**Techniques**

* Intercepting and interrupting an unencrypted email conversation to divert a large bank transfer.
* Setting up a fictional meeting with a malware link disguised as a zoom link.
* Requesting payroll information about current and past employees.
* Whaling email with a phone call

[What is a Whaling Attack? | Whaling Phishing | Mimecast](https://www.mimecast.com/content/whaling-phishing-attack/)

[Whaling: how it works, and what your organisation can do... - NCSC.GOV.UK](https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it)

**Pharming**

Pharming is a type of social engineering cyberattack in which criminals redirect internet users trying to reach a specific website to a different, fake site. These “spoofed” sites aim to capture a victim’s personally identifiable information (PII) and log-in credentials, such as passwords, social security numbers, account numbers, and so on, or else they attempt to install pharming malware on their computer. Pharmers often target websites in the financial sector,

**Techniques**

**Malware-based pharming** hackers may send malicious code in an email which installs a virus or Trojan on a user's computer. This malicious code changes the computer’s host file to direct traffic away from its intended target and toward a fake website instead.

Sending a malicious code

**DNS poisoning**. DNS stands for “Domain Name System” – pharmers can modify the DNS table in a server, causing multiple users to visit fake websites instead of legitimate ones inadvertently. Pharmers can use the fake websites to install viruses

[What is Pharming & How to Protect Yourself (kaspersky.com)](https://www.kaspersky.com/resource-center/definitions/pharming)

**Snooping**

**Definition** is unauthorized access to another person's or company's data. The practice is like eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Malicious hacker keyloggers to monitor keystrokes, capture passwords, and login information, and to intercept e-mail and other private communications and data transmissions. Corporations sometimes snoop on employees legitimately to monitor their use of business computers and track Internet usage; governments may snoop on individuals to collect information and avert crime and terrorism.

[Explanation | CyberSecurity Training | www.cybertraining365.com](https://www.cybertraining365.com/cybertraining/Topics/Snooping)

**Ransomware Attack**

**Definition** malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyberattacks place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Some variants have added additional functionality – such as data theft – to provide further incentive for ransomware victims to pay the ransom.

Victims of malware attacks have three options after an infection: they can either pay the ransom, try to, or restart the device.

**Techniques**

**Locker ransomware.** This type of malware blocks basic computer functions. For example, you may be denied access to the desktop, while the mouse and keyboard are partially disabled and does not affect some critical files.

**Crypto ransomware.** Aims to encrypt your important data, such as documents, pictures, and videos, but not interfere with basic computer functions. Often add a countdown to their ransom demand within the deadline.

.

[Ransomware Attacks and Types | How do Locky, Petya and other ransomware differ? (kaspersky.com)](https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types)