SECURITY BASICS AND IT PROFESSIONAL

S.K. Deraman, N.H. Samad

SECURITY BASICS AND IT PROFFESIONAL

PUBLISHED BY:

POLITEKNIK METrO KUALA LUMPUR
No 2 14 Jalan Setiawangsa 10 Taman Setiawangsa
54200 Kuala Lumpur.
Tel : +603 4251 8000
Faks : +603 4251 7000

SECURITY BASICS AND IT PROFESSIONAL

First Published 2023
@ Politeknik METrO Kuala Lumpur

ISBN 978-967-0074-09-2

Perpustakaan Negara Malaysia

Cataloguing-in-Publication Data

Perpustakaan Negara Malaysia

A catalogue record for this book is available from the National Library of Malaysia

ISBN 978-967-0074-09-2

Preface

This book introduces you about the Security Basics and IT Professional. It mainly focuses on introduction to security, security policies and procedures, security troubleshooting solutions and IT professionalism and ethics.

It basically designs to help students in understanding about the basics of security including the types of threat, security policy, encryption, decryption, troubleshooting process and the professional way to handle the different types of customers.

Since this book provides an outlook of the overall foundation information of security basics and IT professional, after going through this material, you will find yourself at a moderate level. It will help your knowledge from basics to the next levels.

Acknowledgement

بسم الله الرحمن الرحيم

The highest gratitude to Allah SWT because with His permission, this Security Basics and IT Professional Book was successfully published.

This book is published as a guide or reference for students who takes the Security Basics and IT Proffessional course at Malaysia Polytechnic. In preparing this book, various challenges and obstacles need to be faced before being able to produce a book. We would like to express our deepest gratitude to our family, Polytechnic e-Learning Coordinator and colleagues for their guidance and support in the production of this book.

We would also like to thank the following for permission to reproduce copyright photos:

- Canva
- Pixabay

We hope that this book can be put to good use by all who use it. Thank you.

Siti Kamila binti Deraman and Nur Hanifah binti A. Samad
October 2023

Table of Contents

Chapter 1: Introduction to Security

Chapter 2: Security Policy and Procedures

Chapter 3: Security Troubleshooting and Solutions

Chapter 4: IT Proffesional

Chapter 1

Introduction to Security

Chapter 1

Introduction to Security

1.1 Information Security

The term information security is frequently used to describe the tasks of securing information that is in a digital format. This digital information is manipulated by a microprocessor (such as on a personal computer), stored on a storage device (like a hard drive or USB flash drive) and transmitted over a network (such as a local area network or the Internet).

Information security can be best understood by examining its goals and the process of how it is accomplished. The goal of information security is to ensure that protective measures are properly implemented to defend against attacks and prevent the total collapse of the system when a successful attack does occur.

A comprehensive definition of information security involves both the goals and process. Information security may be defined as that which protects the integrity, confidentiality and availability of information on the devices that store, manipulate and transmit the information through products, people and procedures.

Chapter 1

The term 'information security' also can be defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide;

i) integrity
ii) confidentiality
iii) availability

1.1.1 Goals of Security: Confidentiality; Integrity; Availability

Information security is intended to protect information that provides value to people and organizations. There are three protections that must be extended over information: **confidentiality, integrity and availability** or **CIA.**

Goals of security:
CIA
Confidentiality, Integrity and Availability

CONFIDENTIALITY

Confidentiality preserve authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It is important that only approved individuals are able to access important information. For example, the credit card number used to make an online purchase must be kept secure and not made available to other parties.

Confidentiality ensures that only authorized parties can view the information. Providing confidentiality can involve several different security tools, ranging from software to 'scramble' the credit card number stored on the web server to door locks to prevent access to those servers.

INTEGRITY

Integrity guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. Integrity ensures that the information is correct and no unauthorized person or malicious software has altered the data. In the example of the online purchase, an attacker who could change the amount of a purchase from RM10,000.00 to RM1.00 would violate the integrity of the information.

AVAILABILITY

Availability ensure timely and reliable access to and use of information. Information has value if the authorized parties who are assured of its integrity can access the information. Availability ensures that data is accessible to authorized users. This means that the information cannot be 'locked up' so tight that no one can access it.

1.1.2 Differentation between attackers and hackers

ATTACKERS

In computer and computer networks, an attack is an any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

HACKERS

A computer **hacker** is any skilled computer expert who uses their technical knowledge to overcome a problem. Most of them are known as White hat, black hat, grey hat and ethical hacker. While 'hacker' can refer to any skilled computer programmer, the term has become associated in popular culture with a 'security hacker', someone who, with their technical knowledge, uses bugs or exploits to break into computer systems.

1.2 Security Threats

1.2.1 Types of Security Threats

A threat, in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more.

There are four types of security threats:
i) Malicious code = Malware
ii) Hacking
iii) Natural disaster
iv) Theft

The other name for malicious code is Malware.

MALICIOUS CODE

Malicious code is known as Malware. It is the term used to describe any code in any part of a software system that is intended to cause security breaches or damage to a system.

Malicious code is the kind of harmful computer code or web script designed to create system vulnerabilities leading to back doors, security breaches, information and data theft, and other potential damages to files and computing systems.

HACKING

Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorised access to or control over computer network security systems for some illicit purpose.

NATURAL DISASTER

When we are planning a new facility, or selecting a new location to which to move, we should be aware of the area in which the facility will be located. A number of factors could cause us issues in terms of protecting our equipment and may impact the safety of our people and data as well. If the site is located in an area prone to natural disasters such as floods, storms, tornadoes, mudslides or similar issues, we may find our facility to be completely unusable or destroyed at some point.

THEFT

Referring to identity theft. It is a crime in which an imposter obtains key pieces of personally identifiable information such as Social Security or driver's license numbers, to impersonate someone else.

1.2.1 Sources of security threats

There are four sources of security threats:
i) External threats
ii) Internal threats
iii) Unstructured threats
iv) Structured threats

EXTERNAL THREATS

External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers.

INTERNAL THREATS

Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network.

This could be a disgruntled employee, an opportunistic employee or an unhappy past employee whose access is still active. In the case of a past network employee, even if their account is gone, they could be using a compromised account or one they set up before leaving for just this purpose.

Organizations should continuously monitor user activities and network traffic to detect unusual or suspicious behavior

UNSTRUCTURED THREATS

Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company.

For example, if an external company Web site is hacked, the integrity of the company is damaged. Even if the external Web site is separate from the internal information that sits behind a protective firewall, the public does not know that. All the public knows is that the site is not a safe environment to conduct business.

Virus

A program capable of replicating with little or no user intervention, and the replicated programs also replicate.

Worm

A form of virus that spreads by creating duplicates of itself on other drives, systems or networks. A worm working with an e-mail system can mail copies of itself to every address in the e-mail system address book. Code Red and Nimda are examples of high-profile worms that have caused significant damage in recent years.

Trojan Horse

An apparently useful or amusing program, possibly a game or screensaver, but in the background it could be performing other tasks such as deleting or changing data or capturing passwords or keystrokes. A true Trojan horse is not technically a virus because it does not replicate itself.

STRUCTURED THREATS

Structured threats come from hackers that are more highly motivated and technically competent. These people know system vulnerabilities, and can understand and develop exploit-code and scripts. They understand, develop and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies.

1.3 Explain methods of security attacks

1.3.1 Various types of security attacks

There are five types of security attacks,

i) Reconnaissance Attack
ii) Access Attack
iii) Denial of Service Attack
iv) Distributed Denial of Service Attack
v) Malicious Code Attack

RECONNAISSANCE ATTACK

Reconnaissance attacks are general knowledge gathering attacks. These attacks can happen in both logical and physical approaches. Whether the information is gathered via probing the network or through social engineering and physical surveillance, these attacks can be preventable as well. Some common examples of reconnaissance attacks are:

i. Phising
ii. Port scanning
iii. Social engineering

ACCESS ATTACK

Access attacks require some sort of intrusion capability. These can consist of anything as simple as gaining an account holder's credentials to plugging foreign hardware directly into the network infrastructure. The sophistication of these attacks ranges just as far. Often these access attacks can be compared to reconnaissance in being either logical or physical, logical being over the net and physical usually leaning more towards social engineering.

DENIAL OF SERVICE ATTACK

A denial of service means that the network cannot move traffic in any capacity. This can happen from power failure or flooding the network with junk traffic that clogs the network's ability to function. Both historically have happened without any malicious intent and both can be prevented with physical and logical blockers.

DISTRIBUTED DENIAL OF SERVICE ATTACK

A distributed denial-of-service (DDoS) attack is one of the most powerful weapons on the internet. When you hear about a website being 'brought down by hackers', it generally means it has become a victim of a DDoS attack. In short, this means that hackers have attempted to make a website or computer unavailable by flooding or crashing the website with too much traffic.

MALICIOUS CODE ATTACK

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code is an application security threat that cannot be efficiently controlled by conventional antivirus software alone.

Common example: Email
(An email can also include attachments of all kinds, as well as booby-trapped shortcuts and malicious code applets).

QUICK TIPS

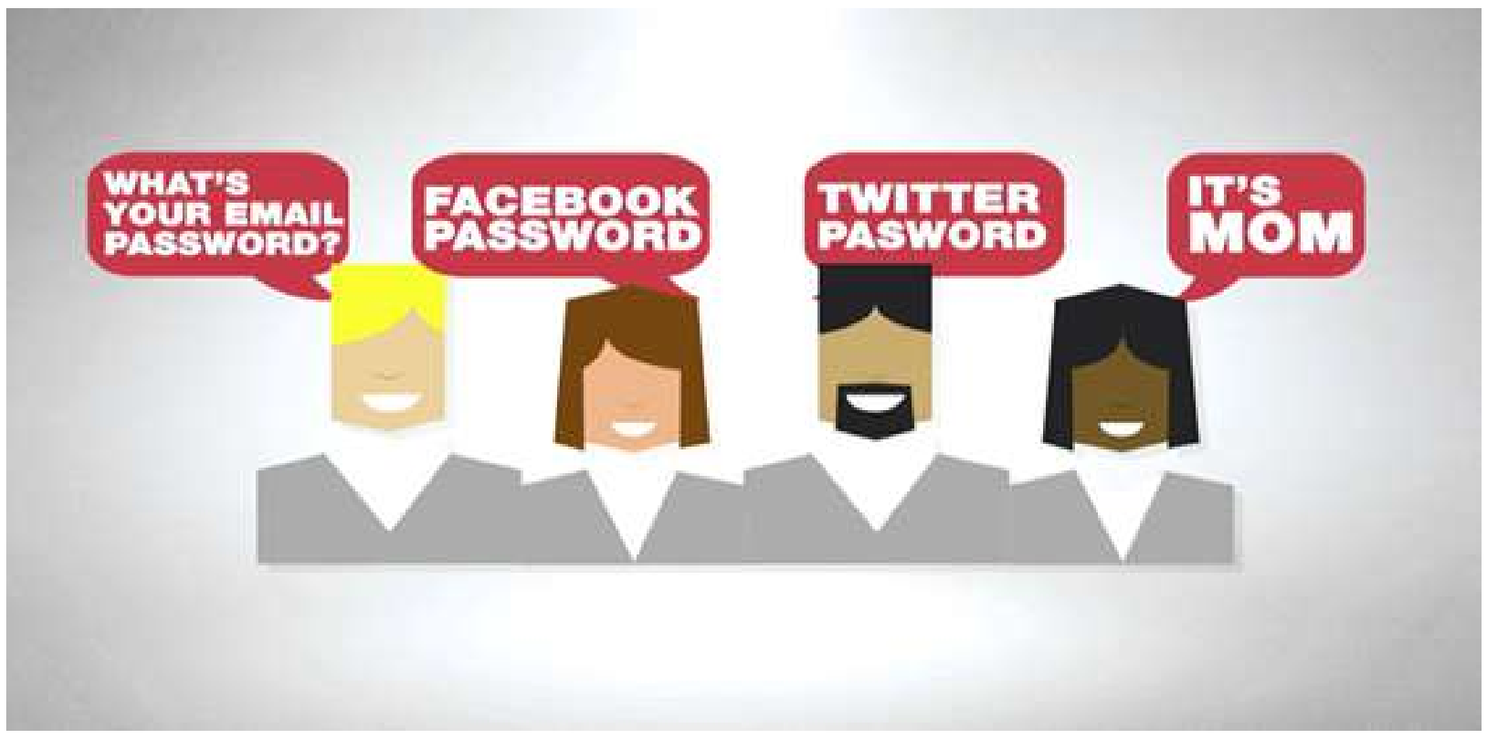
DOS = Denial of Service Attack
DDOS = Distributed Denial of Service Attack

1.3.2 Social Engineering

A social engineer is a person who is able to gain access to equipment or a network by tricking people into providing the necessary access information.

To protect against social engineering:

- Never give out a password.
- Always ask for the ID of the unknown person.
- Restrict access of visitors.
- Escort all visitors.
- Never post your password.
- Lock your computer when you leave your desk.
- Do not let anyone follow you through a door that requires an access card.



There are three types of social engineering:
i. Pretexting
ii. Phishing
iii. Vishing

PRETEXTING

Pretexting is a form of social engineering in which an individual lies to obtain privileged data. A pretext is a false motive. Pretexting often involves a scam where the liar pretends to need information in order to confirm the identity of the person he is talking to.

PHISHING

Phishing is the most common type of social engineering attack that occurs today. At a high level, most phishing scams endeavor to accomplish three things:
i) Obtain personal information such as names, addresses and Social Security Numbers.
ii) Use shortened or misleading links that redirect users to suspicious websites that host phishing landing pages.
iii) Incorporate threats, fear and a sense of urgency in an attempt to manipulate the user into responding quickly.

VISHING

Voice phishing or vishing is a form of criminal phone fraud, using social engineering over the telephone system to gain access to private personal and financial information for the purpose of financial reward.

Understanding social engineering can increase your awareness of potential threats, enabling you to protect yourself and your personal information.

1.4 Describe various tools in information security

1.4.1 Function of Network Mapper, Netstat and Netscan

There are three common tools used in information security.

i) Network Mapper
ii) Netstat
iii) Netscan

NETWORK MAPPER

Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

NETSTAT

Netstat is a common command line TCP/IP networking utility available in most versions of Windows, Linux, UNIX and other operating systems. Netstat provides information and statistics about protocols in use and current TCP/IP network connections. The name derives from the words network and statistics.

NETSCAN

Netscan is a useful tool for checking network and Internet connections. Some useful applications for the average PC user are considered, including checking for malware connections.

Network Mapper is also known as Nmap

1.5 Describe access to data and equipment

There are two ways to access the data and equipment.
i) Data wiping
ii) Hard drive destruction

DATA WIPING

Deleting files from a hard drive does not remove them completely from the computer. This data is not completely removed until the hard drive stores other data in the same location, overwriting the previous data. Hard drives should be fully erased (data wiped) to prevent the possibility of recovery using specialized software.

Data wiping, also known as secure erase is a software-based method of overwriting the data that aims to completely destroy all electronic data residing on a hard disk drive or other digital media. Data wiping is often performed on hard drives containing sensitive data that are considered confidential such as financial information.

HARD DRIVE DESTRUCTION

Companies with sensitive data should always establish clear policies for hard drive disposal. It is important to be aware that formatting and reinstalling an operating system on a computer does not ensure that information cannot be recovered. Destroying the hard drive is the best option for companies with sensitive data.

Drilling holes through a drive's platters is not the most effective method of hard drive destruction. Data can still be recovered using advanced data forensic software. To fully ensure that data cannot be recovered from a hard drive, carefully shatter the platters with a hammer and safely dispose of the pieces.

The only way to fully ensure that data cannot be recovered from a hard drive is to carefully shatter the platters with a hammer and safely dispose of the pieces. To destroy software media (floppy disks and CDs), use a shredding machine designed for shredding these materials.

Hard Drive Recycling - Hard drives that do not contain sensitive data can be reformatted and used in other computers. The drive can be reformatted, and a new operating system can be installed. Two types of formatting can be performed:

i) **Standard format** - Also called high-level formatting, a boot sector is created and a file system is set up on the disk. A standard format can only be performed after a low-level format has been completed.
ii) **Low-level format** - The surface of the disk is marked with sector markers to indicate where data will be stored physically on the disk and tracks are created. Low-level formatting is most often performed at the factory after the hard drive is built.

QUICK TIPS

Government and industry standards like DoD 5220.22-M specify secure data wiping procedures to protect sensitive information

QUIZ YOURSELF!

1. Identify the security goals that involves prevention of unauthorized access of information or resources
   a. Integrity
   b. Availability
   c. Confidentiality
   d. Accountability

"There is a network printer in the hallway of the company where you work. Many employees don't pick up their printouts immediately and leave them on the printer"

2. Predict the consequences to the reliability of information based on the situation given above
   a. The integrity of the information is not guaranteed
   b. The accountability of the information is not guaranteed
   c. The availability of the information is no longer guaranteed
   d. The confidentiality of the information is no longer guaranteed

"Internet scam done by cyber-criminals where the user is convinced digitally to provide confidential information"

3. Select the type of attacks based on the statement given above
   a. Dos attack
   b. Website attack
   c. Phishing attack
   d. Brute force attack

4. Identify the famous hacker and social engineer turned his skills toward cybersecurity and became a consultant
   a. Kevin Mitnick
   b. Julian Assange
   c. Edward Snowden
   d. Mark Zuckerberg

5. Select the common strategy that social engineering attacks frequently use to achieve their goals
   a. Weak passwords
   b. Strong encryption
   c. Regular system updates
   d. Hardware vulnerabilities

6. Identify the common aim of both traditional and digital forms of social engineering
   a. To sell products and services
   b. To improve social interactions
   c. To promote cybersecurity awareness
   d. To gain unauthorized access or information

7. Choose the CORRECT definition of phishing
   a. A type of virus
   b. A recreational fishing activity
   c. A computer programming language
   d. A social engineering technique that uses fake websites or emails to trick individuals into revealing personal information

8. Identify the the primary goal of a social engineering attack
   a. To launch a DDoS attack on a website
   b. To physically break into a secure facility
   c. To install antivirus software on a target's computer
   d. To manipulate people into revealing confidential information

9. Identify the type of cyberattack is designed to intercept and eavesdrop on communication between two parties without their knowledge
   a. DDoS attack
   b. Phishing attack
   c. SQL injection attack
   d. Man-in-the-middle (MitM) attack

10. Select the CORRECT example of a social engineering attack
   a. Configuring a firewall
   b. Forging a digital signature
   c. Installing antivirus software
   d. Sending deceptive emails to trick someone into revealing their password

11. Identify the common type of malware that can encrypt your files and demand a ransom for their release
   a. Rootkit
   b. Trojan horse
   c. Ransomware
   d. Phishing attack

ANSWER!

1. C
2. D
3. C
4. A
5. A
6. A
7. D
8. D
9. D
10. C
11. C

Chapter 2

Security Policies and Procedures

Chapter 2

Security Policy and Procedures

2.1 Understanding Security Policy

Security starts with an organization determining what actions must be taken to create and maintain a secure environment. That information is recorded in a formal security policy.

A **security policy** is a document or series of documents that clearly defines the defense mechanisms an organization will employ in order to keep information secure.

A good security policy should be a high-level, brief, formalized statement of the security practices that management expects employees and other stakeholders to follow. It should be concise and easy to understand so that everyone can follow the guidance set forth in it.

A security policy lays down specific expectations for management, technical staff and employees. A clear and well-documented security policy will determine what action an organization takes when a security violation is encountered. In the absence of clear policy, organizations put themselves at risk and often flounder in responding to a violation.

SECURITY POLICY

Managers

For managers, a security policy identifies the expectations of senior management about roles, responsibilities and actions that should be taken by management with regard to security controls.

Technical staff

For technical staff, a security policy clarifies which security controls should be used on the network, in the physical facilities and on computer systems.

Employees

For all employees, a security policy describes how they should conduct themselves when using the computer systems, e-mail, phones and voice mail.

2.1.1 The needs of security policy for an organizations

There are four main reasons why an organizations need a security policy.

i) Legal compliance with Information security regulations like HIPAA and Gramm-Leach Bliley require information security policies and standards.
ii) MasterCard and Visa require organizations that accept their credit and debit cards to have information security policies and standards.
iii) Every information security effective practice contains a requirement for organization-wide information security policies and standards.
iv) In the event of an information incident negatively affecting third parties, it may be argued that the absence of information security policies and standards is evidence of information negligence.

7 SECURITY POLICY REQUIREMENTS

REQUIREMENT 1

Identify organizational issues that impact information security policy

REQUIREMENT 2

Identify the various classes of policy users

REQUIREMENT 3

Organize information security policies and standards into meaningful categories

REQUIREMENT 4

Review draft policies and standards with management, users, and legal counsel

REQUIREMENT 5

Train all personnel in the organization's information security policies and standards

REQUIREMENT 6

Enforce the information security policies and standards

REQUIREMENT 7

Review and modify policies and standards, as appropriate but at least annually

2.1.2 Username and password

Password Policy is used as a way of authentication before retrieving any confidential sources.

A Strong password should have the following characteristics:

i) English uppercase characters (A through Z)
ii) English lowercase characters (a through z)
iii) Base 10 digits (0 through 9)
iv) Symbols (for example, !, $, #, %)

User should also change their password frequently, at least every 30 days or within three months.

USERNAME DO AND DONT'S

Do	Dont's
Usernames can contain : letters (a-z), numbers (0-9), dashes (-), underscores (_), apostrophes ('), and periods (.).	Usernames can't contain : an ampersand (&), equal sign (=), brackets (<,>), plus sign (+), comma (,), or more than one period (.) in a row.

2.1.3 File and folder permissions

On NTFS volumes, you can set security permissions on files and folders. These permissions grant or deny access to the files and folders.

FILE PERMISSION

- Full Control
- Modify
- Read & Execute
- Read
- Write

FOLDER PERMISSION

- Full Control
- Modify
- Read & Execute
- List Folder Contents
- Read
- Write

2.2 Security procedures

Procedures are detailed step-by-step tasks that should be performed to achieve a certain goal. For example; we can write procedures on how to install operating systems, configure security mechanisms, implement access control lists, set up new user accounts, assign computer privileges, audit activities, destroy material, report incidents and much more.

Procedures are considered the lowest level in the policy chain because they are closest to the computers and users (compared to policies) and provide detailed steps for configuration and installation issues.

Procedures spell out how the policy, standards and guidelines will actually be implemented in an operating environment. If a policy states that all individuals who access confidential information must be properly authenticated, the supporting procedures will explain the steps for this to happen by defining the access criteria for authorization, how access control mechanisms are implemented and configured and how access activities are audited.

The only difference for file and folder permissions is:

- **List folder contents**

There are a several of security procedures that can be implement in any organization which is:
i) Security Policies
ii) Data Protection
ii) Protecting Against Malicious Software

2.2.1 Data protection

There are number of approach that we can take to protect our data. Software firewalls, biometrics and smart cards, data backups and data encryption are some of the approaches that we can take to protect our data.

SOFTWARE FIREWALL

A software firewall is a program that runs on a computer to allow or deny traffic between the computer and other computers to which it is connected. The software firewall applies a set of rules to data transmissions through inspection and filtering of data packets. Windows Firewall is an example of a software firewall. It is installed by default when the OS is installed.

Every communication using TCP/IP is associated with a port number. HTTP, for instance, uses port 80 by default. A software firewall, is capable of protecting a computer from intrusion through data ports.

You can control the type of data sent to another computer by selecting which ports will be open and which will be blocked. You must create exceptions to allow certain traffic or applications to connect to the computer. Firewalls block incoming and outgoing network connections, unless exceptions are defined to open and close the ports required by a program.

There are 8 steps to disable ports with the Windows Firewall in Windows 7.

STEP 1

Select Start > Control Panel > Windows Firewall > Advanced settings.

STEP 2

In the left pane, choose to configure either Inbound Rules or Outbound Rules in the left pane and click New Rule in the right pane.

STEP 3

Select the Port radio button and click Next.

STEP 4

Choose TCP or UDP.

STEP 5

Choose All local ports or Specific local ports to define individual ports or a port range and click Next.

STEP 6

Choose Block the connection and click Next.

STEP 7

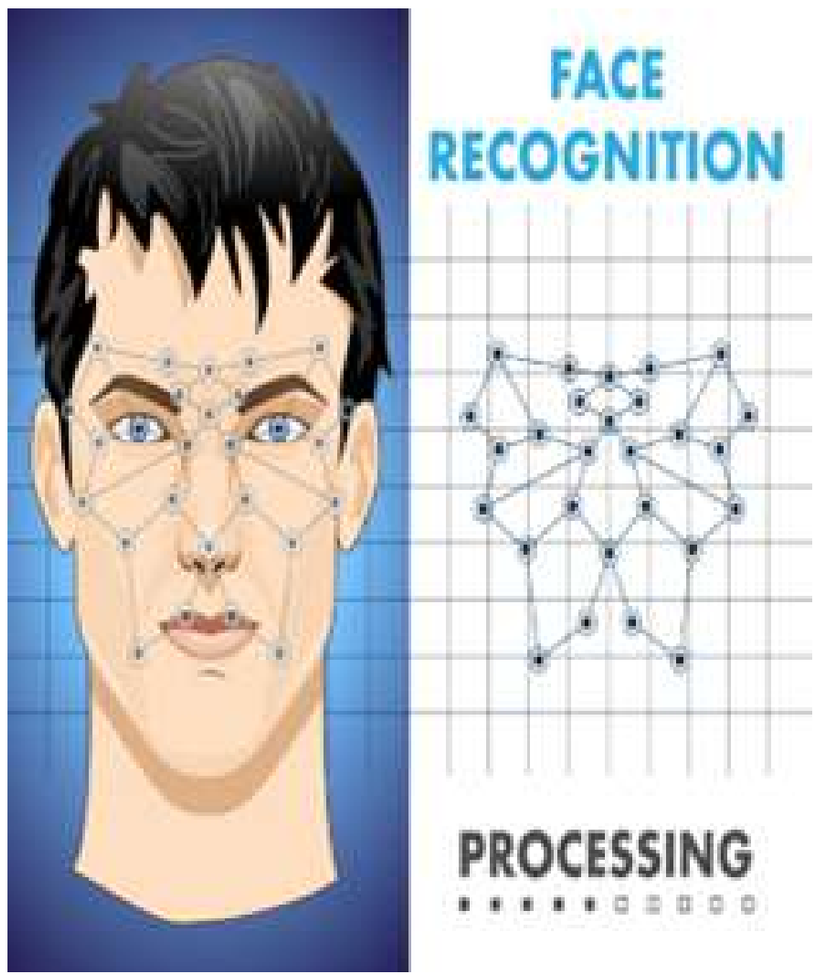
Choose when the rule applies and click Next.

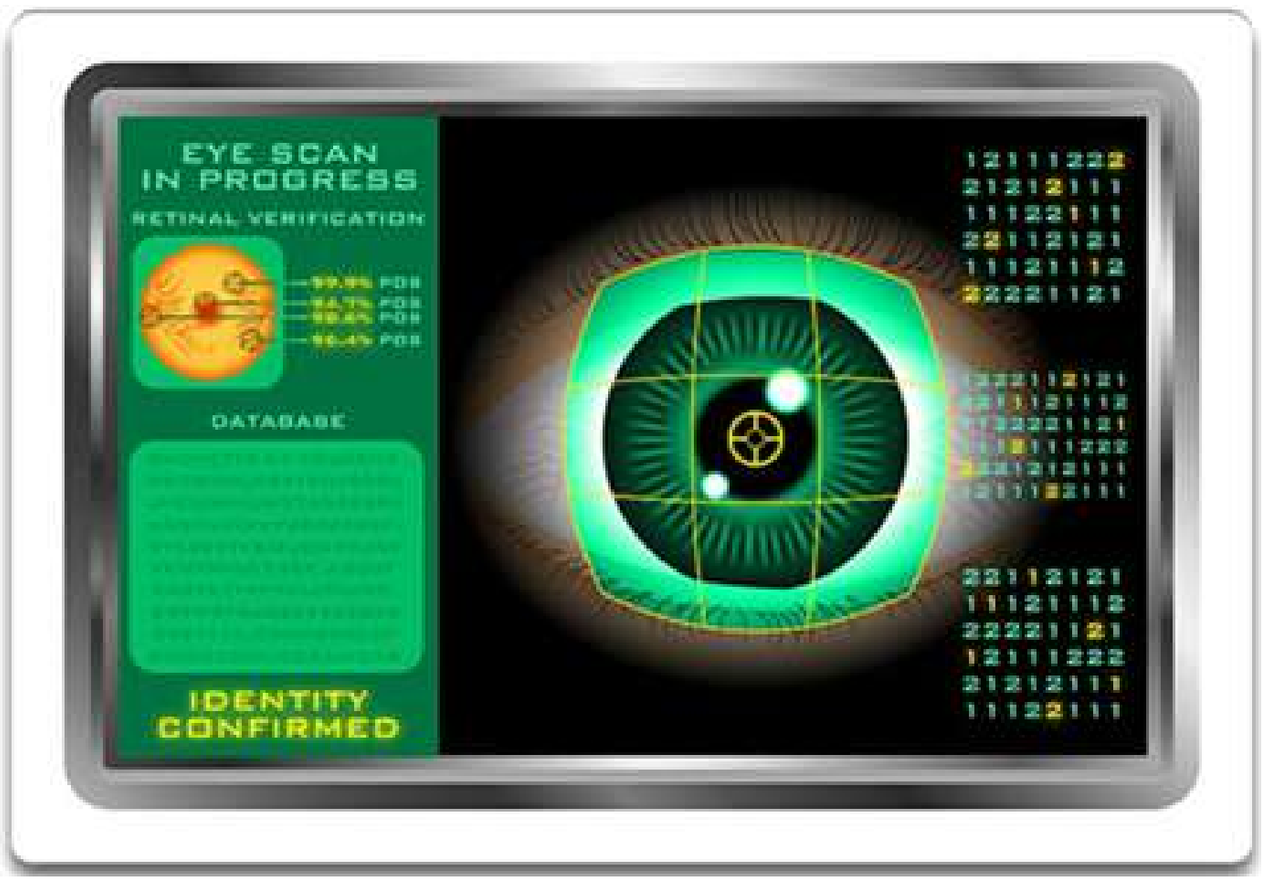
STEP 8

Provide a name and optional description for the rule and click Finish.

BIOMETRICS AND SMART CARD

Biometric security compares physical characteristics against stored profiles to authenticate people. A profile is a data file containing known characteristics of an individual. A fingerprint, a face pattern or retina scan are all examples of biometric data.





In theory, biometric security is more secure than security measures such as passwords or smart cards, because passwords can be discovered and smart cards can be stolen. Common biometric devices available include fingerprint readers, retina scanners, and face and voice recognition devices. The user is granted access if their characteristics match saved settings and the correct login information is supplied.

Biometric devices measure physical information about a user. It is ideal for highly secure areas when combined with a secondary security measure such as a password or pin. However, for most small organizations, this type of solution is too expensive.

A **smart card** is a small plastic card, about the size of a credit card, with a small chip embedded in it.

The chip is an intelligent data carrier, capable of processing, storing, and safeguarding data. Smart cards store private information, such as bank account numbers, personal identification, medical records and digital signatures. Smart cards provide authentication and encryption to keep data safe.

A **security key fob** is a small device that resembles the ornament on a key ring.

It has a radio that communicates with a computer over a short range. The fob is small enough to attach to a key ring. The computer must detect the signal from the key fob before it accepts a username and password.

DATA BACKUP

A data backup stores a copy of the information on a computer to removable backup media that can be kept in a safe place. Backing up data is one of the most effective ways of protecting against data loss. Data can be lost or damaged in circumstances such as theft, equipment failure or a disaster. If the computer hardware fails, the data can be restored from the backup to functional hardware.

Data backups should be performed on a regular basis and included in a security plan. The most current data backup is usually stored offsite to protect the backup media if anything happens to the main facility. Backup media is often reused to save on media costs.

These are some considerations for data backups:

i) Frequency
a) Backups can take a long time. Sometimes it is easier to make a full backup monthly or weekly, and then do frequent partial backups of any data that has changed since the last full backup.
b) However, having many partial backups increases the amount of time needed to restore the data.

ii) Storage
For extra security, backups should be transported to an approved offsite storage location on a daily, weekly or monthly rotation as required by the security policy.

iii) Security
Backups can be protected with passwords. The password is entered before the data on the backup media can be restored.

iv) Validation
Backups need to be validate to ensure the integrity of the data.

DATA ENCRYPTION

Encryption is often used to protect data. Encryption is where data is transformed using a complicated algorithm to make it unreadable. A special key must be used to return the unreadable information back into readable data. Software programs are used to encrypt files, folders and even entire drives.

Encrypting File System (EFS) is a Windows feature that can encrypt data. EFS is directly linked to a specific user account. Only the user that encrypted the data will be able to access it after it has been encrypted using EFS.

Encrypting File System (EFS)

To encrypt data using EFS, follow these steps:

Step 1. Select one or more files or folders.

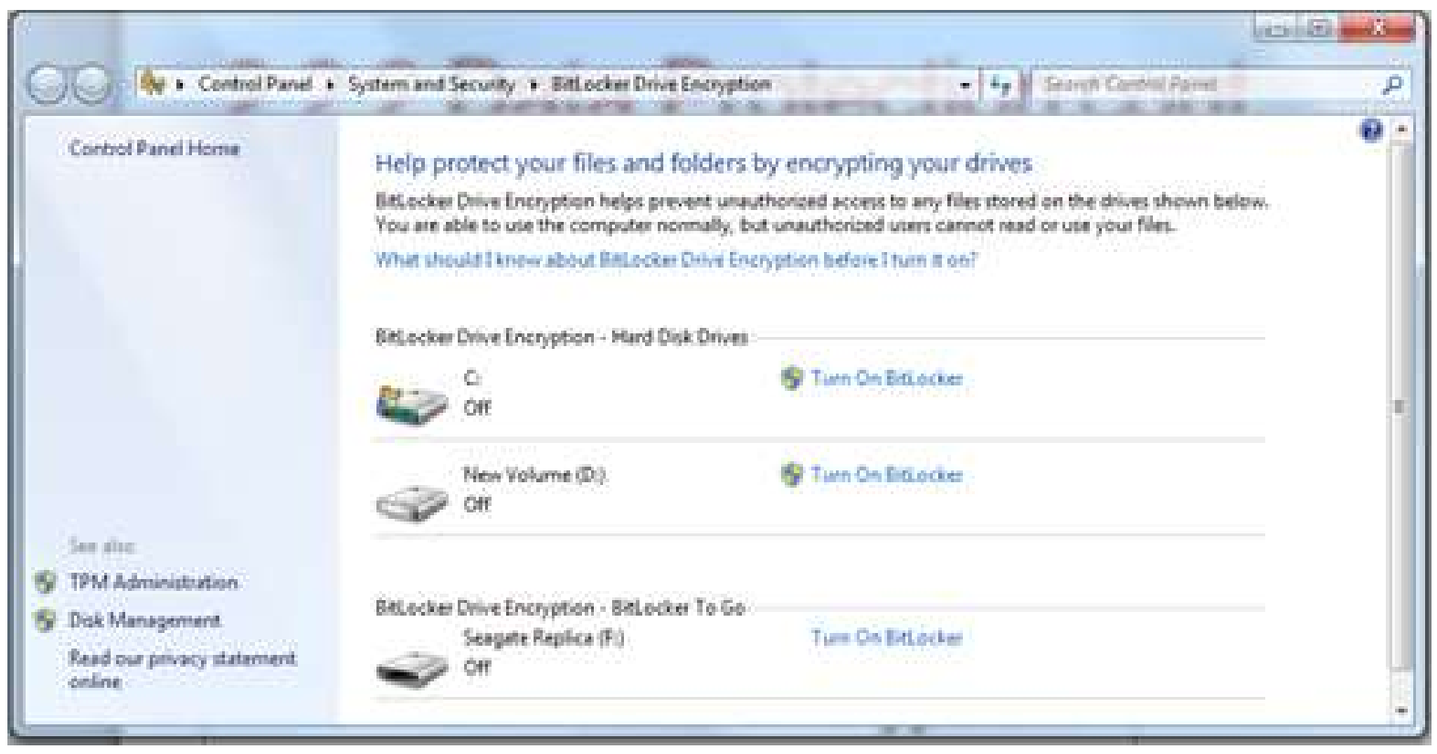
Step 2. Right-click the selected data > Properties.

Step 3. Click Advanced.

Step 4. Select the encrypt contents to secure data check box.

Step 5. Files and folders that have been encrypted with EFS are displayed in green.

In Windows 7 and Windows Vista Ultimate and Enterprise editions, a feature called **BitLocker** is included to encrypt the entire hard drive volume. BitLocker is also able to encrypt removable drives.



To use BitLocker, at least two volumes must be present on a hard disk. A system volume is left unencrypted and must be at least 100 MB. This volume holds the files required by Windows to boot. Windows 7 creates this volume by default when it is installed.

2.2.2 Protection against malicious software

Certain types of attacks, such as those performed by spyware and phishing, collect data about the user that can be used by an attacker to gain confidential information. You should run virus and spyware scanning programs to detect and remove unwanted software. Many browsers now come equipped with special tools and settings that prevent the operation of several forms of malicious software.

2.3 Encryption Technology

There are four cryptographic terminologies and three common communication encryption types as follows:

a) cryptographic terminologies
   i) Encryption
   ii) Cipher Text
   iii) Decryption
   iv) Cryptanalysis

b) common communication encryption types:
   i) Symmetric
   ii) Asymmetric
   iii) Hash encoding

Encryption

A process of converting a data (plaintext) into a form that cannot be easily understood (ciphertext) by unauthorized people.

Decryption

A process to convert the ciphertext into the plaintext. Decryption requires a secret key or password.

Ciphertext

The disguised (encrypted) file or message that could not been read directly.

Plaintext

Plaintext is an original text.

Cryptanalysis

Cryptanalysis is the science of cracking codes and decoding secrets.

ENCRYPTION

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the Internet or other computer networks. Modern encryption algorithms play a vital role in the security assurance of IT systems and communications as they can provide not only confidentiality, but also the following key elements of security:

i) Authentication : The origin of a message can be verified.
ii) Integrity: Proof that the contents of a message have not been changed since it was sent.
iii) Non-repudiation: The sender of a message cannot deny sending the message.

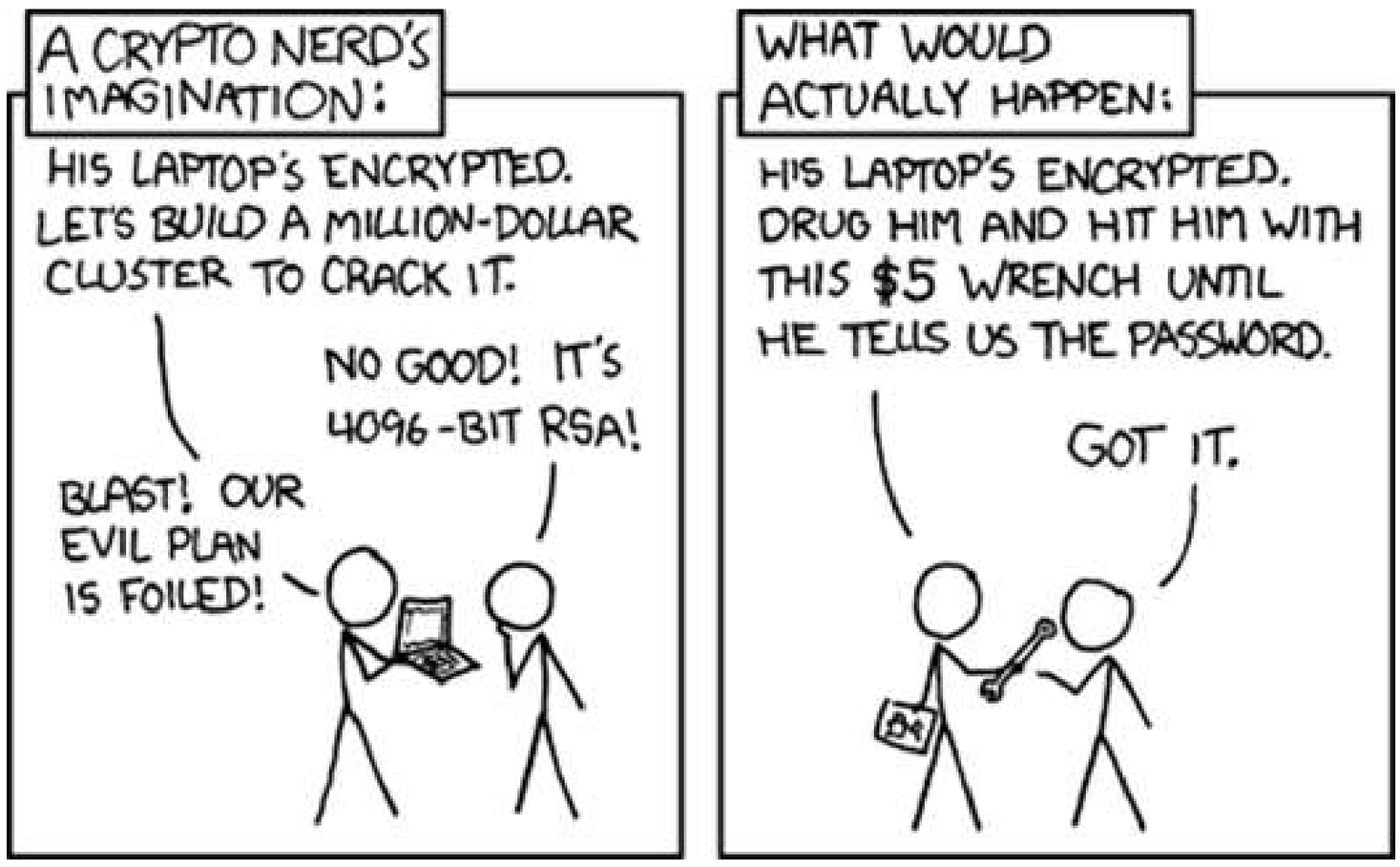
CIPHER TEXT

User can encrypt the plaintext to the ciphertext using the ciphertext table.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

1	2	3	4	5	6	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

Plaintext: LITTLE GREEN APPLES
Ciphertext: FCNNF5 AL55H IJJF5M



ENCRYPTION TYPES

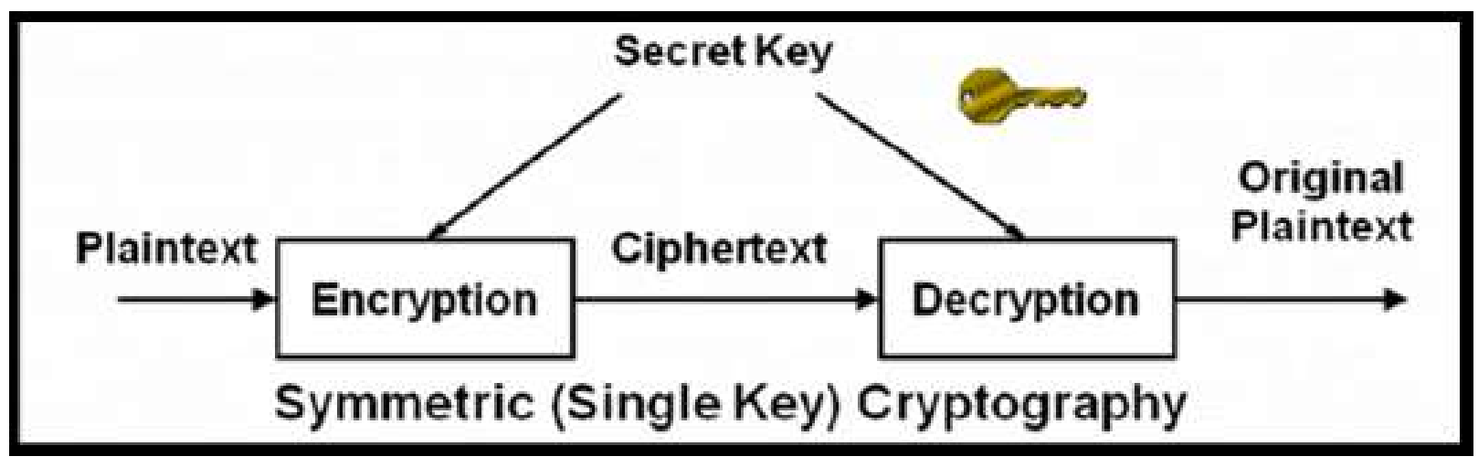
There are two types of encryption which is symmetric and assymetric encryption. The encryption method is known as Hash Encoding.

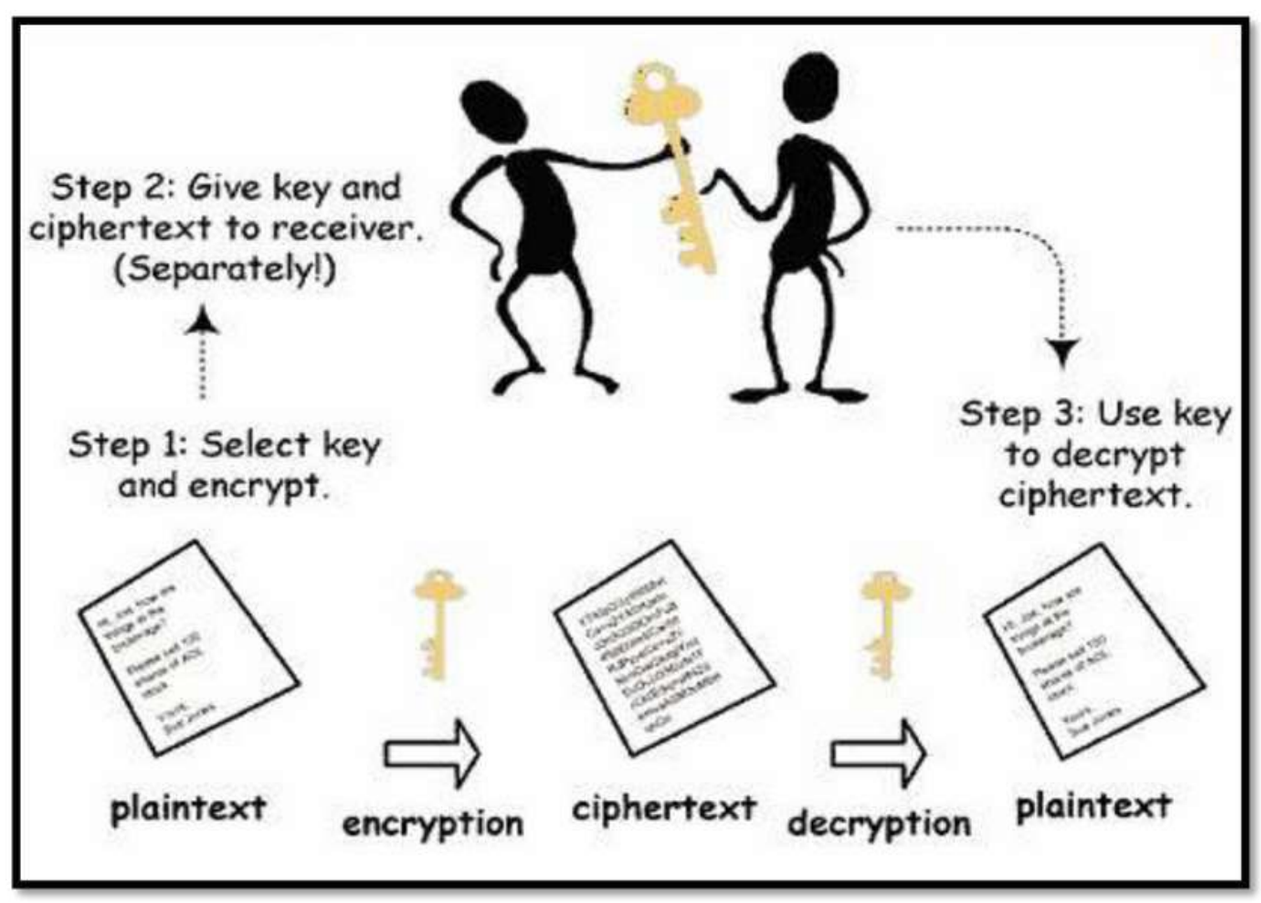
QUICK TIPS

The German Enigma machine, used during World War II, was one of the most famous encryption devices. Breaking its code was a significant achievement for the Allies

SYMMETRIC ENCRYPTION

Symmetric encryption is based on single key. It will use a private key or secret key. It may also be referred to as shared key or shared secret encryption. In symmetric encryption, a single key is used both to encrypt and decrypt traffic.





Symmetric encryption's job is to take readable data ('plaintext' in crypto), scramble it to make it unreadable (protecting it from prying eyes while it's being stored on a disk or transmitted over a network), then unscramble it again when it's needed. It's generally fast and there are lots of good encryption methods to choose from. The most important thing to remember about symmetric encryption is that both sides the encrypter, and the decrypter need access to the same key.

A key, for symmetric encryption purposes, is a string of data that is fed to the encrypter in order to scramble the data and make it encrypted. It is best if this key is completely random, but there are ways to derive keys from (hopefully really good) passwords as well. The tricky part about using symmetric encryption is how to store the key and make it available only to the software that needs it.

Symmetric encryption algorithms can be extremely fast and their relatively low complexity allows for easy implementation in hardware. However, they require that all hosts participating in the encryption have already been configured with the secret key through some external means.

Uses of symmetric encryption

In services that store encrypted data on behalf of a user (like cloud backup services) when those services leave the decryption key in the hands of the user. To encrypt computer or device storage - one particularly neat property of a well-encrypted device is that it can be really quickly erased: just make sure the key is destroyed. The resulting encrypted data still stored on the device is then useless to anyone.

To create a secure channel between two network endpoints provided, there's a separate scheme for securely exchanging the key.

ADVANTAGES

The advantages of symmetric encryption are as follows:

i) Fast
ii) Relatively Secure : Symmetric key ciphers can be composed to produce stronger ciphers
iii) Widely understood

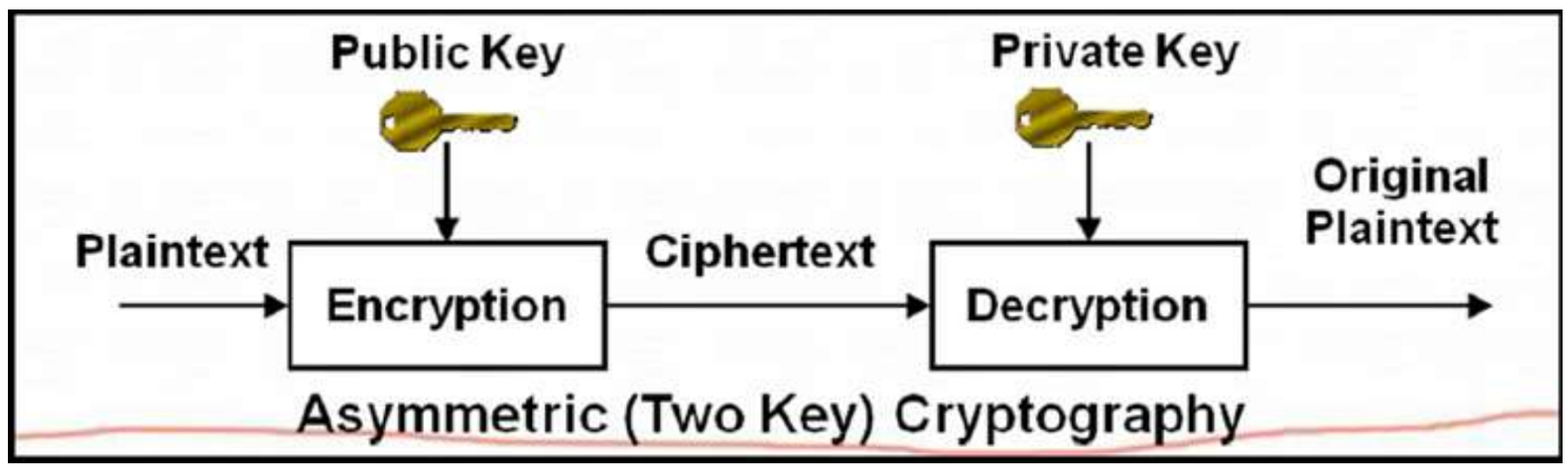
DISADVANTAGES

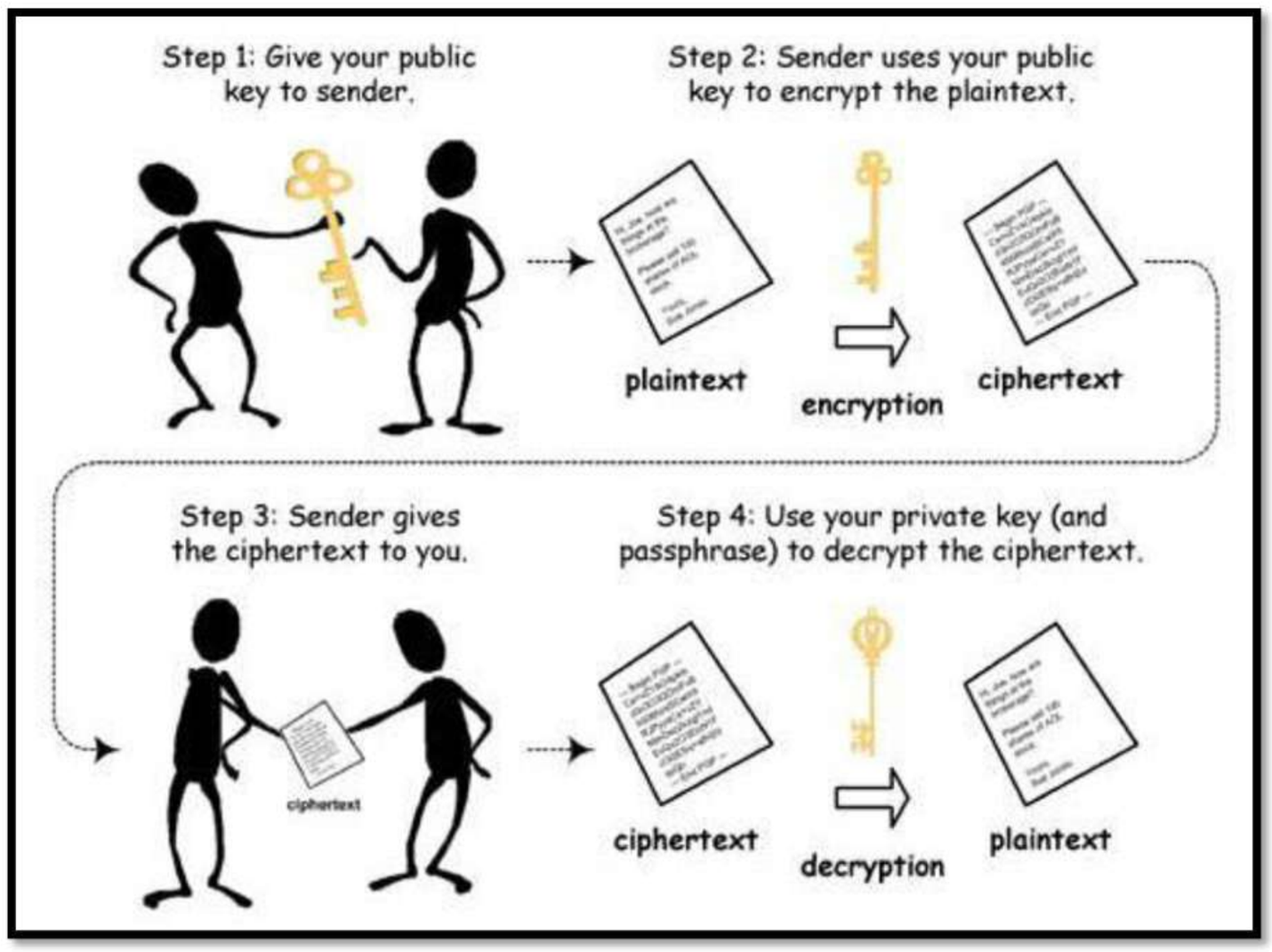
The disadvantages of symmetric encryption are as follows:

i) Requires secret sharing
ii) Complex administration : In large networks, there are many keys pairs to be managed
iii) No authentication
iv) Key must remain secret at both ends

ASSYMMETRIC ENCRYPTION

Asymmetric encryption is also known as public-key cryptography. Asymmetric encryption differs from symmetric encryption primarily in that two keys are used: one for encryption and one for decryption. Everybody having the public key is able to send encrypted messages to the owner of the secret key.





Asymmetric encryption use two keys to encrypt and decrypt data. These asymmetric keys are referred to as public key and private key. The public key can be used by the sender to encrypt a message and the private key can be used by the receiver to decrypt the message.

Types of encryption:

i) Symmetric
(same key to encrypt and decrypt)

ii) Assymetric
(different key to encrypt and decrypt))

ADVANTAGES

The advantages of assymmetric encryption are as follows:

i) It allows message authentication
ii) It is convenient
iii) It allows for non-repudiation
iv) It detects tampering

DISADVANTAGES

The disadvantages of assymmetric encryption are as follows:

i) It is a slow process
ii) Its public keys are not authenticated
iii) It risks loss of private key, which may be irreparable
iv) It risks widespread security compromise

Differentiation between symmetric and assymetric encryption

Symmetric

i) Both parties share the same key for encryption and decryption.
ii) Key needs to be kept secret.
iii) Not consuming too much computing power.

Assymetric

i) Use pairs of keys. One is used for encryption and the other one for decryption.
ii) Decryption key is typically kept secret, therefore called 'private key' or 'secret key', while the encryption key is spread to all who might want to send encrypted messages, therefore called 'public key'.
iii) Are much slower than symmetric key encryption.

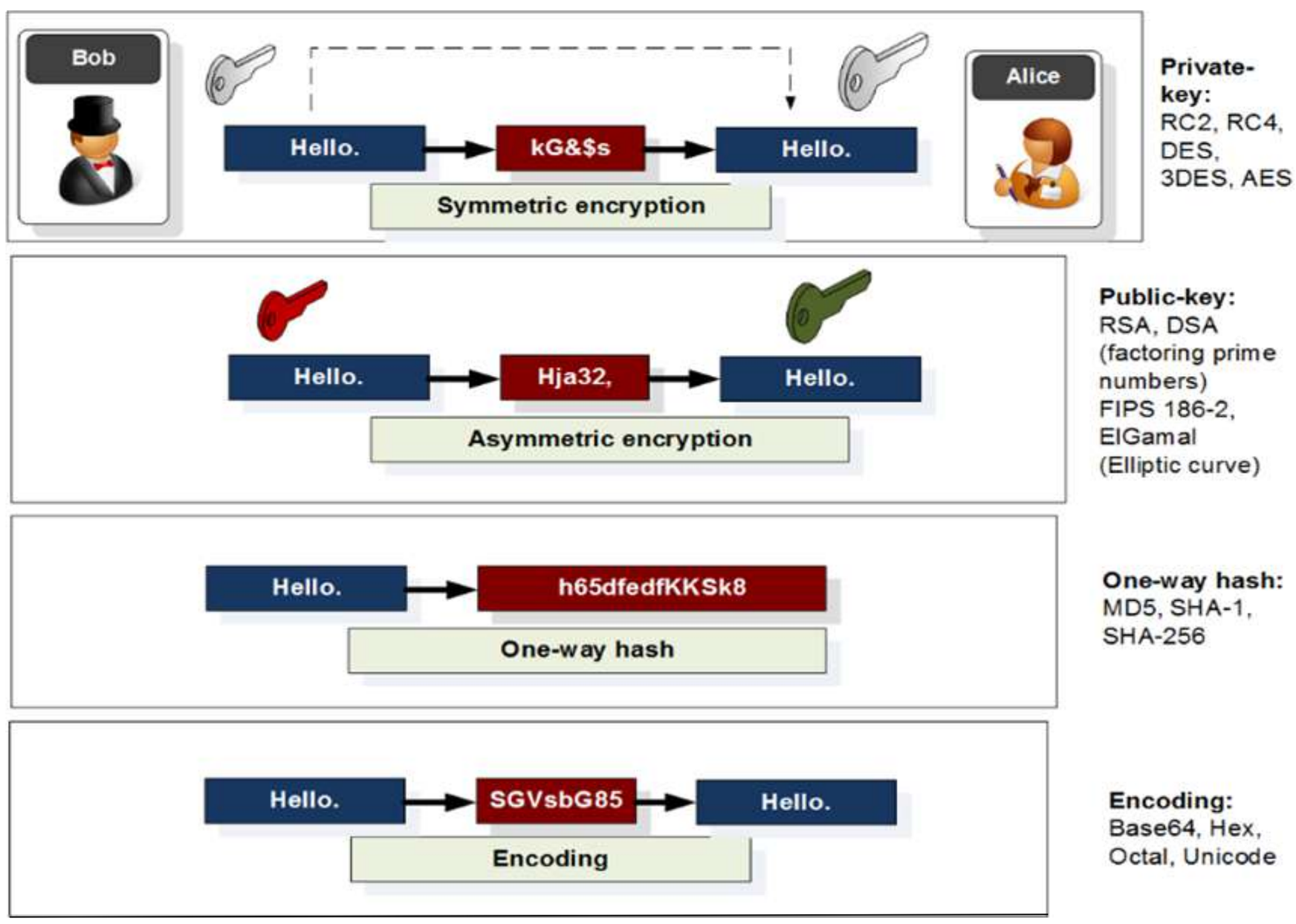
HASH ENCODING

Hashing is what is actually happening when you hear about passwords being 'encrypted'. Hashing is not a form of encryption, though it does use cryptography. Hashing takes data and creates a hash out of it, a string of data with three important properties:

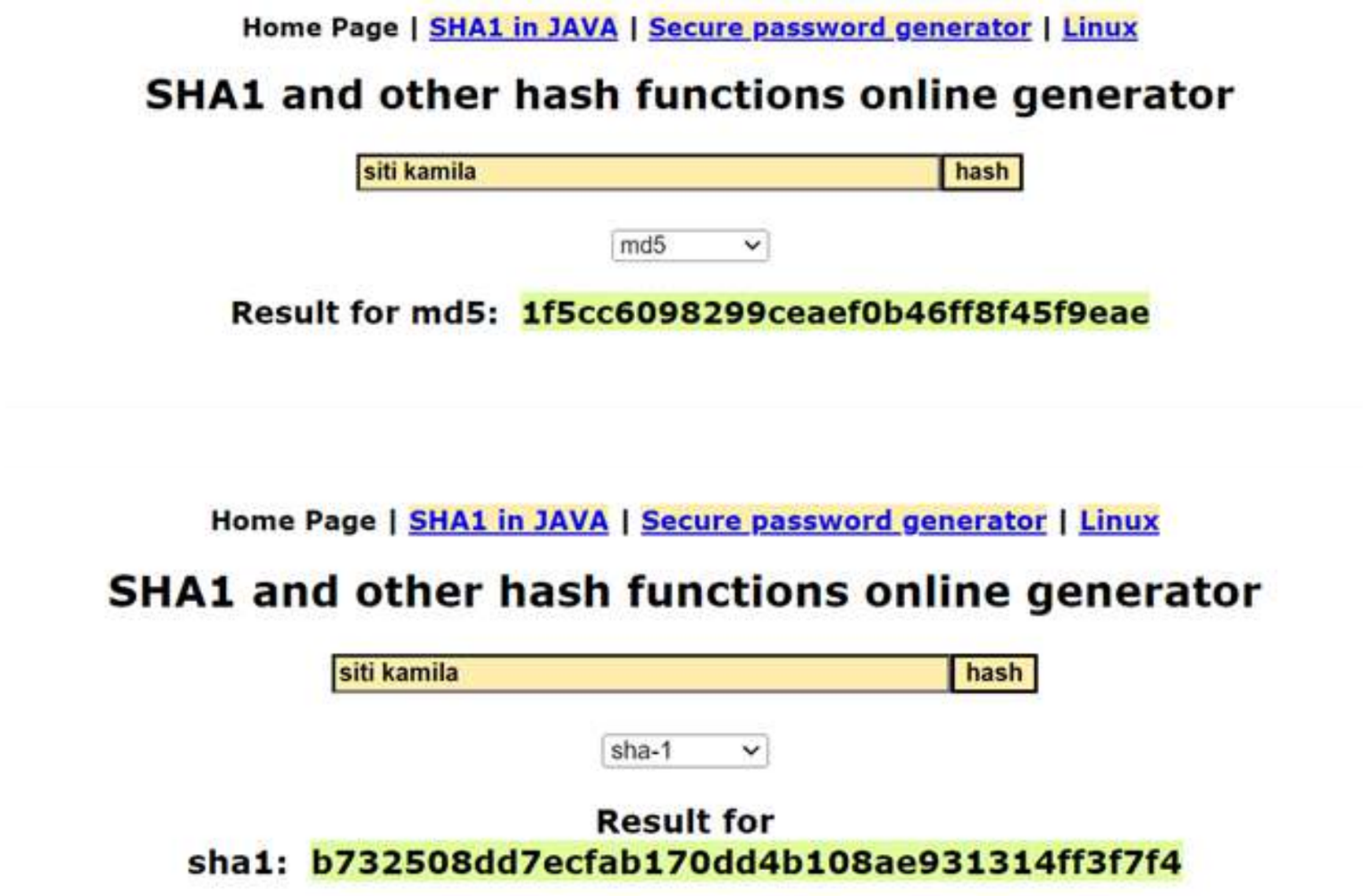
i) The same data will always produce the same hash.
ii) It is impossible to reverse it back to the original data.
iii) Given knowledge of only the hash, it is infeasible to create another string of data that will create the same hash (called a 'collision' in crypto parlance).

Hashing is the changing of a character string into a shorter fixed-length value or key that represents the original string. This shorter hashed key is faster to retrieve and use and is encrypted. The hashing algorithm is called the hash function and is used to encrypt and decrypt digital signatures.

Hash functions, also referred to as message digests that do not use a key, Hashes cannot be used to discover the contents of the original message, or any of its other characteristics, but can be used to determine whether the message has changed.



SHA 1 VS MD5



Example of hash in PHP

```
<?php $hash = password_hash($password, PASSWORD_DEFAULT);

<?php if (password_verify($password, $hash)) { // Success! } else { // Invalid
credentials }
```

QUIZ YOURSELF!

1. Identify the function of encryption
   a. To make password secret
   b. To enable network connection all the time
   c. To make sure the server is secure from attackers
   d. To convert data into a form that cannot be understood by unauthorized people

A contract that defines expectations between an organization and the service vendor to provide an agreed-on level of support

2. Select the CORECT features of the service based on the statement given above
   a. Simple diagnostic
   b. Detailed fees and expenses
   c. Basic problem management procedures
   d. Stored in RAM and caches temporarily

"In encryption, the length of the encryption key is directly related to X"

3. Identify X
   a. The type of algorithm used
   b. The level of security provided
   c. The level of security provided
   d. The speed of encryption and decryption

4. Identify the algorithm that considered one of the most secure and is commonly used in applications like VPNs and secure communication systems
   a. RSA
   b. DES
   c. AES
   d. ROT13

5. Select the CORRECT process of converting encrypted data back into its original, readable form (plaintext)
   a. Encoding
   b. Encryption
   c. Decryption
   d. Compression

6. Identify the definition of term "end-to-end encryption"
   a. Encryption that only works on one end of a communication
   b. Encryption that is applied to every communication except the final one
   c. Encryption that is only used for secure storage, not during transmission
   d. Encryption that extends from the beginning to the end of a communication, ensuring that only the sender and intended recipient can decipher the data

7. Choose the amount of keys use in asymmetric encryption
   a. One key
   b. Two key
   c. Four key
   d. Five key

8. Identify the type of encryption uses the same key for both the encryption and decryption of data
   a. Hybrid encryption
   b. Public-key encryption
   c. Symmetric encryption
   d. Asymmetric encryption

9. Identify the encryption method is often used to secure internet communications and ensure the confidentiality and integrity of data sent between a web browser and a web server
   a. SSH
   b. PGP
   c. HTTPS
   d. SSL/TLS

10. Identify the main advantage of asymmetric encryption over symmetric encryption
   a. Stronger encryption
   b. Simplicity of key management
   c. Faster encryption and decryption
   d. Ability to securely exchange keys over an insecure channel

11. Choose the CORRECT encryption algorithm used for encrypting wireless network traffic, such as Wi-Fi
   a. AES
   b. SSL
   c. WPA
   d. HTTPS

ANSWER!

1. D
2. B
3. C
4. C
5. C
6. D
7. B
8. C
9. D
10. D
11. A

Chapter 3

Security Troubleshooting and Solutions

Chapter 3

Security Troubleshooting and Solutions

3.1 Apply the troubleshooting process to security

The troubleshooting process is used to help resolve security issues. The troubleshooting steps can be used as a guideline to diagnose and repair problems.

There are six main steps in troubleshooting process as follows:

Step 1: Identify the problem
Step 2: Establish a theory of probable causes
Step 3: Test the theory to determine cause
Step 4: Establish a plan of action to resolve the problem and implement the solution
Step 5: Verify full system functionality and implement preventive measures
Step 6: Document finding, actions and outcomes

Computer technicians must be able to analyze a security threat and determine the appropriate method to protect assets and repair damage.

STEP 1

Step 1. Identify the Problem	
Open-ended Questions	• When did the problem start? • What problems are you experiencing? • What websites have you visited recently? • What security software is installed on your computer? • Who else has used your computer recently?
Closed-ended Questions	• Is your security software up to date? • Have you scanned your computer recently for viruses? • Did you open any attachments from a suspicious email? • Have you changed your password recently? • Have you shared your password?

STEP 2

After you have talked to the customer, you can establish a theory of probable causes and create a list of the most common causes of security problems.

Step 2. Establish a Theory of Probable Cause	
Common causes of security problems	• Virus • Trojan Horse • Worm • Spyware • Adware • Grayware or Malware • Phishing scheme • Password compromised • Unprotected equipment rooms • Unsecured work environment

STEP 3

Test theories of probable cause one at a time, starting with the quickest and easiest.

Step 3. Test the Theory to Determine Cause	
Common steps to determine cause	• Disconnect from the network. • Update antivirus and spyware signatures. • Scan computer with protection software. • Check computer for the latest OS patches and updates. • Reboot the computer or network device. • Login as a different user to change your password. • Secure equipment rooms. • Secure work environment. • Enforce security policy.

If the exact cause of the problem has not been determined after all theories have been tested, establish a new theory of probable cause and test it.

STEP 4

After determining the exact cause of the problem, establish a plan of action to resolve the problem and implement a solution. Sometimes quick procedures can determine the exact cause of the problem or even correct the problem. If a quick procedure does not correct the problem, you might need to research the problem further to establish the exact cause.

Step 4: Establish a Plan of Action to Resolve the Problem and Implement the Solution	
If no solution is achieved in the previous step, further research is needed to implement the solution.	• Helpdesk Repair Logs • Other Technicians • Manufacturer FAQs • Technical Websites • Newsgroups • Computer Manuals • Device Manuals • Online Forums • Internet Search

STEP 5

Verify full system functionality and implement any preventive measures if needed.

Step 5: Verify Full System Functionality and if Applicable Implement Preventive Measures	
Verify full functionality	• Re-scan computer to ensure no viruses remain. • Re-scan computer to ensure no spyware remains. • Check the security software logs to ensure no problems remain. • Check computer for the latest OS patches and updates. • Test network and Internet connectivity. • Ensure all applications are working. • Verify access to authorized resources such as shared printers and databases. • Make sure entries are secured. • Ensure security policy is enforced.

STEP 6

List of the tasks required to document the problem and the solution.

Step 6: Document Findings, Actions, and Outcomes	
Document your findings, actions, and outcomes	• Discuss the solution implemented with the customer. • Have the customer verify the problem has been solved. • Provide the customer with all paperwork. • Document the steps taken to solve the problem in the work order and technician's journal. • Document any components used in the repair. • Document the time spent to solve the problem.

3.2 Common Problem and Solutions for Security

Security problems can be attributed to hardware, software or connectivity issues or some combination of the three. The figure is a chart of common security problems and solutions.

Common Problems and Solutions

Problem Symptom	Problem Causes	Possible Solutions
A wireless network is compromised even though 128-bit WEP encryption is in use.	A hacker issuing commonly available wireless hacking tools to crack the encryption.	• Upgrade to WPA2 Encryption. • Add MAC address filtering for older clients that do not support WPA2.
A user is receiving hundreds or thousands of junk emails each day.	The network is not providing detection or protection for the email server from spammers.	Install antivirus or an email software program that removes spam from an email inbox.
An unknown printer repair person is observed looking under keyboards and on desktops.	Visitors are not being monitored properly or user credentials have been stolen to enter the building.	• Contact security or police. • Advise users never to hide passwords near their work area.

Common Problems and Solutions

Problem Symptom	Problem Causes	Possible Solutions
An unauthorized wireless access point is discovered on the network.	A user has added a wireless access point to increase the wireless range of the company network.	• Disconnect and confiscate the unauthorized device. • Enforce security policy by taking action against the person responsible for the security breech.
Users with flash drives are infecting computers on the network with viruses.	The flash drive is infected with a virus and is not scanned by virus protection software when a network computer accesses it.	Set virus protection software to scan removable media when data is accessed.
A Security Alert is displayed.	• The Windows Firewall is turned off. • Virus definitions are out of date. • Malware has been detected.	• Turn on Windows Firewall. • Update virus definitions. • Scan the computer to remove any malware.
Windows Update fails.	• The downloaded update is corrupted. • The update requires a previous update that is not installed.	• Download the update manually and install. • Use System Restore to restore the computer to a time before the attempted update. • Restore the computer from a backup.
System files have been renamed.	The computer has a virus.	• Remove the virus using antivirus software. • Restore the computer from a backup.
Your email contacts report spam coming from your address.	Your email has been hijacked.	• Change your email password. • Contact the email service support to reset the account.

3.3 Protection Against Malicious Software

3.3.1 Malicious software protection program

Malware is malicious software that is installed on a computer without the knowledge or permission of the user. It may take several different anti-malware programs and multiple scans to completely remove all malicious software. Anti-malware available for these purpose are: Anti-virus, anti-spyware, anti-adware and phishing programs.

VIRUS PROTECTION

An antivirus program typically runs automatically in the background and monitors for problems. When a virus is detected, the user is warned, and the program attempts to quarantine or delete the virus.

SPYWARE PROTECTION

Antispyware programs scan for keyloggers, which capture your keystrokes, and other malware so that it can be removed from the computer.

ADWARE PROTECTION

Anti-adware programs look for programs that display advertising on your computer.

PHISHING PROTECTION

Antiphishing programs block the IP addresses of known phishing websites and warn the user about suspicious websites.

It may take several different programs and multiple scans to completely remove all malicious software. Only run one malware protection program at a time.

Signature File Update

New viruses are always being developed, therefore security software must be continually updated. A virus signature is a set of unique data or bits of code that allow it to be identified. Anti-virus software uses a virus signature to find a virus in a computer file system, allowing to detect, quarantine and remove the virus. In the anti-virus software, the virus signature is referred to as a definition file or DAT file.

Step to update signature file

Step 1 Create a Windows Restore Point.
If the file you load is corrupt, setting a restore point allows you to go back to the way things were.

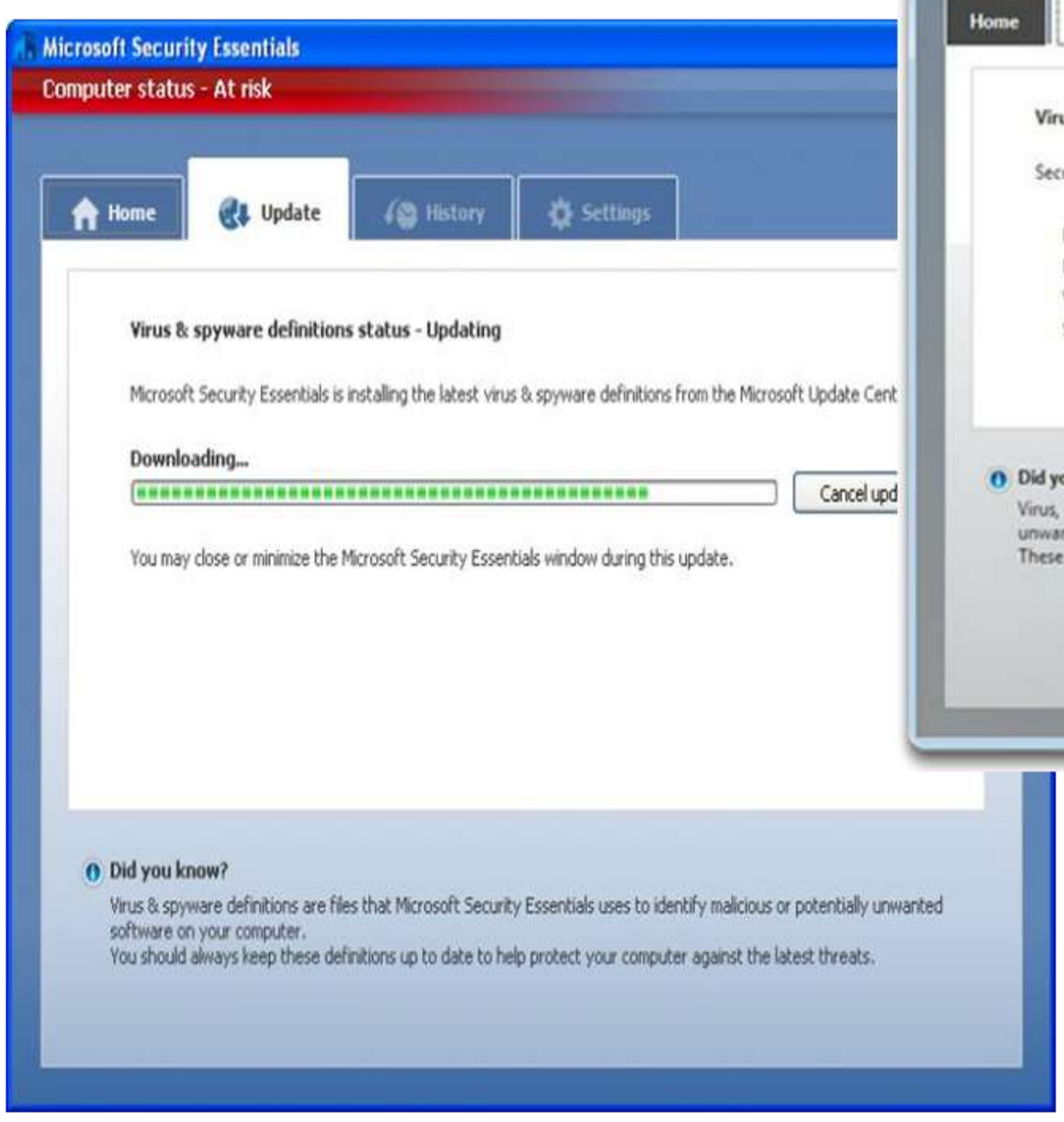
Step 2 Open the antivirus or antispyware program.
If the program is set to execute or obtain updates automatically, you may need to turn the automatic feature off to perform these steps manually.

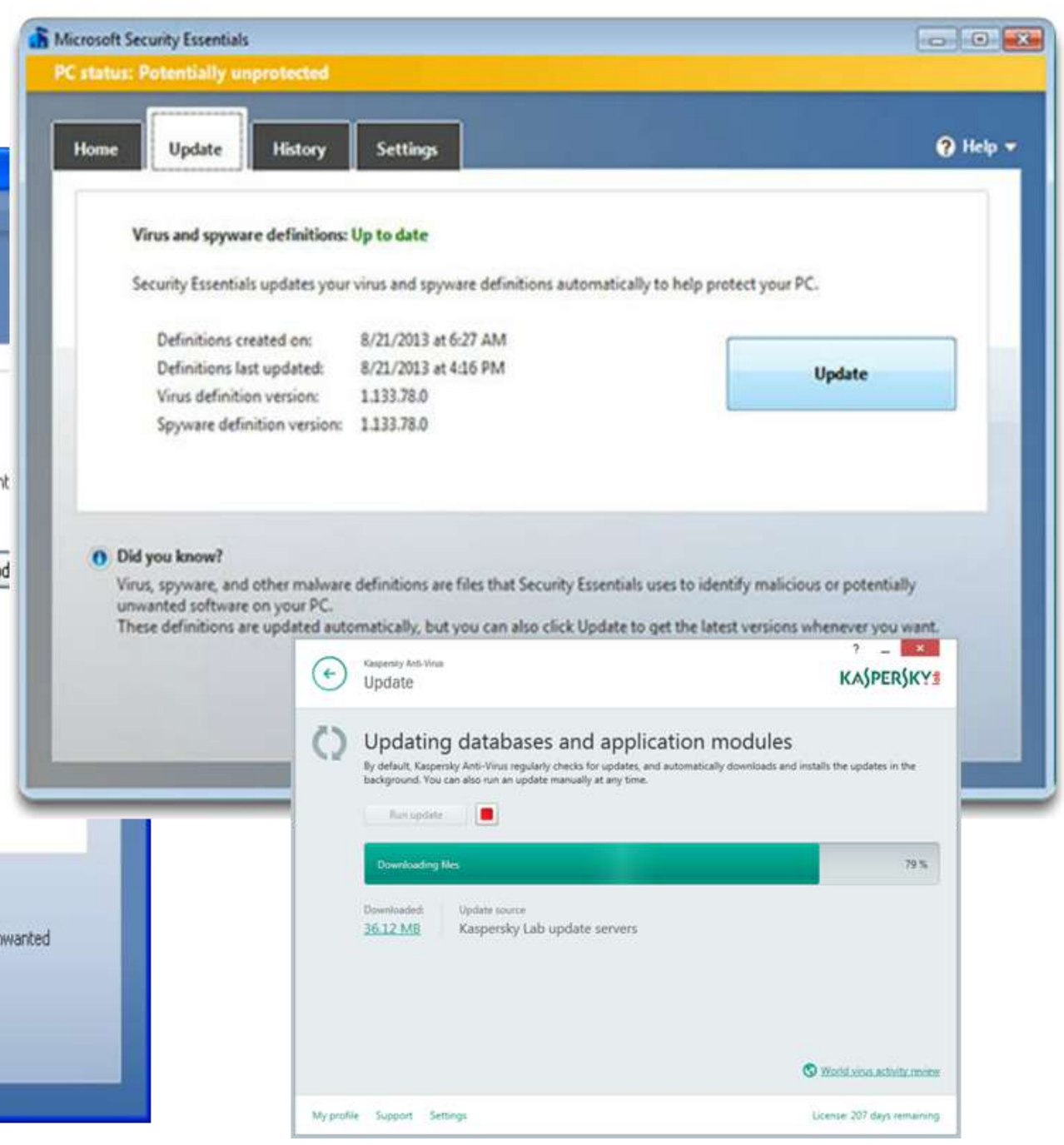
Step 3 Select the **Update** button.

Step 4 After the program is updated, use it to scan the computer.

Step 5 When the scan is complete, check the report for viruses or other problems that could not be treated and delete them yourself.

Step 6 Let the antivirus or antispyware program to automatically update and run on a scheduled basis.





3.4 Protection Physical Equipment

3.4.1 Malicious computer and network equipment protection methods

Physical security is as important as data security. Network infrastructure can be protected by secured telecommunications rooms, equipment cabinets and cages.

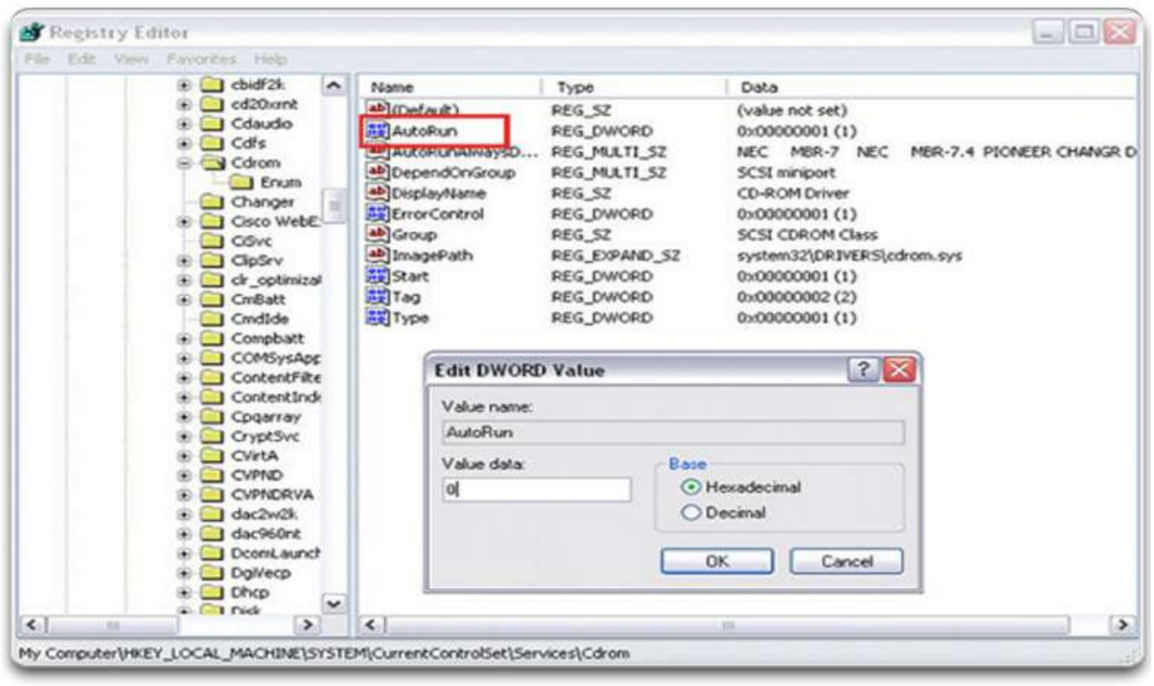
For example:

- Cable locks and security screws for hardware devices
- Wireless detection for unauthorized access points
- Hardware firewalls
- Network management system that detects changes in wiring and patch panels

Another method of hardware security is to disable the AutoRun feature of the operating system. AutoRun automatically follows the instructions in a special file called autorun.inf when it is found on new media.

On Windows, AutoRun is executed first unless it is disabled. If AutoRun is not disabled, it follows the instructions in the autorun.inf file. On Windows Vista and Windows 7, AutoRun is not allowed to bypass AutoPlay. However, on Windows XP, AutoRun bypasses AutoPlay and might launch an application without prompting the user.

This is a security risk because it can automatically run a malicious program and compromise the system, so it is recommended to disable AutoRun.

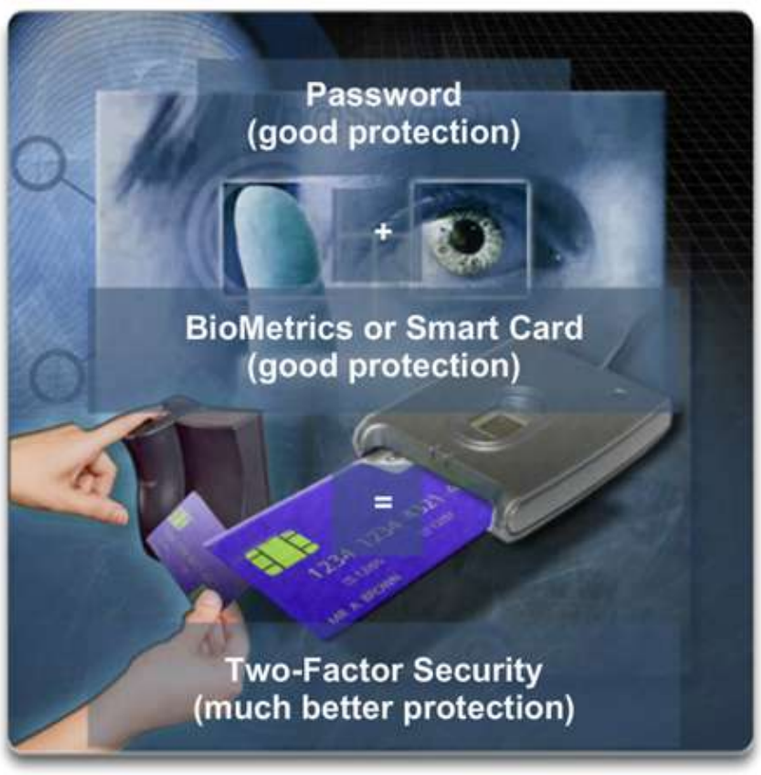


Following steps are required to disable Autorun in Windows XP

- **Step 1** • Select **Start > Run.**
- **Step 2** • Type **regedit** and click **OK.**
- **Step 3** • Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom.**
- **Step 4** • Double-click **AutoRun**. In the Value Data text box, type **0** and click **OK**
- **Step 5** • Close the Registry Editor.
- **Step 6** • You might have to log out and then log back in for this change to take effect.

Two-factor authentication

Two - factor Authentication use an overlapping protection techniques to prevent unauthorized access to sensitive data. An example of two-factor authentication is using a password and a smart card to protect an asset.



For access to facilities, there are several means of protection:
i) Card keys that store user data, including level of access
ii) Biometric sensors that identify physical characteristics of the user, such as fingerprints or retinas
iii) Posted security guard
iv) Sensors, such as RFID tags, to monitor equipment

PIN Card

Factors that determine the most effective security equipment to use to secure equipment and data include:

i) How the equipment is used
ii) Where the computer equipment is located
iii) What type of user access to data is required

For instance, a computer in a busy public place, such as a library, requires additional protection from theft and vandalism. In a busy call center, a server may need to be secured in a locked equipment room. Where it is necessary to use a laptop computer in a public place, a security dongle, ensures that the system locks if the user and laptop are separated.

A USB Security Dongle

3.4.2 Security hardware

There are several methods of physically protecting computer equipment:
i) Use cable locks with equipment.
ii) Keep telecommunication rooms locked.
iii) Fit equipment with security screws.
iv) Use security cages around equipment.
v) Label and install sensors, such as Radio Frequency Identification (RFID) tags, on equipment.
vi) Install physical alarms triggered by motion-detection sensors.
vii)Use webcams with motion-detection and surveillance software

Laptop Cable Lock

Security Screws and Locks

For access to facilities, there are several means of protection:
i) Card keys that store user data, including level of access
ii) Biometric sensors that identify physical characteristics of the user, such as fingerprints or retinas
iii) Posted security guard
iv) Sensors, such as RFID tags, to monitor equipment

SERVICE PACK AND SECURITY PATCHES

Regular security updates are essential to combat new viruses or worms. A technician should understand how and when to install patches and updates.

- **Patches** are code updates that manufacturers provide to prevent a newly discovered virus or worm from making a successful attack.
- A **Service Pack** is a combination of patches and updates.

Following steps are required to update the operating system with a service pack or security patch.

Step 1. Create a restore point prior to installing an update.

Step 2. Check for updates to ensure that you have the latest ones.

Step 3. Download updates using Automatic Updates or from the operating system manufacturer's website.

Step 4. Install the update.

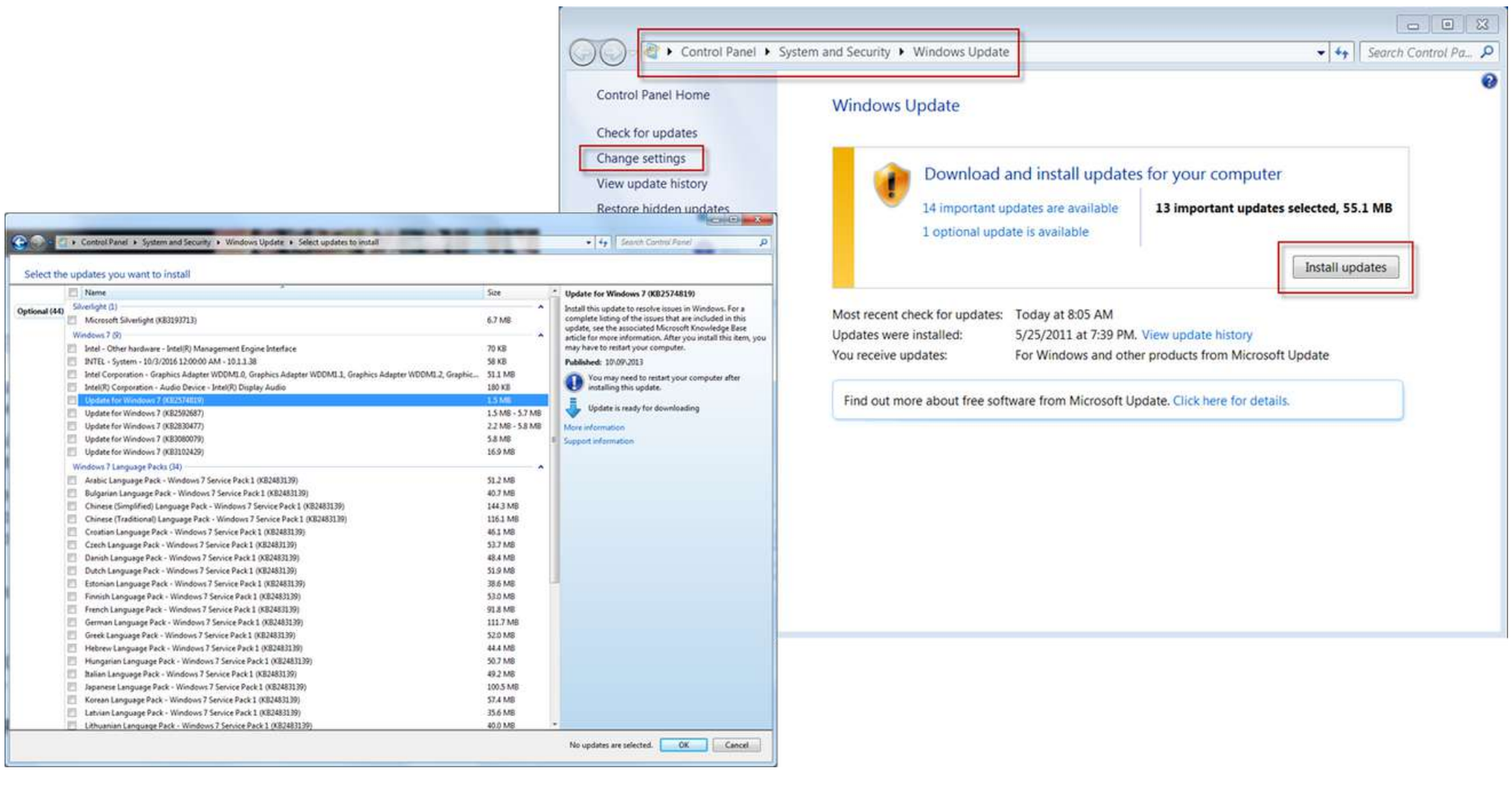
Step 5. Reboot the computer if necessary.

Step 6. Ensure that the computer is operating properly.

Windows automatically downloads and installs updates to operating systems by default. However, the updates might conflict with an organization's security policy or other settings on a computer.

The following Windows options allow you to control when software is updated.

Automatic	Downloads and installs updates automatically without user intervention.
Only download updates	Downloads the updates automatically, but the user is required to install them.
Notify me	Notifies the user that updates are available and gives the option to download and install.
Turn off automatic updates	Prevents any checking for updates.



QUIZ YOURSELF!

1. Identify the recommended practice for protecting the computer's data during a power outage
   a. Use a portable hard drive
   b. Keep data on a magnetic tape
   c. Keep a backup of data on a USB flash drive
   d. Invest in an uninterruptible power supply (UPS)

Ali are concerned about physical damage to his computer equipment during a move

2. Select the CORECT preventive measure Ali need to take to overcome the physical damage
   a. Increase the screen resolution
   b. Apply a screen protector to the monitor
   c. Hire professional movers to handle the equipment
   d. Use bubble wrap or foam padding to protect fragile components

Your computer is displaying the "Blue Screen of Death" (BSOD)

3. Select the CORRECT step to troubleshoot the issue based on the information above
   a. Panic and unplug all cables
   b. Replace the computer's hard drive
   c. Note the error code and research it for possible solutions
   d. Restart the computer and hope the issue doesn't reoccur

4. You're troubleshooting a slow internet connection. Identify the step if the issue is with the ISP or internal network
   a. Restart the router
   b. Change the Wi-Fi password
   c. Unplug and replug all cables
   d. Test the connection with a different device

5. You suspect that your computer's performance has slowed down due to malware. Identify the step to troubleshoot and fix the issue
   a. Buy a new computer
   b. Increase the screen resolution
   c. Reinstall the operating system
   d. Scan the computer with antivirus and anti-malware software

6. Your smartphone is overheating and experiencing battery drain. Identify the potential solution
   a. Delete all text messages and call logs
   b. Keep the phone plugged in at all times
   c. Install more apps to improve performance
   d. Decrease the screen brightness and close background apps

7. When troubleshooting a computer that won't start, identify the first step need to take
   a. Update all device drivers
   b. Replace the motherboard
   c. Reinstall the operating system
   d. Check the power supply and ensure it's plugged in

8. You're unable to access a website. Identify the common initial troubleshooting step
   a. Reboot the router
   b. Install a new web browser
   c. Reformat the computer's hard drive
   d. Call the Internet Service Provider (ISP)

9. Your printer is not responding when you send a print job. Identify the troubleshooting step need to take to resolve the issue
   a. Restart the computer
   b. Reload the paper tray
   c. Check ink levels in the cartridges
   d. Replace the printer with a new one

10. You suspect a hardware issue with your computer's RAM. Identify the potential troubleshooting step
   a. Replace the CPU cooler
   b. Delete all files in the Recycle Bin
   c. Update your graphics card driver
   d. Remove and reseat the RAM modules in their slots

11. You're troubleshooting an issue where a software application crashes frequently. Identify the step might help resolve this
   a. Replace the monitor
   b. Restart your computer
   c. Upgrade your computer's GPU
   d. Check for software updates or patches

ANSWER!

1. D
2. D
3. C
4. D
5. D
6. D
7. D
8. A
9. C
10. D
11. D

Chapter 4

IT PROFESSIONAL

Chapter 4

IT Professional

4.1 Communication skill and IT professional

An **IT professional** must be familiar with the legal and ethical issues that are inherent in this industry. They also need to learn on how to use a good communication skills to handle the customer.

4.1.1 Communication Skills, Troubleshooting and Professional Behaviour

A knowledgeable technician who uses good communication skills will always be in demand in the jobs market. As technical knowledge increases, so does ability to quickly determine a problem and find a solution. A technician should establish a good rapport with the customer since a relaxed customer is better able to explain the details of the problem.

The technician has access to several communication and research tools. Any of these resources can be used to help gather information for the troubleshooting process:

Technician Resources

- Personal Experience
- Scripts
- Websites
- Search Engines
- Online FAQs
- Co-workers
- Support vendors
- Diagnostic repair tools
- Manufacturer manuals
- Email

Communication Skills and Professionalism

A technician's professionalism and good communication skills will enhance their creditability with the customer. Successful technicians control their own reactions and emotions from one customer call to the next. A good rule for all technicians to follow is that a new customer call means a fresh start.

4.2 Practice Proper Attitude While Working with a Customer

Determine customer problem

The first tasks of the technician is to determine the type of computer problem that the customer is experiencing. There are three rules at the beginning of conversation:
i) Know - Call your customer by name.
ii) Relate - Use brief communication to create a one-to-one connection between you and your customer.
iii) Understand - Determine the customer's level of knowledge about the computer to know how to effectively communicate with the customer.

The technician should:
i) Practice active listening skills.
ii) Do not interrupt the customer.
iii) Listen carefully to what the other person is saying, and let them finish their thought.
iv) After the customer has explained the problem, clarify what the customer has said.
v) Ask some follow-up questions, if needed.
vi) Use all of the information to complete the work order.

Three rules to begin a conversation.
i) Know
ii) Relate
iii) Understand

Displaying Professional Behavior with Customer

When dealing with customers, it is necessary to be professional in all aspects. Technicians need to handle customers with respect and prompt attention. On a phone call, they need to know how to:

i) Place a customer on hold.
ii) Transfer a customer without losing the call.
iii) Help the customer focus on and communicate the problem.
iv) Stay positive by focusing on what you can do to help.
v) Convey an interest in helping the customer.

The process to follow before put a customer on hold

How to Put a Customer on Hold

Do	Do Not
• Let the customer finish talking. • Explain that you will have to put the customer on hold and why. • Ask if it is all right to put the customer on hold. • Once given consent, tell the customer you will be just a minute.	• Interrupt. • Abruptly put the customer on hold. • Put on hold without an explanation and the customer's consent.

The process for transferring a call

How to Transfer a Call

Do	Do Not
• Let the customer finish talking. • Explain that you will have to transfer the call, tell the customer to whom, and why. • Tell the customer the number you are transferring the customer to. (e.g. #142) • Ask if it is all right to transfer the call now. • Once given consent, begin the transfer. • Tell the new technician who you are, the ticket number, and the name of the customer.	• Interrupt. • Abruptly transfer the call. • Transfer without an explanation and the customer consent. • Transfer without informing the new technician.

The following is a list of behaviors to avoid when communicating with a customer :

- Do not minimize a customer's problems.
- Do not use jargon, abbreviations, acronyms, and slang.
- Do not use a negative attitude or tone of voice.
- Do not argue with customers or becoming defensive.
- Do not say culturally insensitive remarks.
- Do not be judgmental or insulting or call the customer names.
- Avoid distractions and do not interrupt when talking with customers.
- Do not take personal calls when talking with customers.
- Do not talk to co-workers about unrelated subjects when talking with the customer.
- Avoid unnecessary holds and abrupt holds.
- Do not transfer a call without explaining the purpose of the transfer and getting customer consent.
- Do not use negative remarks about other technicians to the customer.

Keeping the Customer Focused on the Problem

Recognizing these traits will help them to manage the call accordingly.

i) Talkative Customer
ii) Rude Customer
iii) Angry Customer
iv) Knowledgeable Customer
v) Inexperienced Customer

Clearly communicate the expected timeline for resolution and provide updates to manage customer expectations throughout the troubleshooting process.

TALKATIVE CUSTOMER

A talkative customer discusses everything except the problem and uses the call to socialize.

Talkative Customer

Do:

- Allow the customer to talk for one minute.
- Gather as much information about the problem as possible.
- Politely step in to refocus the customer. This is the exception to the rule of never interrupting a customer.
- Ask as many closed-ended questions as you need to once you have regained control of the call.

Do Not:

Encourage non-problem related conversation by asking social questions such as "How are you today?".

RUDE CUSTOMER

A rude customer complains during the call, makes negative comments, may be abusive and uncooperative, and may be easily aggravated.

Rude Customer

Do:

- Listen very carefully, as you do not want to ask the customer to repeat any information.
- Follow a step-by-step approach to determining and solving the problem.
- If the customer has a favorite technician, try to contact that technician to see if they can take the call. As an example, tell the customer, "I can either help you right now or see if (the preferred technician) is available. They will be available in two hours. Will that be acceptable?" If the customer wants to wait for the other technician, record this in the ticket.
- Apologize for the wait time and the inconvenience, even if there has been no wait time.
- Reiterate that you want to solve their problem as quickly as possible.

Rude Customer

Do Not:

- Ask the customer to do any obvious steps if there is any way you can determine the problem without them.
- Be rude to the customer, even if they are rude to you.

ANGRY CUSTOMER

An angry customer talks loudly, tries to speak when the technician is talking, usually frustrated and upset that they have to call somebody to fix the problem.

Angry Customer

Do:

- Let the customer tell their problem without interrupting, even if they are angry. This allows the customer to release some of their anger before you proceed.
- Sympathize with the customer's problem.
- Apologize for wait time or inconvenience.

Do Not:

- If at all possible, try not to put this customer on hold or transfer the call.
- Spend call time talking about what caused the problem (rather, redirect the conversation to solving the problem).

KNOWLEDGEABLE CUSTOMER

A knowledgeable customer wants to speak with a technician that is equally experienced in computers and usually tries to control the call.

Knowledgeable Customer

Do:

- If you are a level one technician, you might try to set up a conference call with a level two technician.
- Give the customer the overall approach to what you are trying to verify.

Do Not:

- Follow a step-by-step process with this customer.
- Ask to check the obvious, such as the power cord or the power switch. As an example, you could suggest a reboot instead.

INEXPERIENCED CUSTOMER

An inexperienced customer has difficulty describing the problem and may not able to follow directions correctly.

Inexperienced Customer

Do:
- Use a simple step-by-step process of instructions.
- Speak in plain terms.

Do Not:
- Use industry jargon.
- Be condescending to your customer or belittle them.

Proper netiquette

For email and text communications, there is a set of personal and business etiquette rules called Netiquette.

Basic Netiquette

- Be pleasant and polite.
- Begin each email, even within a thread, with an appropriate greeting.
- Never send chain letters via email.
- Do not send or reply to flames.
- Use mixed case. UPPER CASE IS CONSIDERED SHOUTING.
- Check grammar and spelling before you post.
- Be ethical.
- Never mail or post anything you would not say to someone's face.

4.3 Explain Employee Best Practice

Time and Stress Management Technique

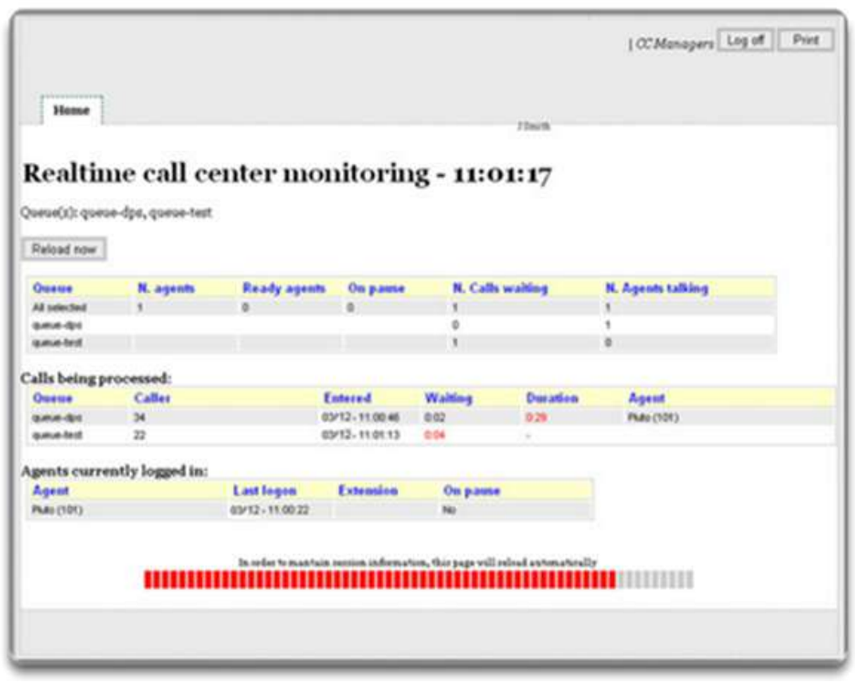
WORKSTATION ERGONOMICS

- Make sure that your desk layout works well.
- Have your headset and phone in a position that is easy to reach and easy to use.
- Adjust your chair to a comfortable height.
- Adjust your monitor to a comfortable angle.
- Place your keyboard and mouse in a comfortable position.
- Minimize external distractions such as noise.

TIME MANAGEMENT

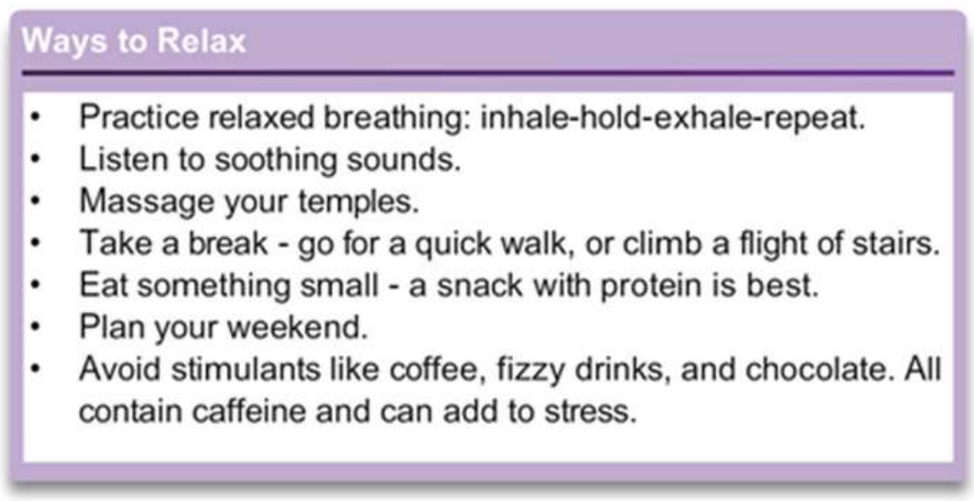
Follow the business policy of company.

- Keep a list of callback customers.
- Do not give favorite customers faster or better service.
- When reviewing the call boards, do not take only the easy customer calls.
- Do not take the call of another technician, without permission.



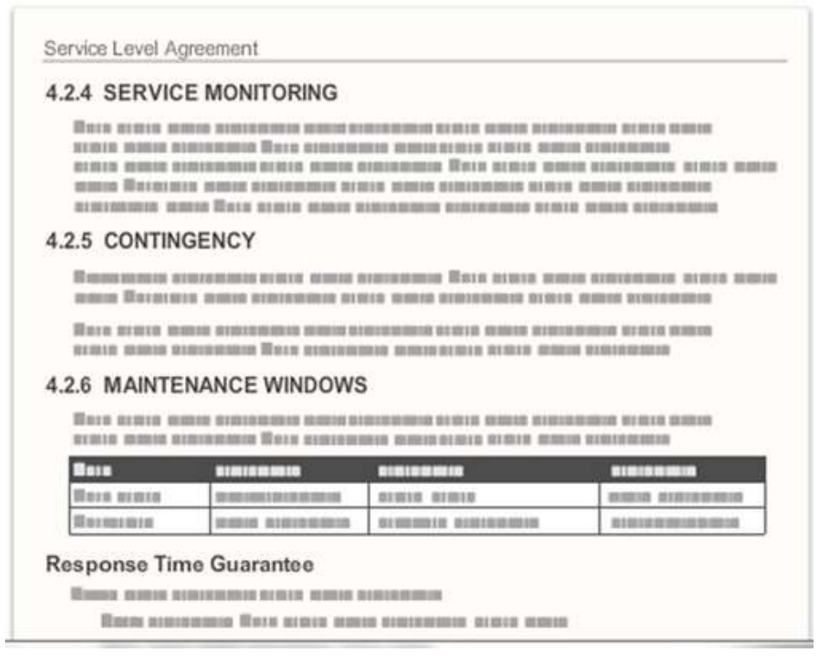
STRESS MANAGEMENT

- Do not carry any frustrations from one call to the next.
- Do some physical activity to relieve stress.
- Stand up and take a short walk.
- Do a few simple stretch movements or squeeze a tension ball.
- Take a break and try to relax.



Service Level Agreement (SLA)

When dealing with customers, it is important to adhere to that customer's service level agreement (SLA). An SLA is a contract that defines expectations between an organization and the service vendor to provide an agreed-on level of support. A legal agreement that contains the responsibilities and liabilities of all parties involved.



Some of the contents of an SLA usually include the following:

i) Response time guarantees (often based on type of call and level of service agreement)
ii) Equipment and software that is supported
iii) Where service is provided
iv) Preventive maintenance
v) Diagnostics
vi) Part availability (equivalent parts)
vii) Cost and penalties
viii)Time of service availability (for example, 24x7 or Monday to Friday, 8 a.m. to 5 p.m. EST)

CUSTOMER CALL RULES

Most call centers have very specific rules on how to handle customer calls:
i) Maximum time on call (example: 15 minutes)
ii) Maximum call time in queue (example: 3 minutes)
iii) Number of calls per day (example: minimum of 30)
iv) Passing calls on to other technicians (example: only when absolutely necessary and not without that technician's permission)
v) What you can and cannot promise to the customer (see that customer's SLA for details)
vi) When to follow the SLA and when to escalate to management

CALL CENTER EMPLOYEE RULES

There are also rules to cover general daily activities of employees:

- Arrive at your workstation on time and early enough to become prepared, usually about 15 to 20 minutes before the first call.
- Do not exceed the allowed number and length of breaks.
- Do not take a break or go to lunch if there is a call on the board.
- Do not take a break or go to lunch at the same time as other technicians (stagger breaks among technicians).
- Do not leave an ongoing call to take a break, go to lunch, or take some personal time.
- Make sure that another technician is available if you have to leave.
- Contact the customer if you are going to be late for an appointment.
- If no other technician is available, check with the customer to see if you can call back later.
- Do not show favoritism to certain customers.
- Do not take another technician's calls without permission.
- Do not talk negatively about the capabilities of another technician.

CUSTOMER SATISFACTION

The following rules should be followed by all employees to ensure customer satisfaction:

- Set and meet a reasonable timeline for the call or appointment and communicate this to the customer.
- Communicate service expectations to the customer as early as possible.
- Communicate the repair status with the customer, including explanations for any delays.
- Offer different repair or replacement options to the customer, if applicable.
- Give the customer proper documentation on all services provided.
- Follow up with the customer at a later date to verify satisfaction.

4.4 Understand Ethical and Legal Issues in the IT Industry

Ethical and legal considerations

Computer Forensics is the collection and analysis of data from computer systems, networks wireless communications and storage devices as part of a criminal investigation.

Illegal computer or network usage

Depending on the country, illegal computer or network usage may include:

- Identity theft
- Using a computer to sell counterfeit goods
- Using pirated software on a computer or network
- Using a computer or network to create unauthorized copies of copyrighted materials, such as movies, television programs, music and video games
- Using a computer or network to sell unauthorized copies of copyrighted materials
- Pornography

Type of Data Collection

There are two basic types of data that need to be collected when conducting computer forensics procedures which is persistent data and volatile data.
i) Persistent data - Stored on local drive, when computer turned off this data is preserved
ii) Volatile data - Stored in Ram and cache, disappears when computer is turned off.

Cyber law

- Cyber law is a term to describe the international, regional, country and state laws that affect computer security professionals.
- Cyber laws explain the circumstances under which data (evidence) can be collected from computers, data storage devices, networks, and wireless communications.
- IT professionals should be aware of the cyber laws in their country, region or state.

Documentation

- The documentation required by a system administrator and a computer forensics expert is extremely detailed.
- They must document not only what evidence was gathered, but how it was gathered and with which tools.
- Document as much information about the security incident as possible. These best practices provide an audit trail for the information collection process.
- The following, at a minimum, should be documented if illegal activity is discovered:
- Intial reason for accessing the computer or network
- Time and date
- Peripherals that are connected to the computer
- All network connections
- Physical area where the computer is located
- Illegal material found
- Illegal activity that you have witnessed (or you suspect has occurred)
- Which procedures you have executed on the computer or network

Chain of custody

For evidence to be admitted, it must be authenticated. A system administrator should be able to prove how this evidence was collected, where it has been physically stored and who has had access to it between the time of collection and its entry into the court proceedings

4.5 Understand Call Center Technicians Task

Call center

A **call center** environment is usually very professional and fast-paced. It is a help desk system where customers call in and are placed on a callboard. The available technicians take the customer calls. All the computers in a call center have help desk software. The technicians use this software to manage many of their job functions.

Each call center has business policies regarding call priority. A sample chart of how calls can be named, defined, and prioritized.

Call Prioritization

Name	Definition	Priority
Down	The company cannot operate any of its computer equipment.	1 (Most Urgent)
Hardware	One (or more) of the company's computers is not functioning correctly.	2 (Urgent)
Software	One (or more) of the company's computers is experiencing software or operating system errors.	2 (Urgent)
Network	One (or more) of the company's computers cannot access the network.	2 (Urgent)
Enhancement	There has been a request from the company for additional computer functionality.	3 (Important)

Maintaining an unbroken chain of custody is crucial to ensure that evidence remains untampered and admissible in court.

TECHNICIANS LEVELS

There are two level of technicians which is level one technician and level two technician.

Level One technicians responsibility

Level one technicians gather pertinent information from the customer. The technician has to accurately enter all information into the ticket or work order.

Information Checklist

- Contact information
- What is the manufacturer and model of computer?
- What OS is the computer using?
- Is the computer plugged in to the wall or running on battery power?
- Is the computer on a network? If so, is it a wired or wireless connection?
- Was any specific application being used when the problem occurred?
- Have any new drivers or updates been installed recently? If so, what are they?
- Description of the problem
- Priority of problem

If the level one technician cannot solve the problem, it is escalated to a level two technician.

Level Two technicians responsibility

Level two technicians ussually more knowledgeable about technology. They may have been working for the company for a longer period of time. When a problem cannot be resolved within a predetermined amount of time, the level one technician prepares an escalated work order to level two technicians. Level two technicians receives escalated work orders from level-one technicians and calls the customer back to ask any additional questions. They also may use remote access software to access the customer's computer to diagnose the problem and possibly to resolve the issue.

Escalated Work Order

QUIZ YOURSELF!

1. Identify the primary role of a level one IT technician
   a. Overseeing cybersecurity protocols
   b. Designing complex software applications
   c. Managing the organization's network infrastructure
   d. Providing technical support and assistance to end-users

Abu is a technician level 2. He encounters a problem that he can't resolve. Abu need to take the next step.

2. Select the CORECT step Abu need’s to take to solve the problem
   a. Pretend to be a level three technician
   b. Delete all the records related to the problem
   c. Create a PowerPoint presentation about the problem
   d. Escalate the issue to a level three technician or higher

"A user is unable to access a shared network drive"

3. Identify who is best suited to help the user
   a. Level two technician
   b. Level one technician
   c. Outsourced IT support
   d. Chief Executive Officer (CEO)

4. Select the kind of issues are typically escalated to a level two technician
   a. Printer paper jams
   b. Office furniture procurement
   c. Password resets and email setup
   d. Server configuration and network troubleshooting

5. Select the CORRECT primary responsibility of a level two IT technician
   a. Resolving more complex technical problems
   b. Managing the company's finances and budget
   c. Assisting end-users with basic technical issues
   d. Developing custom software solutions for the organization

6. Identify what should a technician do when interacting with the customer to determine the customer's problem
   a. Drink coffee
   b. Fill out the paper
   c. Listen to him/her
   d. Explain the theory first

7. Choose the primary role of a level one IT technician in terms of user support

a. Handling server maintenance
b. Managing the organization's finances
c. Providing in-depth software development
d. Offering basic troubleshooting and technical assistance

8. Identify which of the following would be given a priority level of urgent for call service

a. A customer would like to review and make changes to their SLA
b. One or more of the company's computers cannot access the network
c. A customer would like to discuss options for expanding the number of computers it has
d. One or more of the company's computer needs software updates unrelated to security or functionality

9. Level two technicians will often have access to resources that level ones do not. Select which of the following is an example that would be available to both level one and level two technicians

a. Remote access software
b. As much time as is necessary to fix the problem
c. Software database to search for common solutions
d. The option to travel to the remote site to fix the problem if necessary

10. Identify the common task for a level one technician when dealing with software-related issues

a. Monitoring network traffic
b. Setting up an entire data center
c. Debugging complex software code
d. Installing and updating software applications

11. A critical server in the data center experiences a hardware failure. Identify the level of technician is most likely to handle this emergency

a. Level two technician
b. Level one technician
c. Level three technician
d. Chief Executive Officer (CEO)

ANSWER!

1. D
2. D
3. B
4. D
5. A
6. C
7. D
8. B
9. C
10. D
11. B

Appendix

References

References

1. Ciampa, M. (2020). CompTIA Security+ Guide to Network Security Fundamentals. United States: Cengage Learning.
2. Chapple, M., Seidl, D. (2021). CompTIA Security+ Study Guide: Exam SY0-601. United Kingdom: Wiley.
3. Whitman, M. E., Mattord, H. J. (2021). Principles of Information Security. United States: Cengage.
4. Docter, Q. (2018). CompTIA IT Fundamentals (ITF+) Study Guide: Exam FC0-U61. United States: Wiley.
5. https://www.tripwire.com/state-of-security/vulnerability-management/3-types-of-network-attacks/
6. https://www.youtube.com/watch?v=4t4kBkMsDbQ
7. https://www.youtube.com/watch?v=PSA8D4kxmeI
8. Krutz, R. L., Vines, R. D. (2003). Advanced CISSP Prep Guide: Exam Q&A. Germany: Wiley.
9. Small, M. J. (2019). A Quick Guide To Understanding IT Security Basics For IT Professionals. (n.p.): Amazon Digital Services LLC - Kdp.
10. Swanson, C. (2020). Professional Security Management: A Strategic Guide. United Kingdom: Taylor & Francis.
11. Miller, A. (2022). Cybersecurity Career Guide. United Kingdom: Manning.
12. Barker, J. (2020). Confident Cyber Security: How to Get Started in Cyber Security and Futureproof Your Career. United Kingdom: Kogan Page.
13. Viega, J., McGraw, G. (2001). Building Secure Software: How to Avoid Security Problems the Right Way. India: Pearson Education.
14. Nagelhout, R. (2016). Digital Era Encryption and Decryption. United States: Rosen Publishing Group.

POLITEKNIK
MALAYSIA
METrO KUALA LUMPUR

ISBN 978-967-0074-09-2