1.1 Security principles

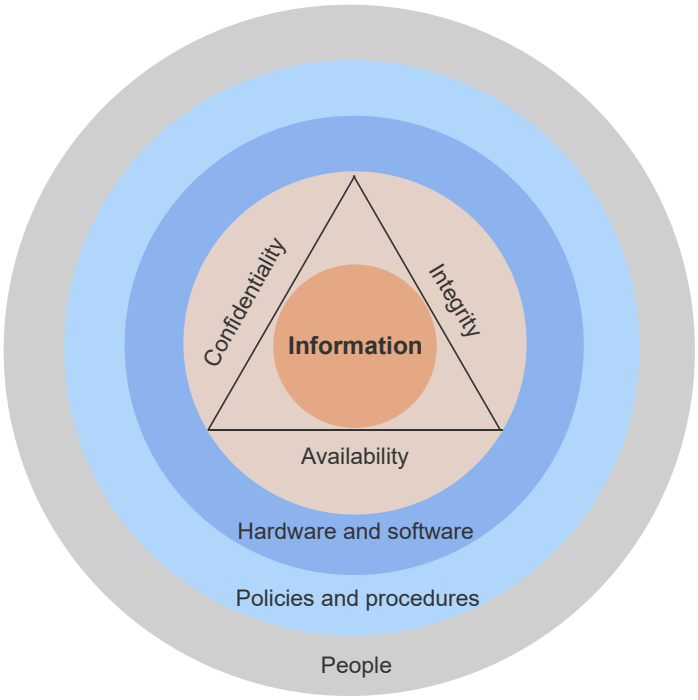
Information security

Information security, or ***InfoSec***, is the practice of protecting information from unauthorized access, disclosure, disruption, destruction, or modification. The goal of InfoSec is to preserve three information security principles:

- ***Confidentiality*** is the security principle that ensures information is only disclosed or made available to authorized users. Ex: A customer's credit card number used in an online transaction should not be disclosed to other customers.
- ***Integrity*** is the security principle that ensures information is only modified in an authorized manner. Ex: A bank customer should not be able to increase the customer's account balance without adding funds to the account.
- ***Availability*** is the security principle that ensures information is accessible by authorized users whenever required. Ex: A patient's medical records should be available to the patient's doctors whenever the doctors need to access the records.

Information security encompasses the hardware and software systems, policies, procedures and people that help prevent, detect, and remediate attacks aimed at compromising the confidentiality, integrity and availability of information.

PARTICIPATION ACTIVITY 1.1.1: Information security principles.



Animation content:

Four concentric circles. The most inner circle is labeled information and is inside a triangle. The triangle sides are labeled confidentiality, integrity and availability. The second circle is labeled hardware and software. The third circle is labeled policies and procedures. The fourth circle is labeled

people.
Step 1: The goal of information security is to preserve the confidentiality, integrity and availability of information (also known as the CIA triad).
Step 2: The three security principles are preserved using various hardware and software systems and tools, such as firewalls, anti-virus software and biometric authentication systems.
Step 3: Policies and procedures are established to ensure information is handled securely, such as instituting password and acceptable use policies and conducting security audits.
Step 4: People are trained to securely use hardware and software systems and to be able to recognize threats to information through security awareness and education programs.

Animation captions:

1. The goal of information security is to preserve the confidentiality, integrity and availability of information (also known as the CIA triad).
2. The three security principles are preserved using various hardware and software systems and tools, such as firewalls, anti-virus software and biometric authentication systems.
3. Policies and procedures are established to ensure information is handled securely, such as instituting password and acceptable use policies and conducting security audits.
4. People are trained to securely use hardware and software systems and to be able to recognize threats to information through security awareness and education programs.

PARTICIPATION ACTIVITY 1.1.2: Information security.

Select the compromised information security principle in each scenario.

1) A patient's medical records are posted on a hospital's public website.
   - ○ Confidentiality
   - ○ Integrity
   - ○ Availability

2) The only copy of a file containing confidential information is deleted from a USB drive.
   - ○ Confidentiality
   - ○ Integrity
   - ○ Availability

3) A company's financial records are modified by an employee who is authorized to view, but not modify the records.
   - ○ Confidentiality
   - ○ Integrity
   - ○ Availability

4) Bank account balances are not accessible on a mobile banking app.
   - ○ Confidentiality

- Integrity
- Availability

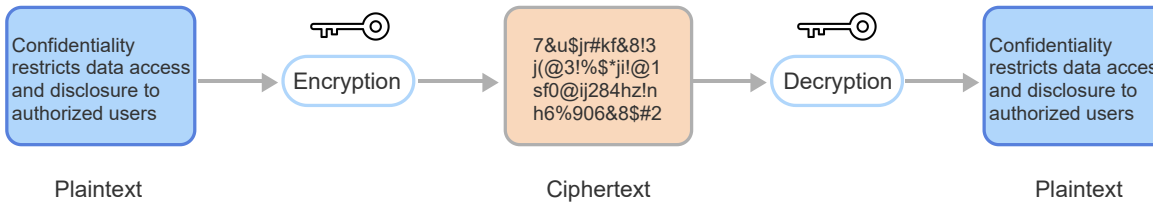
5) A file containing the personally identifiable information (PII) of a company's customers is emailed to an outside vendor by mistake.
   - Confidentiality
   - Integrity
   - Availability

Confidentiality

Confidentiality means restricting information access and disclosure to authorized users and includes measures for protecting proprietary information and personal privacy. Threats to confidentiality are wide ranging, from stealing passwords and capturing network traffic to conducting social engineering attacks. Confidentiality breaches may also be unintentional, such as emailing sensitive information to wrong recipients and publishing private information on public websites.

Confidentiality controls protect data from unauthorized access and use and include encryption, access control lists and authentication systems. Ex: Encrypting an email protects the confidentiality of the email's content. Additional confidentiality controls include administrative solutions such as security policies and user awareness and training programs. Physical controls such as security gates and locks restrict access to facilities and equipment that process information.

PARTICIPATION ACTIVITY 1.1.3: Encryption for preserving data confidentiality.



Animation content:

Three rectangles in a row with two ovals in between the rectangles. Each oval has an image of a key on top. The leftmost rectangle is labeled plaintext and has some data written inside, the middle rectangle is labeled ciphertext and has scrambled data written inside, the rightmost rectangle is labeled plaintext and has the same data as the leftmost rectangle written inside.
Step 1: Confidentiality means data should only be disclosed to authorized users. Encryption can be

used to preserve data confidentiality.
Step 2: The unencrypted data is known as plaintext. Plaintext is encrypted using an encryption algorithm and a key.
Step 3: The output of an encryption algorithm is ciphertext. Ciphertext is stored and/or transmitted instead of plaintext. Since ciphertext is encrypted (scrambled), the original data is not disclosed to unauthorized users.
Step 4: The ciphertext can be decrypted with the decryption algorithm and the decryption key. Only authorized users have access to the decryption key. The decryption algorithm's output is the plaintext.

Animation captions:

1. Confidentiality means data should only be disclosed to authorized users. Encryption can be used to preserve data confidentiality.
2. The unencrypted data is known as plaintext. Plaintext is encrypted using an encryption algorithm and a key.
3. The output of an encryption algorithm is ciphertext. Ciphertext is stored and/or transmitted instead of plaintext. Since ciphertext is encrypted (scrambled), the original data is not disclosed to unauthorized users.
4. The ciphertext can be decrypted with the decryption algorithm and the decryption key. Only authorized users have access to the decryption key. The decryption algorithm's output is the plaintext.

PARTICIPATION ACTIVITY 1.1.4: Confidentiality.

1) Which security control can be used to protect the confidentiality of information transmitted over a wireless connection?
   - An access control list
   - An authentication system
   - Encryption

2) Why would unencrypted data on a network compromise the confidentiality principle?
   - Because the data may be modified by unauthorized users
   - Because the data may be made available to authorized users
   - Because the data may be made available to unauthorized users

3) Which one of the following scenarios may compromise the confidentiality of information?
   - Modifying the contents of an encrypted file containing a patient's medical records

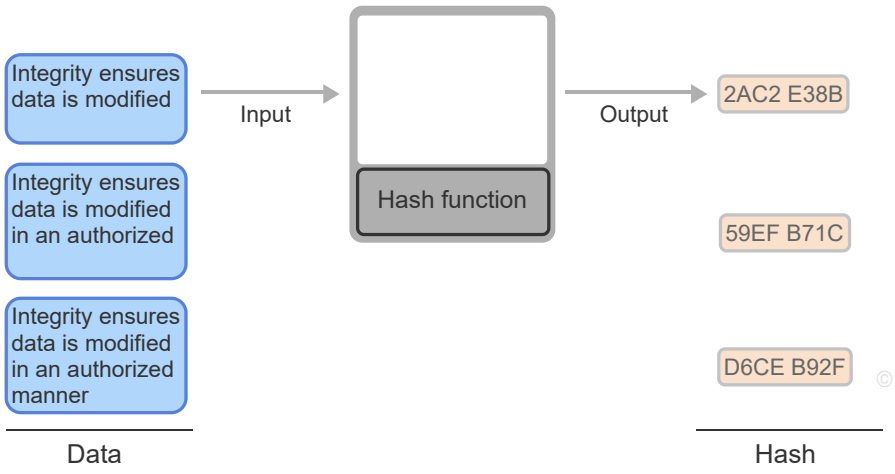
- Sending encrypted national security secrets over a wireless network
- Leaving trade secrets displayed on an unattended computer monitor

Integrity

Integrity means information cannot be modified in an unauthorized manner. Data at rest (data stored on systems), data in transit (data transmitted between systems), and data in use (data in processing) should be protected to maintain data integrity. Integrity breaches may be malicious such as a virus that corrupts the contents of a file, or unintentional such as data loss resulting from a system malfunction or user error.

Integrity controls protect data from unauthorized modification and ensure the correctness and completeness of data. Access control can help prevent authorized users from making unauthorized changes. Hash verifications and digital signatures help ensure that transactions are authentic and that data has not been modified or corrupted. Administrative solutions aimed at ensuring data integrity include user training and data access policies.

PARTICIPATION ACTIVITY 1.1.5: Hash function for preserving data integrity.



Animation content:

Static image: A box representing a hash function in the middle with one arrow on the left of the box pointing towards the box and one arrow on right of the box pointing to the right. Three rectangles on the left of the hash function box with each rectangle having data of different sizes written inside. Three rectangles on the right of the hash function box with each rectangle having data of the same

size written inside.
Step 1: A hash function maps a variable-length string to a fixed-size value called a hash.
Step 2: The output of a hash function is always the same size regardless of the input string size.
Step 3: Since any changes to a hash function's input string results in a different hash, a hash function can be used to detect data modifications and validate data integrity.

Animation captions:

1. A hash function maps a variable-length string to a fixed-size value called a hash.
2. The output of a hash function is always the same size regardless of the input string size.
3. Since any changes to a hash function's input string results in a different hash, a hash function can be used for detecting data modifications and validating data integrity.

PARTICIPATION ACTIVITY | 1.1.6: Integrity.

1) Why does an operating system preserve the integrity of user files by assigning file and directory permissions?

   - Because all users should be able to modify the files
   - Because the files should not be accessed
   - Because only authorized users should be able to modify the files

2) Why would a software vendor publish the hash of a software patch along with the patch?

   - to ensure users that the patch is available whenever the users want to download the patch
   - to make sure that only authorized users can download and install the patch
   - to enable users to verify that the patch has not been modified before installing the patch

3) A database transaction log contains a history of all data modifications in a database. How can a transaction log be used to preserve data integrity after a database server crashes due to a hardware failure?

   - A transaction log can be used to remove all unauthorized modifications to the database.
   - A transaction log can be used to modify all the previous database

transactions.

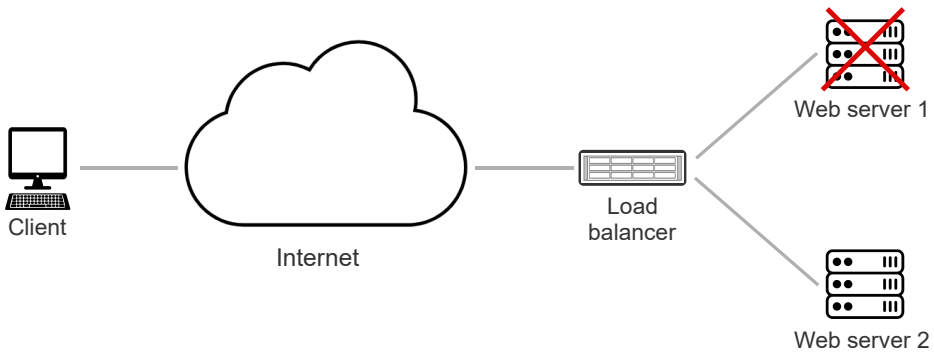
A transaction log can be used to reapply all the previous modifications to the database.

Availability

Availability means information must be accessible whenever needed. Threats to availability may be non-malicious including hardware failures and disruptions caused by natural events such as hurricanes and earthquakes. Malicious attacks include various forms of sabotage intended to cause harm to an organization by denying users' access to information, such as distributed denial-of-service (DDoS) attacks against a company's website.

Availability controls protect timely and uninterrupted access to information and include provisioning backup servers, diversifying power sources, and creating hardware redundancies. Ex: Network interface card (NIC) teaming combines multiple physical network adapters into a single logical adaptor to improve redundancy. Software tools can be used to monitor system performance and network traffic, and firewalls and routers can help mitigate the impact of DDoS attacks.

PARTICIPATION ACTIVITY 1.1.7: Load balancer for preserving data availability.



Animation content:

An image of a cloud labeled internet. A client computer on the left of the cloud. A load balancer on the right of the cloud. The load balancer is connected to two web servers.
Step 1: The availability principle is impacted if a web server fails to respond to a web client's request due to a hardware failure or server overload.
Step 2: A load balancer improves data availability by distributing web traffic across multiple identical web servers.
Step 3: If a web server fails, the load balancer directs the traffic to the other web server to preserve data availability.

Animation captions:

1. The availability principle is impacted if a web server fails to respond to a web client's request due to a hardware failure or server overload.

2. A load balancer improves data availability by distributing web traffic across multiple identical web servers.
3. If a web server fails, the load balancer directs the traffic to the other web server to preserve data availability.

PARTICIPATION ACTIVITY 1.1.8: Availability.

1) Which one of the following measures help increase data availability?
   - Removing surface dust from a web server's motherboard
   - Reducing the number of servers in a web server cluster
   - Decreasing the frequency of web server data backups

2) Which of the following actions improves the availability of a server's files?
   - Disabling the server's anti-malware software
   - Regularly patching the server's operating system
   - Removing the server's redundant network card

3) Redundant array of independent disks (RAID) is a data storage technology that combines multiple physical disk drives into one logical unit. How does RAID help preserve the availability principle?
   - By reducing storage costs
   - By increasing performance
   - By improving data redundancy

1.2 Vulnerabilities

Security vulnerabilities

In an ideal world, a system could be perfectly secure and support a user's needs. In reality, resource, time, and budget constraints exist. Thus, a system always contains some weaknesses. Ex: A company firewall can filter employee web traffic by either allowing access or blocking access to certain websites. Allowing employees to visit only approved websites is the more secure option. However, creating a complete list of preapproved websites is time-consuming and impractical.

A ***vulnerability*** is a weakness or flaw in a system's design, implementation, operation, or management. Ex: A router with a default password is a vulnerability resulting from poor implementation.

A ***threat*** is any event that can potentially impact a system negatively through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. A threat exploits a vulnerability.

A threat can be:

- Accidental - Software or operator error
- Intentional - Virus, ransomware, or phishing
- Natural - Earthquake, hurricane, or flood

A ***threat actor*** is a person or group who exploits a vulnerability. A threat actor uses a threat to damage the system or access confidential data. Ex: A competitor steals design plans for a new product.

PARTICIPATION ACTIVITY 1.2.1: Vulnerabilities.

Animation content:

Static image: A "Vulnerability" label above an icon of a person sitting at a desk working on a red laptop. A "Threat" label above an open envelope with a red bug. A "Threat actor" label above a red icon of a person at a desk working on a laptop.

Animation captions:

1. An attacker sends an employee an email with an attachment containing a virus. The employee opens the email attachment and infects the computer.
2. The vulnerability is the employee without adequate security training.
3. The threat is the virus. The virus exploits the inadequately trained employee.
4. The threat actor is the attacker. The attacker uses the virus to exploit the inadequately trained employee.

PARTICIPATION ACTIVITY 1.2.2: HBGary SQL injection attack.

Identify the vulnerability, threat, and threat actor in the given scenario.

In 2011, the hacker group called Anonymous carried out an SQL injection attack on an IT firm called HBGary. The attack was successful because HBGary's website did not validate input.

Anonymous published the company's internal emails, destroyed data, and defaced the company website.

1) Vulnerability
   - Hacker group Anonymous
   - No input validation
   - SQL injection

2) Threat
   - Hacker group Anonymous
   - Published internal emails
   - SQL injection

3) Threat actor
   - Hacker group Anonymous
   - HBGary
   - SQL injection

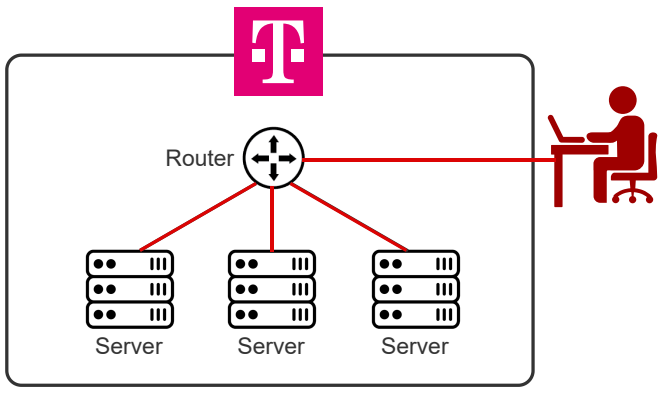
Impact of vulnerability exploitations

When a threat actor exploits a vulnerability, confidential data may be exposed. A ***data breach*** is the exposure of data to an unauthorized user. A data breach may include data loss or data exfiltration. ***Data loss*** is the loss of access to data. ***Data exfiltration*** is the unauthorized transfer of data.

A data breach can result in:

- Identity theft - An attacker may use personal information to apply for loans or use medical insurance benefits.
- Financial loss - An attacker may request a ransom, or the organization may be fined for inadequate security.
- Reputation damage - Consumers may lose trust in the targeted organization.
- Availability loss - Employees or customers may be unable to access data to perform necessary tasks.

PARTICIPATION ACTIVITY 1.2.3: T-Mobile breach impacts.



Data breach	Data exfiltration	Identity theft	Financial loss
Attacker accessed customer information	Attacker copied customer information	Stolen information included customer social security numbers	$350 million settlemen to customers and $150 million toward improving security

Animation content:

Static image: A box labeled with a T-Mobile logo. Inside the box is a router with red connections to three servers. The router also has a red connection that goes outside of the box to a red icon of a person at a desk on a laptop. A "Data breach" label over the text "Attacker accessed customer information." A "Data exfiltration" label over the text "Attacker copied customer information." An "Identity theft" label over the text "Stolen information included customer social security numbers." A "Financial loss" label over the text "$350 million settlement to customers and $150 million toward improving security."

Animation captions:

1. In 2021, an attacker hacked into T-Mobile's internal system through an unprotected router.
2. T-Mobile experienced a data breach because the attacker gained access to the servers that store customer information.
3. T-Mobile experienced data exfiltration because the attacker copied customer information. The attacker listed the customer information for sale on the dark web.
4. T-Mobile customers may continue to experience identity theft because customers' information is still circulating on the dark web.
5. T-Mobile experienced financial loss because T-Mobile was sued by affected customers. T-Mobile agreed to pay the affected customers $350 million and invest $150 million in security improvements.

PARTICIPATION ACTIVITY | 1.2.4: Colonial Pipeline attack.

Identify the impacts in the given scenario.

In 2021, a hacker group called DarkSide attacked Colonial Pipeline using ransomware. DarkSide blocked access to Colonial Pipeline's billing operations and demanded a $4.4 million ransom. The pipeline was shut down for one week while Colonial Pipeline paid the ransom and attempted to restore billing operations. The shutdown resulted in gas shortages across the east coast of the United States.

How to use this tool

Financial loss | **Reputation damage** | **Data breach** | **Availability loss**

	DarkSide gained access to Colonial Pipeline's billing operations.
	Colonial Pipeline paid a $4.4 million ransom and may be fined $1 million by US pipeline regulators.
	Colonial Pipeline's CEO testified to the US Senate that DarkSide used a stolen

	password to log on to Colonial Pipeline's network through a legacy VPN not protected with multifactor authentication.
	Colonial Pipeline could not bill customers.

Reset

Exploring further:

- HBGary SQL injection attack
- T-Mobile breach
- Colonial Pipeline ransomware attack

1.3 Threat actors and attack vectors

Threat actors

Threat actors exploit vulnerabilities for various reasons, including harming a person, organization or government, accessing confidential information, or gaining competitive advantage. Threat actors have varying degrees of technical expertise, computing capabilities, and financial resources. Threat actors may be motivated by financial gain, service disruption, blackmail, or revenge. Threat actors may be internal to an organization and have access to the organization's data (insider threats), or external with no access privileges. Threat actors include security hackers, script kiddies, hacktivists, state actors, criminal syndicates and corporate competitors.

Security hacker

A ***security hacker*** is a person who uses various techniques to exploit vulnerabilities in computer systems or networks. Security hackers can be categorized into three groups:

- A ***white hat hacker***, or ***ethical hacker***, is a non-malicious security hacker who is tasked by a system's owner to identify the system's vulnerabilities.
- A ***gray hat hacker*** is a non-malicious security hacker who attempts to find a system's vulnerabilities without the knowledge of the system owner and for the purpose of informing the system's owner about the threats to the system.
- A ***black hat hacker*** is a malicious security hacker who identifies and exploits a system's vulnerabilities without the knowledge or consent of the system's owner.

A ***script kiddie*** is an unskilled person who uses malicious scripts developed by security hackers to exploit a system's vulnerabilities. A script kiddie lacks the programming skills to understand how malicious scripts operate or the consequences of running those scripts. Ex: A script kiddie may execute a script that launches a UDP flood attack without having any knowledge of transport layer protocols.

Table 1.3.1: Security hackers.

Security hacker	Permission	Intention	Motivation	Legality
White hat	authorized	non-malicious	financial (compensated by system owner)	legal
Gray hat	semi-authorized	non-malicious	improve security	illegal (in most jurisdictions)
Black hat	unauthorized	malicious	profit	illegal

PARTICIPATION ACTIVITY 1.3.1: Security hacker.

1) A _____ hat hacker's intention is to improve the security of a system without being tasked to do so by the system's owner.
   - white
   - gray
   - black

2) A security hacker who is compensated for finding a system's vulnerability by the system owner is a _____ hat hacker.
   - white
   - gray
   - black

3) A security hacker who retrieves credit card numbers stored in a database and sells those numbers for a profit is a _____ hat hacker.
   - white
   - gray
   - black

4) A security hacker who voluntarily attempts and finds a vulnerability in a network router and informs the network administrator of the vulnerability is a _____ hat hacker.
   - white
   - gray
   - black

Other threat actors

An ***advanced persistent threat (APT)*** is a threat actor who gains unauthorized access to a high-value target for an extended period of time. An APT is typically sponsored by a nation-state or state actor with the aim of stealing government, military or corporate secrets of another nation. A ***state actor*** is a person or group who is acting on behalf of a government. APT targets may include critical infrastructure such as power and water distribution systems, or election websites and voting systems.

An activist is a person who believes in social or political change and participates in activities such as public protests to support a cause. A ***hacker activist*** or ***hacktivist*** is an activist who uses computer-based techniques to promote the activist's agenda. Hacktivists often operate as part of a coordinated group or organization. Common targets for hacktivists include multinational corporations, government agencies or other entities perceived as morally wrong or unjust by hacktivists. Ex: A hacktivist group may deface a company's website which is conducting business in a country with a history of human rights abuses.

A ***cyber syndicate*** is a criminal syndicate which uses the Internet to engage in criminal conduct. Internet-based criminal activities include fraud, extortion, ransom and identity theft. Criminal syndicates are organized and well-funded and are capable of conducting sophisticated attacks against a wide range of targets from online retailers to major banks and financial institutions. Ex: A criminal syndicate may encrypt an organization's confidential data and demand a ransom for decrypting the data.

A ***competitor*** is a rival organization whose activities have the potential to reduce another organization's share of the market. An organization's competitor may exploit vulnerabilities in the organization's systems to perform espionage, harm reputation, or deny customer access. Ex: A competitor may seek to shut down the target organization's sales event, steal customer information, or corrupt manufacturing databases.

PARTICIPATION ACTIVITY 1.3.2: Threat actors.

Select the most likely threat actor in each scenario.

1) An attack is easily traced back to the attacker.
   - White hat hacker
   - Competitor
   - Script kiddie

2) A denial of service attack against an oil company's website which was responsible for a large oil spill.
   - Competitor
   - Hacktivist
   - Gray hat hacker

3) A phishing campaign aimed at tricking a company's accounting department to wire transfer money to a company masquerading as a legitimate entity.
   - Script kiddie
   - State actor
   - Criminal syndicate

4) A persistent attack aimed at gaining long-term access to a system for the purpose of gathering national secrets.
   - Competitor

- Script kiddie
- APT

5) Using a newly hired employee's authentication credentials at the employee's previous company to gain access to the company's proprietary information.
   - Hacktivist
   - Competitor
   - Criminal syndicate

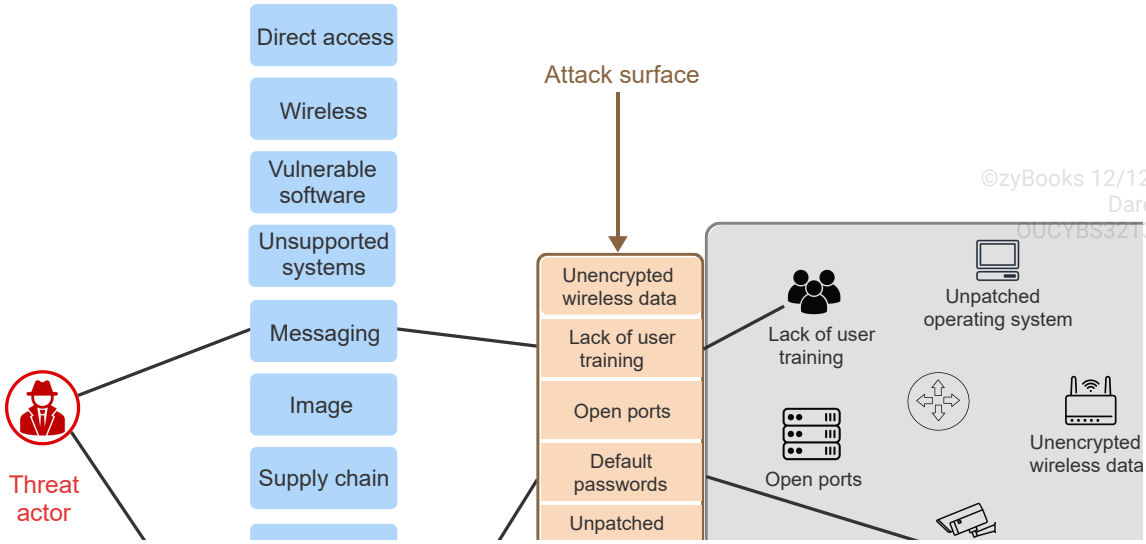
Attack vectors and surface

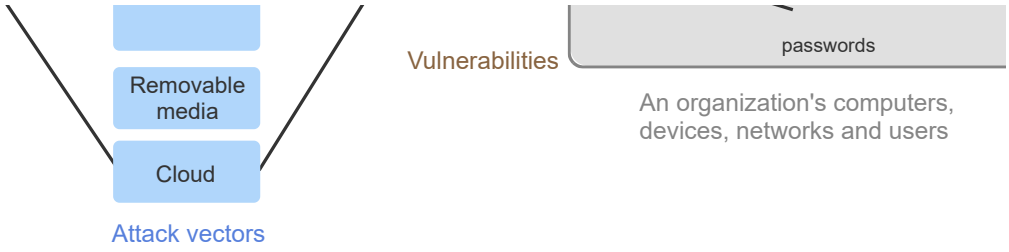
A threat actor can use different methods to exploit a vulnerability. An ***attack vector***, or ***threat vector***, is a path or means by which an attack is realized. Ex: Email is an attack vector because Email can be used to deliver malware to a target user. Common attack vectors include:

- Direct access: Accessing a computer or network directly through a physical connection
- Wireless: Intercepting and modifying wireless data
- Vulnerable software: Accessing a computer or network through a known software vulnerability
- Unsupported systems and applications: Accessing a computer or network through a system or application that no longer receives security updates
- Messaging: Attaching malware or including a malicious link in an email, instant message, or SMS message
- Image: Embedding malicious code within an image file
- Supply chain: Modifying a hardware or software product as the product moves through the supply chain
- Social media: Delivering customized attacks against a target based on the target's social media posts
- Removable media: Delivering malware using removable media such as USB flash drives
- Cloud: Using cloud computing, network, and storage resources to launch an attack against a target

An ***attack surface*** is the sum of the points on a system's boundary where a threat actor can attempt to enter, cause an effect on, or extract data from. A system's attack surface consists of the system's vulnerabilities. Reducing a system's vulnerabilities reduces the system's attack surface and improves the system's security.

PARTICIPATION ACTIVITY 1.3.3: Attack vectors and surface.





Animation content:

Static image: A threat actor on the left, next to seven attack vectors, next to five elements in the attack surface, and computers, devices, networks and users of an organization in a box.
Step 1: An organization's computing devices, networking equipment and users have vulnerabilities which can be exploited by a threat actor.
Step 2: The organization's attack surface is the set of all the organization's vulnerabilities.
Attack vectors are the pathways by which a threat actor can exploit an organization's vulnerabilities.
Step 3: Ex: A threat actor can take advantage of the organization's lack of user training programs to trick users into opening malicious email attachments or clicking embedded links to malicious websites.
Step 4: Ex: A threat actor can use virtual servers in the cloud to connect to devices such as CCTV cameras which are using the manufacturer's default passwords.

Animation captions:

1. An organization's computing devices, networking equipment and users have vulnerabilities which can be exploited by a threat actor.
2. The organization's attack surface is the set of all the organization's vulnerabilities.
3. Attack vectors are the pathways by which a threat actor can exploit an organization's vulnerabilities.
4. Ex: A threat actor can take advantage of the organization's lack of user training programs to trick users into opening malicious email attachments or clicking embedded links to malicious websites.
5. Ex: A threat actor can use virtual servers in the cloud to connect to devices such as CCTV cameras which are using the manufacturer's default passwords.

PARTICIPATION ACTIVITY 1.3.4: Attack vectors.

Identify the threat vector used in each scenario.

How to use this tool

Wireless **Cloud** **Direct access** **Messaging** **Removable media** **Social media** **Supply chain**

	A malware-infected laptop is connected to a network switch with a cable

	An authentication exchange between a laptop and an access point is captured over the air and replayed at a later time
	An email containing malware is sent to a company employee
	A keylogger is loaded onto every USB drive at a manufacturing plant
	A Facebook channel is used to trick targets into signing up for a webinar by clicking a link to a malicious website
	A virus is loaded on an employee's company assigned external hard disk drive
	Spoofed requests are sent to a cloud-based application to exhaust the application's resources

Reset

Shadow IT

*A **shadow IT** is the information technology systems deployed at a company without the knowledge of the company's IT department. Shadow IT systems are created to bypass the limitations of centrally managed IT systems. Ex: A company's marketing department may create and deploy a new web application without following the company's secure coding practices or performing adequate security testing.*

Shadow IT systems are threats that introduce security and compliance concerns because such systems are not monitored or configured according to a company's security policies.

1.4 Threat intelligence and research sources

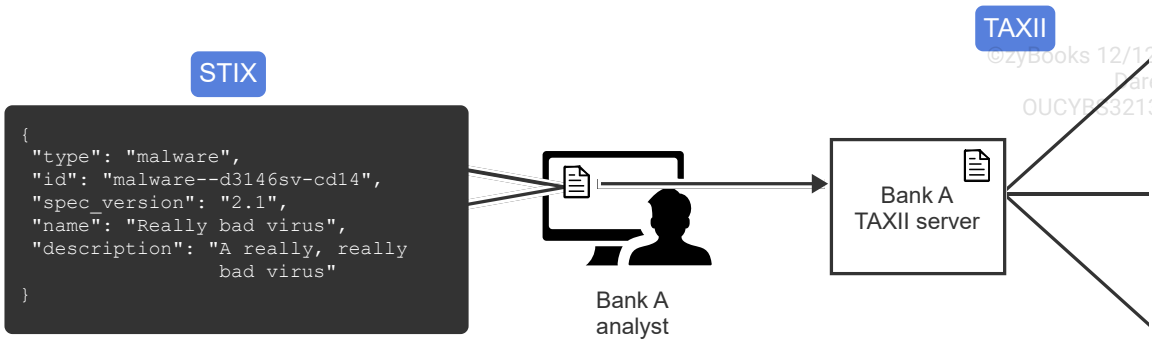
Threat intelligence

Organizations share threat intelligence to reduce the impact of new threats. Threat intelligence can also be used to automate defenses. Ex: Blocking a malicious IP address identified by another organization. ***Automated indicator sharing (AIS)*** is a capability that enables the real-time exchange of threat intelligence. The US Government offers AIS to help defend against newly discovered threats.

To share threat intelligence, organizations must use common standards for describing and exchanging threat intelligence. AIS exchanges threat indicators using STIX and TAXII. ***Structured threat information expression (STIX)*** is a standardized

markup language for expressing threat intelligence. ***Trusted automated exchange of intelligence information (TAXII)*** is an application protocol for sharing threat intelligence.

PARTICIPATION ACTIVITY | 1.4.1: Threat intelligence sharing.



Animation content:

Static image: A code block labeled "STIX".
Begin STIX code:
{
"type": "malware",
"id": "malware--d3146sv-cd14",
"spec_version": "2.1",
"name": "Really bad virus",
"description": "A really, really bad virus"
}
End STIX code.
The code block is connected to a file icon on a desktop computer. A person labeled "Bank A analyst" is at the computer. An arrow points from the file icon to another box labeled "Bank A TAXII server" with a copy of the file icon. Three arrows point from the "Bank A TAXII server" box to three more boxes labeled "Bank B TAXII server," "Bank C TAXII server," and "Bank D TAXII server." Each box also has a copy of the file icon.
Step 1: An analyst for Bank A identifies a new threat. To share the threat with other banks, the analyst first represents the threat using the STIX markup language.
Bank A analyst appears next to a desktop computer with a file icon. A black box labeled "STIX" appears connected to the file icon. The STIX code appears in the black box.
Step 2: The STIX package is sent to Bank A's TAXII server.
A "TAXII" label appears above a box labeled "Bank A TAXII server." An arrow appears while a copy of the file icon flies from the desktop computer to the Bank A TAXII server.
Step 3: Bank A's TAXII server can then share the threat intelligence with other banks. Banks B, C, and D can use the intelligence to protect against the identified virus.
Three boxes appear, labeled "Bank B TAXII server," "Bank C TAXII server," and "Bank D TAXII server." Arrows appear from the Bank A TAXII server to each of the other TAXII servers. Copies of the file icon fly from the Bank A TAXII server to each of the other TAXII servers.

©zyBooks 12/12/24 17:58 2172291 Daren Diaz OUCYBS3213FreezeFall2024

Animation captions:

1. An analyst for Bank A identifies a new threat. To share the threat with other banks, the analyst first represents the threat using the STIX markup language.
2. The STIX package is sent to Bank A's TAXII server.
3. Bank A's TAXII server can then share the threat intelligence with other banks. Banks B, C, and D can use the intelligence to protect against the identified virus.

PARTICIPATION ACTIVITY 1.4.2: Threat intelligence sharing.

1) AIS, STIX, and TAXII _____.
   - block malicious IP addresses
   - identify new threats
   - share threat intelligence

2) A STIX package is a _____.
   - description of a threat
   - threat sharing organization
   - virus

3) Peyton is an IT professional at a small company. Peyton can ensure the company integrates AIS threat intelligence by connecting directly to AIS, subscribing to an AIS-integrated commercial provider, or _____.
   - becoming a member of an information sharing and analysis center (ISAC)
   - watching GitHub repositories
   - searching the dark web

Threat intelligence sources

Threat intelligence is organized and shared by threat intelligence sources. A ***threat intelligence source*** is a public or private information resource on security threats, attacks, and attackers. ***Open-source intelligence (OSINT)*** is intelligence derived from publicly available information on an individual or organization. Ex: Data gathered from an employee's LinkedIn profile.

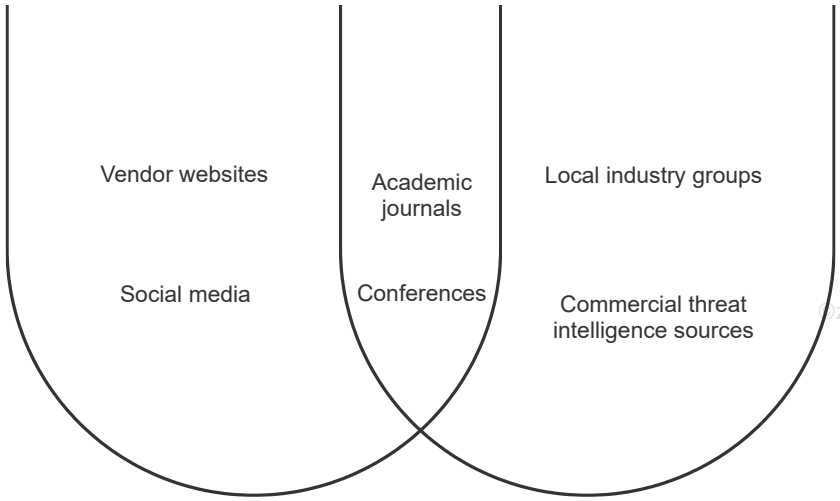
Alternatively, closed-source intelligence is private information only accessible to members of a specified group. Ex: Infragard is a threat intelligence source maintained by the US Federal Bureau of Investigation to protect critical US infrastructure. Infragard intelligence is only available to members of critical infrastructure industries such as energy and healthcare.

An organization can use intelligence gathered from threat intelligence sources to determine the likelihood of future security events, called ***predictive analysis***.

PARTICIPATION ACTIVITY 1.4.3: Threat intelligence sources.

OSINT

Closed source intelligence



Animation content:

Static image: Venn diagram. The left side is labeled "OSINT" and contains "Vendor websites" and "Social media." The right side is labeled "Closed source intelligence" and contains "Local industry groups" and "Commercial threat intelligence sources." The overlapping section includes "Academic journals" and "Conferences."

Animation captions:

1. Vendor websites, request for comments (RFCs), and social media are OSINT because each source is publicly available.
2. Closed source intelligence sources often require a subscription or membership. Ex: CrowdStrike's Falcon Intelligence requires a subscription.
3. Academic journals and conferences may be OSINT or closed source intelligence. Ex: The Computers and Security journal requires a subscription, but the Array journal is open source.

PARTICIPATION ACTIVITY | 1.4.4: Threat intelligence sources.

1) What term is used to describe information gathered from publicly available resources?
   - Closed source intelligence
   - OSINT
   - Vendor websites

2) Which source provides closed source intelligence?
   - Common Vulnerabilities and Exposures (CVE)
   - Microsoft security blog series
   - The Aviation ISAC

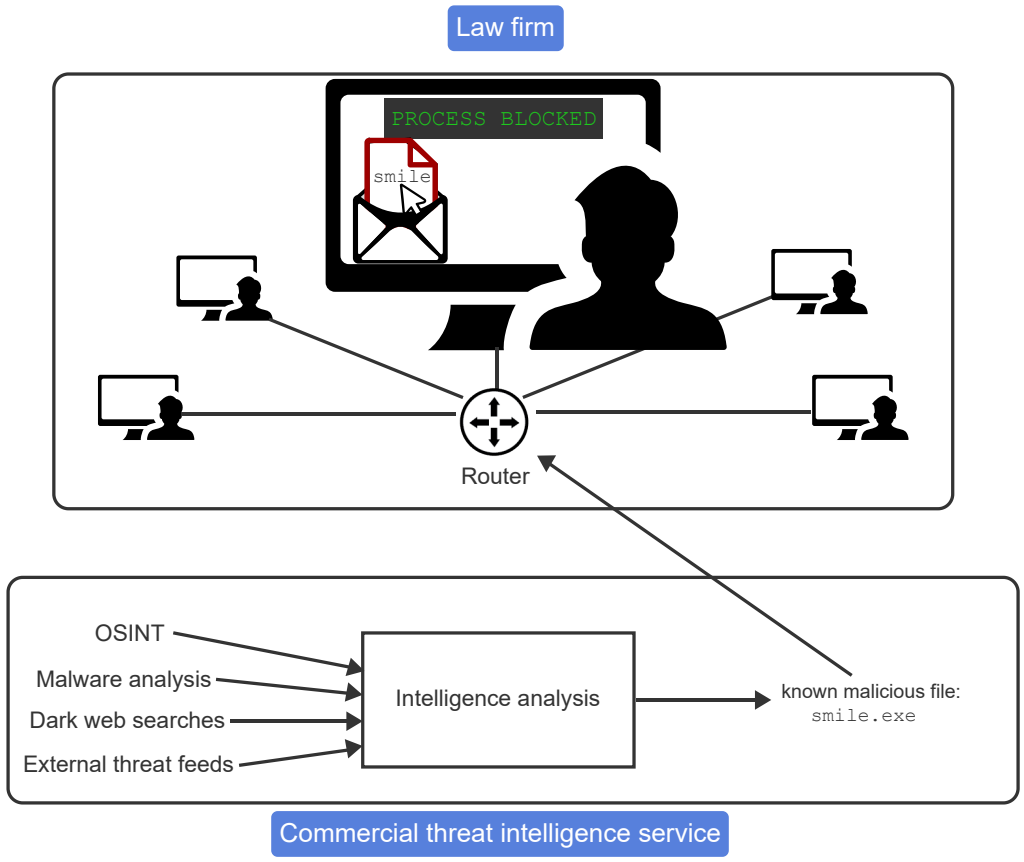
Commercial services and intelligence feeds

An organization may outsource intelligence analysis due to limited resources or other constraints. Commercial threat intelligence services gather and analyze threat intelligence to provide actionable information to a client. Ex: The IntSights commercial service integrates with an organization's Active Directory. If IntSights discovers compromised credentials on the dark web, IntSight automatically locks down the compromised account and notifies the user to reset the affected credentials.

Intelligence is continuously updated, stored in databases, and shared through feeds. Threat feeds include information about known threats and threat actors. An organization uses threat feeds to defend against known adversary tactics, techniques, and procedures. Ex: CrowdStrike's Falcon Intelligence includes threat feeds that can be read and interpreted by security devices.

An organization uses vulnerability feeds to understand current risks. A ***vulnerability database*** is a database for storing, maintaining, and disseminating information, via feeds, about security vulnerabilities in a system or software. Ex: The US Government maintains the National Vulnerability Database (NVD) to provide quality vulnerability information at no cost. The NVD offers several vulnerability feeds, such as the JSON vulnerability feeds.

PARTICIPATION ACTIVITY 1.4.5: Threat intelligence services.



Animation content:

Static image: Two boxes labeled "Law firm" and "Commercial threat intelligence service." The Law firm box contains a router connected to five computer icons. The center computer is enlarged. The enlarged computer screen contains an envelope with a red file labeled "smile." A cursor is on the file. Above the file is a box with the text "PROCESS BLOCKED." The Commercial threat intelligence service box is below the Law firm box. On the left side of the Commercial threat intelligence services box is a list: "OSINT," "Malware analysis," "Dark web searches," and "External threat feeds." Each listed item has an arrow pointing to a single box labeled "Intelligence analysis." The Intelligence analysis box has an

arrow pointing to the text "known malicious file: smile.exe." The text "known malicious file: smile.exe" has an arrow pointing to the router in the Law firm box.
Step 1: A small law firm wants to use threat intelligence to protect the firm's network, but the firm does not have the resources to analyze threat intelligence from several sources.
A box labeled "Law firm" appears and contains a router connected to five computer icons.
Step 2: The law firm hires a commercial threat intelligence service to collect and interpret threat intelligence. Here, the analysis shows a file called smile.exe is a known malicious file.
A box labeled "Commercial threat intelligence service" appears. On the left side of the Commercial threat intelligence services box a list appears: "OSINT," "Malware analysis," "Dark web searches," and "External threat feeds." Arrows appear from each listed item to a box that appears labeled "Intelligence analysis." An arrow appears from the Intelligence analysis box to the appearing text "known malicious file: smile.exe."
Step 3: The analysis results are integrated into the law firm's security. Here, a law firm employee tries to open a file called smile.exe. The process is automatically blocked because smile.exe has been identified as malicious.
An arrow appears from the text "known malicious file: smile.exe" to the router in the Law firm box. The middle computer icon is enlarged. A closed envelope appears and flies onto the enlarged computer. The envelope opens and reveals a red file labeled "smile." A cursor appears and moves onto the red file. A "PROCESS BLOCKED" text box appears above the red file.

Animation captions:

1. A small law firm wants to use threat intelligence to protect the firm's network, but the firm does not have the resources to analyze threat intelligence from several sources.
2. The law firm hires a commercial threat intelligence service to collect and interpret threat intelligence. Here, the analysis shows a file called smile.exe is a known malicious file.
3. The analysis results are integrated into the law firm's security. Here, a law firm employee tries to open a file called smile.exe. The process is automatically blocked because smile.exe has been identified as malicious.

PARTICIPATION ACTIVITY 1.4.6: Automated intelligence.

1) An organization should collect data from both threat and vulnerability feeds because _____.
   - more data is always better
   - threat feeds and vulnerability feeds are focused on different aspects of security

2) The main advantage to using a commercial threat intelligence service is _____.
   - more data
   - quality analysis and specific recommendations

Threat maps

A threat map shows active attacks across the world. Debate surrounds the usefulness of threat maps for understanding cyberattacks. However, most threat maps include additional useful information. Ex: The Kaspersky cyberthreat real-time map categorizes threats by data source, such as botnet activity detection and ransomware.

Image source: Best threat maps by Amigos da Verdade is licensed under CC BY-SA 4.0, via Wikimedia Commons

Exploring further:

- National Vulnerability Database (NVD)
- CrowdStrike Falcon Intelligence
- Infragard
- Common Vulnerabilities and Exposures (CVE)
- Microsoft security blog series
- Kaspersky cyberthreat real-time map

1.5 Social engineering

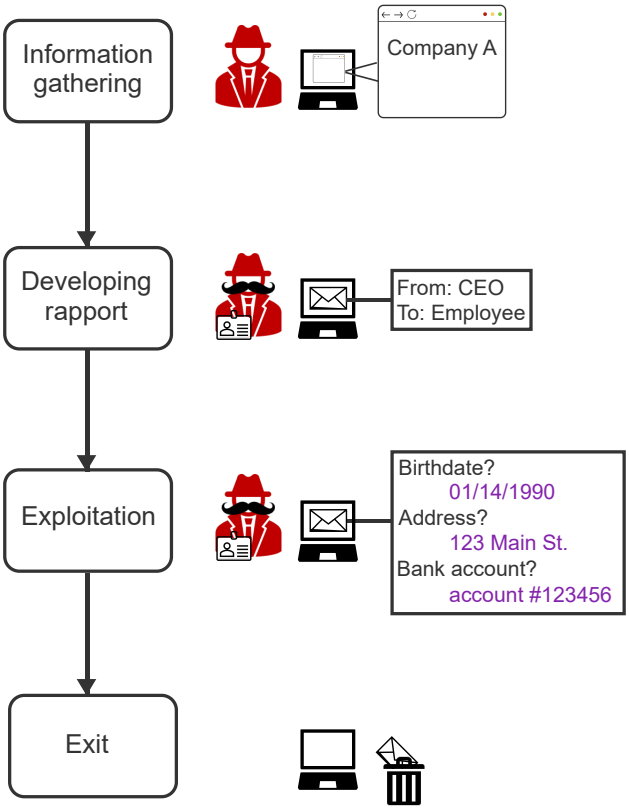
Social engineering

In information security, ***social engineering*** is the manipulation of people into revealing information or performing actions that may compromise a system's security. Ex: An attacker calls a target under the pretext of an IRS investigation. The attacker requests the target's social security number to confirm the target's identity. The attacker can then use this information to apply for a loan.

An attacker may use social engineering to convince a target to:

- Click a malicious link
- Pay for nonexistent goods
- Share personal information

PARTICIPATION ACTIVITY 1.5.1: Social engineering lifecycle.



Animation content:

Static figure: A flow chart of the steps of the social engineering lifecycle.
Step 1: First, an attacker gathers information, like a company CEO's name and email address.
The label "Information gathering" is highlighted. An attacker appears next to a computer. A browser displaying "Company A" appears on the computer.
Step 2: The attacker crafts an email that appears to be sent from the CEO.
The label "Developing rapport" is highlighted. An attacker appears next to a computer. A mustache and ID badge appear on the attacker. An email icon appears on the computer screen and is labeled "From: CEO, To: Employee."
Step 3: The attacker requests personal information. The employee believes the email is from the CEO and responds with the requested information.
The label "Exploitation" is highlighted. The disguised attacker appears next to the computer with the email. The email is labeled "Birthdate? Address? Bank account?" The email moves off the screen and then returns. The email is then labeled "Birthdate? 01/14/1990. Address? 123 Main St. Bank account? Account #123456."
Step 4: The attacker ends communication, collects the information, and removes all traces of the attack.
The label "Exit" is highlighted. The disguised attacker appears next to the computer with the email and a trash can. The email is moved to the trash can. The attacker disappears.

Animation captions:

1. First, an attacker gathers information, like a company CEO's name and email address.
2. The attacker crafts an email that appears to be sent from the CEO.
3. The attacker requests personal information. The employee believes the email is from the CEO and responds with the requested information.

4. The attacker ends communication, collects the information, and removes all traces of the attack.

PARTICIPATION ACTIVITY 1.5.2: Social engineering.

1) An attacker may use social engineering to _____.
   - gain a target's login credentials
   - crash a target's computer
   - recruit a target

2) An email appears to be from a user's bank and includes a link to view account information. To confirm the email's validity, the user should _____.
   - click the link to see where it goes
   - reply to the email asking for verification
   - open a new tab and log in to the bank's legitimate website

3) A repair person arrives at an office building. The receptionist is unaware of the service call. The receptionist should _____.
   - let the repair person in the office
   - confirm the service call was placed
   - write down the repair person's name

Social engineering attack classification

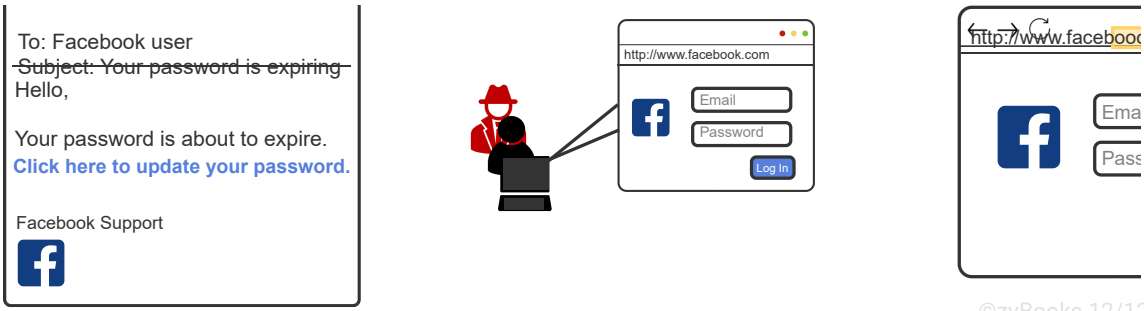
An attacker manipulates a target by creating a situation that the target will not question. A social engineering attack is classified by the strategy used during the attack.

- Social-based - The attack exploits a target's emotion to alter a target's actions.
- Physical-based - The attack relies on physical proximity to a target.
- Technical-based - The attack uses technology to interfere with a target's usual actions.

PARTICIPATION ACTIVITY 1.5.3: Social engineering attack classification.

Stealing a target's Facebook password

Social-based | Physical-based | Technical-



Animation content:

Static figure: Three images of social engineering attacks under the label "Stealing a target's Facebook password."
Step 1: An attacker can steal a target's Facebook password using a social-based, a physical-based, or a technical-based attack. The labels "Social-based," "Physical-based," and "Technical-based" appear.
Step 2: In a social-based attack, a target receives an email stating that the target's Facebook password is expiring. The email includes a malicious link to steal the password.
An email appears under "Social-based." The email is from "Facebook" to "Facebook user." The subject is "Your password is expiring." The body of the email says, "Hello, Your password is about to expire. Click here to update your password. Facebook support."
Step 3: In a physical-based attack, the attacker watches the target enter the target's Facebook password.
A person working on a laptop appears under "Physical-based." A callout for the laptop shows the Facebook login screen. A red attacker appears behind the person.
Step 4: In a technical-based attack, the attacker sets up an illegitimate website at http://www.faceboook.com to steal the password of users who accidentally add an extra "o" in Facebook.
A browser with a Facebook login page appears under "Technical-based." The URL is "http://www.faceboook.com." A highlight appears over the three O's in the URL.

Animation captions:

1. An attacker can steal a target's Facebook password using a social-based, a physical-based, or a technical-based attack.
2. In a social-based attack, a target receives an email stating that the target's Facebook password is expiring. The email includes a malicious link to steal the password.
3. In a physical-based attack, the attacker watches the target enter the target's Facebook password.
4. In a technical-based attack, the attacker sets up an illegitimate website at http://www.faceboook.com to steal the password of users who accidentally add an extra "o" in Facebook.

PARTICIPATION ACTIVITY | 1.5.4: Social engineering attack classification.

Select the type of attack described in each scenario.

1) When a target enters the URL for Amazon, the target is redirected to an

illegitimate site that looks like Amazon's homepage.

- Social-based
- Physical-based
- Technical-based

2) A target receives a friend request from a profile with the name and picture of a target's acquaintance.

- Social-based
- Physical-based
- Technical-based

3) A target enters credit card information in a public area with an attacker nearby.

- Social-based
- Physical-based
- Technical-based

Influence principles

A social engineering attack is successful when a target takes an action against the target's best interests. An ***influence principle*** is a concept that takes advantage of human nature to manipulate a target. An attacker uses influence principles to manipulate the target and avoid suspicion. Ex: A target is approached by an attacker wearing a white lab coat and a stethoscope. The target assumes the attacker is a doctor and shares personal medical information.

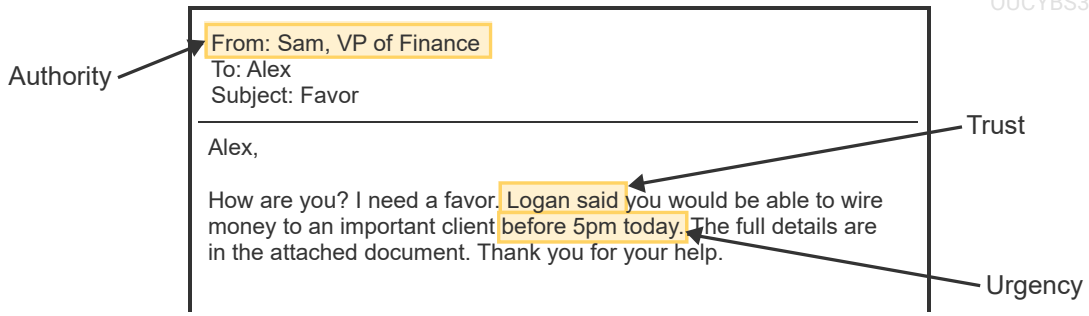
Personal influence principles include:

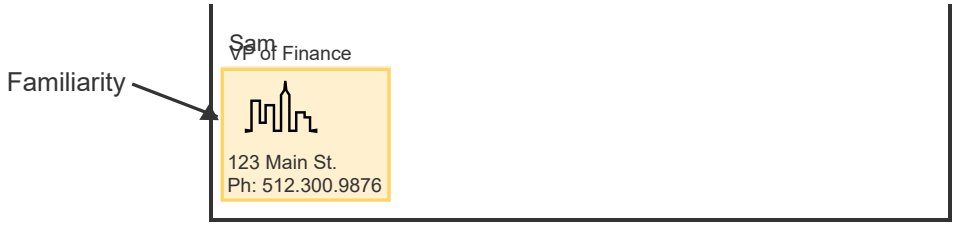
- Authority - A target believes the attacker is in a position of power over the target.
- Familiarity - A target believes the attacker is a known individual or associated with a known organization.
- Intimidation - A target believes the attacker can inflict harm.
- Trust - A target believes the attacker is trustworthy because the attacker has built a connection with the target.

Situational influence principles include:

- Consensus - A target believes the attacker's suggested action has been done by others.
- Scarcity - A target believes the attacker's suggested action has limited availability.
- Urgency - A target believes the attacker's suggested action has a time constraint.

PARTICIPATION ACTIVITY 1.5.5: Influence principles.





Animation content:

Static figure: An email from an attacker to a target. The email is from "Sam, VP of Finance" to "Alex." The subject is "Favor." The body of the email says, "Alex, How are you? I need a favor. Logan said you would be able to wire money to an important client before 5pm today. The full details are in the attached document. Thank you for your help. Sam, VP of Finance." A company logo is included at the bottom of the email.
Step 1: An attacker hopes an employee will wire money to the attacker's account. The attacker uses personal influence principles so the employee feels comfortable completing the transaction.
The full email appears.
Step 2: The attacker establishes authority by writing the email as the company's Vice President of Finance.
"From: Sam, VP of Finance" is highlighted and labeled with "Authority."
Step 3: The attacker establishes trust and creates a connection by referring to the employee's supervisor by name. "Logan said" is highlighted and labeled with "Trust."
Step 4: The attacker establishes a sense of urgency by giving the target a deadline.
"Before 5pm today" is highlighted and labeled with "Urgency."
Step 5: The attacker establishes familiarity by including the standard company signature and logo.
The company logo is highlighted and labeled with "Familiarity."

Animation captions:

1. An attacker hopes an employee will wire money to the attacker's account. The attacker uses personal influence principles so the employee feels comfortable completing the transaction.
2. The attacker establishes authority by writing the email as the company's Vice President of Finance.
3. The attacker establishes trust and creates a connection by referring to the employee's supervisor by name.
4. The attacker establishes a sense of urgency by giving the target a deadline.
5. The attacker establishes familiarity by including the standard company signature and logo.

PARTICIPATION ACTIVITY | 1.5.6: Influence principles.

Identify the influence principle used in each scenario.

How to use this tool

Urgency **Intimidation** **Familiarity** **Scarcity** **Authority** **Trust** **Consensus**

An attacker advertises a free product if the target clicks a link within 20

	seconds. A 20-second timer counts down next to the link.
	An attacker will permanently erase a target's personal data if the target does not send money.
	An attacker includes fake product reviews when advertising an illegitimate product.
	An attacker disguised as a police officer says a target's laptop is needed for an investigation.
	An attacker claims to have attended the same college as a target.
	An attacker sends a target an email that looks like the target's regular water bill and arrives a day before the legitimate water bill.
	An attacker claims to sell the last two tickets to a sold-out concert.

Reset

CHALLENGE ACTIVITY | 1.5.1: Social engineering.

581480.4344582.qx3zqy7

Start

Select the activity performed in each step of the social engineering lifecycle.

Pick

Pick

Pick

1.6 Social engineering: Physical and technical-based attacks

Physical-based attacks

An attacker can use physical proximity to gain information or unauthorized access to a secure area. Physical-based attacks do not require technical expertise. Ex: An attacker learns a target's cell phone password by watching the target enter the password.

Physical-based social engineering attacks include:

- ***Dumpster diving*** is the act of searching garbage for valuable information.
- ***Shoulder surfing*** is the act of physically watching a target input sensitive information.
- ***Tailgating*** is the act of following an authorized person through a security checkpoint to gain access.

PARTICIPATION ACTIVITY | 1.6.1: Physical-based attacks.

Animation content:

Static figure: Three types of physical-based social engineering attacks: dumpster diving, shoulder surfing, and tailgating.
Step 1: An attacker discovers confidential information on documents that were not shredded before disposal. The label "Dumpster diving" appears above a person working near a trash can full of paper. An attacker takes paper from the trash can and walks away.
Step 2: An attacker learns a target's sensitive information by watching the target. The label "Shoulder

surfing" is above a person working on a laptop. An attacker leans over the person from behind to see the laptop.
Step 3: An attacker gains entry to a secure area by following an authorized person. The label "Tailgating" is above a closed door with an ID scanner and an employee with an ID badge. An attacker follows the employee through the door.

Animation captions:

1. An attacker discovers confidential information on documents that were not shredded before disposal.
2. An attacker learns a target's sensitive information by watching the target.
3. An attacker gains entry to a secure area by following an authorized person.

PARTICIPATION ACTIVITY 1.6.2: Physical-based attacks.

Which social engineering attack is mitigated by the security measure described in each statement?

1) Ryan shreds documents with sensitive information before disposal.
   - ○ Dumpster diving
   - ○ Shoulder surfing
   - ○ Tailgating

2) A research company assigns a guard at the entrance of a secure area.
   - ○ Dumpster diving
   - ○ Shoulder surfing
   - ○ Tailgating

3) When working in a public place, Jordan chooses a seat against a wall.
   - ○ Dumpster diving
   - ○ Shoulder surfing
   - ○ Tailgating

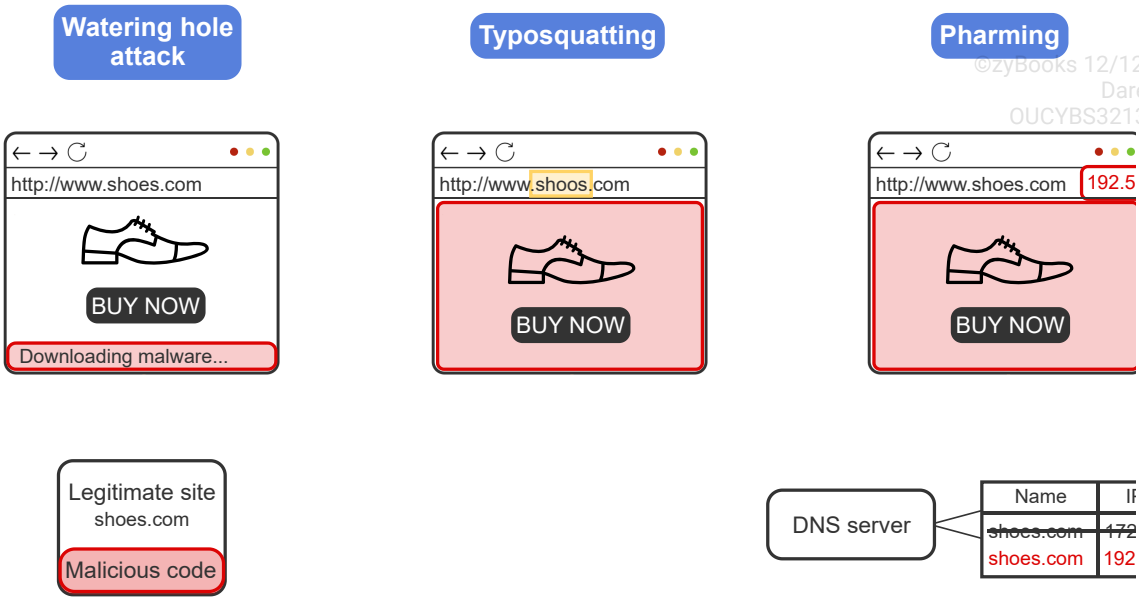
Technical-based attacks

An attacker can use technical means to attack a target through the web. Technical-based attacks do not require a target to click a fraudulent link or respond to an email.

Technical-based social engineering attacks include:

- A ***watering hole attack*** is an attack that compromises a website frequently visited by a target to infect the target's device with malware. Ex: An attacker injects malware into an ecommerce site. When visiting the site, a user's device becomes infected, so the attacker can spy on the user.
- ***Typosquatting*** is an attack using a fraudulent site with a web address based on common misspellings. Ex: An attacker creates a fraudulent site at www.foogle.com to attack users who mistype the first letter in Google.
- ***Pharming*** is an attack using altered DNS entries to redirect a target to a fraudulent site. Ex: An attacker redirects a target to a fraudulent version of Gmail to gain the target's email credentials.

PARTICIPATION ACTIVITY | 1.6.3: Technical-based attacks.



Animation content:

Static image: Three browsers showing technical-based social engineering attacks.
Step 1: An attacker compromises a legitimate site so that a user's computer is infected with malware when the user visits the site.
The label "Watering hole attack" appears above a web browser. Below the browser is a box labeled "Legitimate site shoes.com." Inside the box is a smaller red box labeled "Malicious code." The web address "http://www.shoes.com" appears in the browser address bar. A shoe icon and a button labeled "Buy now" appear in the browser window. A red box moves from the red "Malicious code" box to the bottom of the browser. The text "Downloading malware..." appears in the red box at the bottom of the browser.
Step 2: An attacker creates a fraudulent site at shoe.com to attack users who forget the second 's' in shoes.com.
The label "Typosquatting" appears above a web browser. The web address "http://www.shoos.com" appears in the browser address bar. A yellow highlight box appears over the text "shoos." A shoe icon, a button labeled "Buy now," and a red highlight box appear in the browser window.
Step 3: In a pharming attack, an attacker changes the DNS entry for shoes.com to a fraudulent site's IP address.
The label "Pharming" appears above a box labeled "DNS server." The DNS server box is connected to a table with columns "Name" and "IP address." The first row of the table has the name "shoes.com" and the IP address "172.32.156.1." A strikethrough line appears over the table's first line. A second line appears in red text with the name "shoes.com" and the IP address "192.56.14.255."
Step 4: When a user enters shoes.com in the address bar, the fraudulent IP address is returned and the user is directed to the attacker's fraudulent site.
The DNS server and table move down and a browser appears. The web address "http://www.shoes.com" appears in the browser address bar. A copy of the red IP address from the table's second line, 192.56.14.255, moves from the table to the browser address bar. A shoe icon, a button labeled "Buy now," and a red highlight box appear in the browser window.

Animation captions:

1. An attacker compromises a legitimate site so that a user's computer is infected with malware when the user visits the site.
2. An attacker creates a fraudulent site at shoe.com to attack users who forget the second 's' in shoes.com.
3. In a pharming attack, an attacker changes the DNS entry for shoes.com to a fraudulent site's IP address.
4. When a user enters shoes.com in the address bar, the fraudulent IP address is returned and the user is directed to the attacker's fraudulent site.

PARTICIPATION ACTIVITY 1.6.4: Technical-based attacks.

1) In a _____ attack, a target is directed to a legitimate site.
   - watering hole
   - typosquatting
   - pharming

2) Alex enters a bank's correct web address, but Alex notices the website looks slightly different. Alex may be part of a _____ attack.
   - watering hole
   - typosquatting
   - pharming

3) Using a bookmark to navigate to a website mitigates a _____ attack.
   - watering hole
   - typosquatting
   - pharming

4) If an attacker alters the DNS entry for expedia.com on the Cloudflare DNS server, _____ users who enter expedia.com will be redirected to the attacker's fraudulent site.
   - all
   - some

5) In a successful watering hole attack, the compromised site will infect _____ users' devices when visiting the site.
   - all
   - some

1.7 Social engineering: Social-based attacks

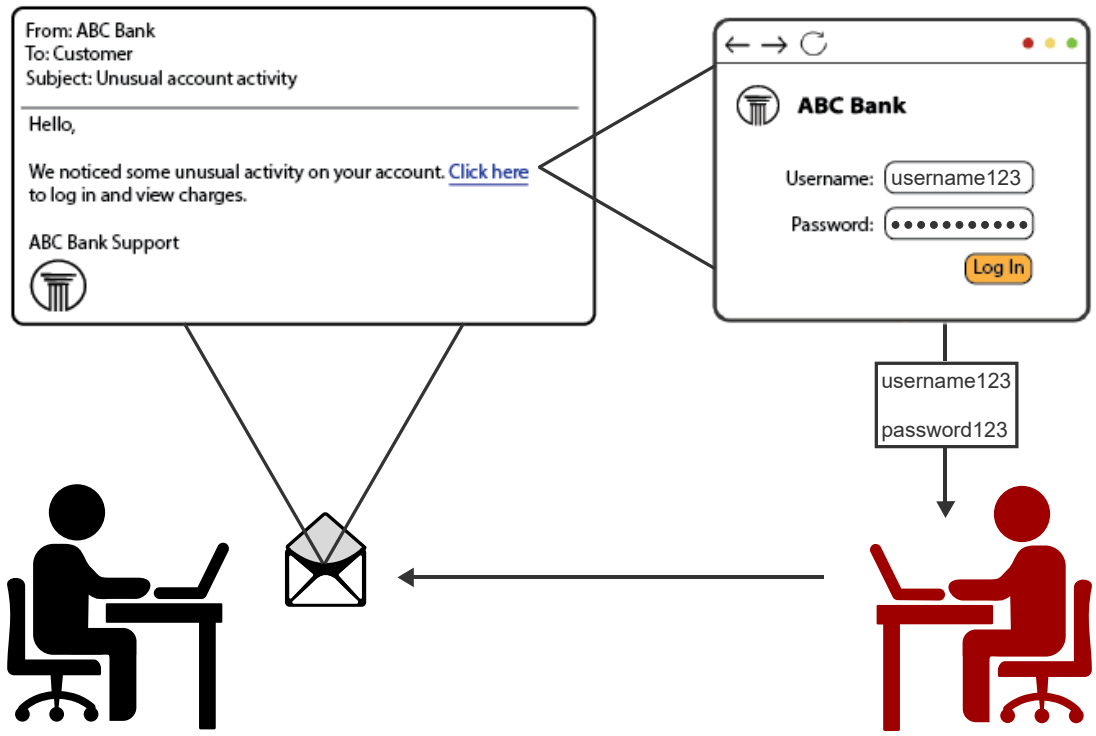
Phishing

Phishing is a social-based attack in which an attacker "fishes" for confidential information by sending a fraudulent message to a target. An attacker uses phishing to gain a target's login credentials, social security number, banking information, or other confidential information. Email is used for most phishing attacks, but other methods exist.

- ***Vishing*** is phishing via phone.
- ***Smishing*** is phishing via text (SMS) message.

Ex: A target receives a text message that appears to be from the IRS. The text message states that the target can click on the included link to view the status of the target's tax return. The fraudulent link collects the target's personal information.

PARTICIPATION ACTIVITY 1.7.1: Phishing.



Animation captions:

1. An attacker sends a phishing email to a target. The target believes the email is from the target's bank.
2. When the target clicks the link, a browser opens with a login screen.
3. When the target enters login credentials, the credentials are sent to the attacker.

PARTICIPATION ACTIVITY 1.7.2: Phishing.

1) Which scenario describes a phishing attack?

   An attacker learns a target's credit card information by _____.

   - stealing the target's credit card.
   - watching the target enter the information online in a public area
   - sending the target an email about a recent purchase and asking for credit card information

2) Morgan receives a suspicious text with a link to track an Amazon order. An attacker is attempting to gain Morgan's Amazon credentials. Morgan is the target of a _____ attack.

   - smishing
   - spam
   - vishing

3) Avery receives a call from an unknown number. The caller claims to be calling from Avery's credit card company and requests the security code that was sent to Avery via text message. Avery is the target of a _____ attack.

   - smishing
   - SPIM
   - vishing

4) A phishing attack is successful when the target _____.

   - forwards the phishing message to friends
   - receives the phishing message
   - reveals confidential information

5) The best defense against a phishing attack is _____.

   - antivirus software
   - education
   - spam filters

©zyBooks 12/12/24 17:58 2172291
Daren Diaz
OUCYBS3213FreezeFall2024

Spear phishing and whaling

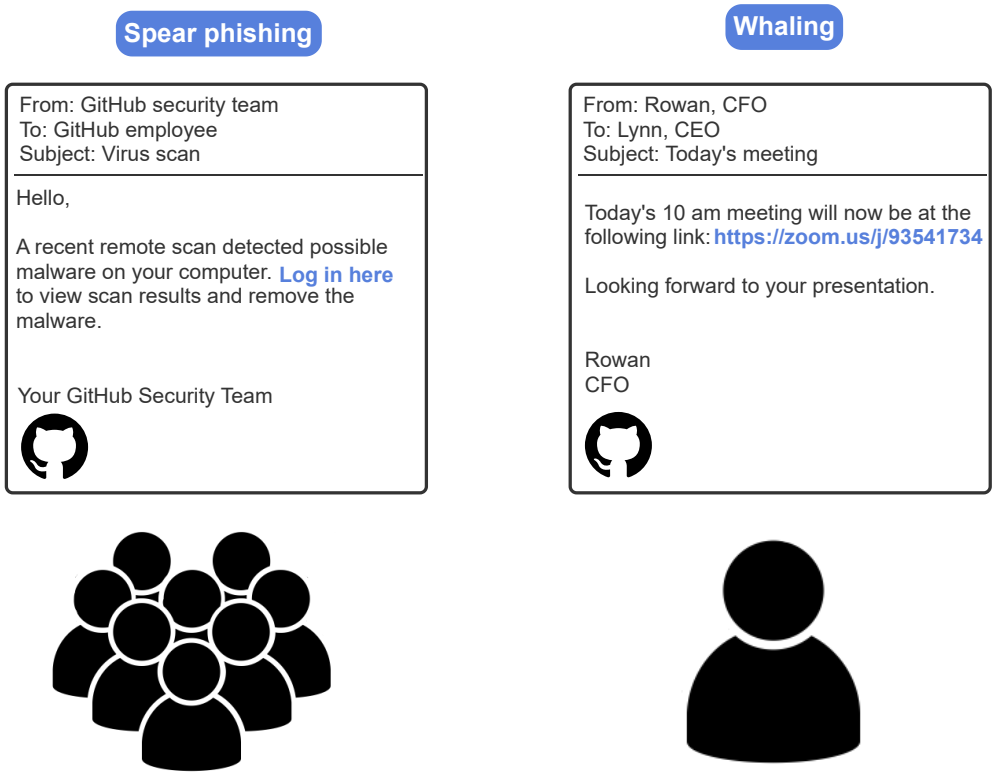
In a general phishing attack, an attacker sends a phishing message to random targets. Alternatively, an attacker may use background information to direct an attack at a specific group or person via email, phone, or text.

Spear phishing is a phishing attack aimed at a specific group or individual. Ex: An attacker sends a text message to Netflix customers that says a new device has logged into the customer's account. The text message includes a fraudulent link that installs malware on customers' devices.

Whaling is a phishing attack aimed at a high-value individual like a CEO. Ex: An attacker poses as Microsoft Support and emails a company's president a password update request. The email includes a link to a fraudulent password update page that steals the company president's Microsoft credentials.

Spear phishing and whaling can be used for financial gain. ***Business email compromise (BEC)*** is an attack where an attacker impersonates a trusted individual to trick a company's employees into making fraudulent financial transactions. Ex: An attacker poses as a supplier and emails a company accountant an invoice with a request to wire funds.

PARTICIPATION ACTIVITY | 1.7.3: Spear phishing and whaling.



Animation content:

Two emails.
Step 1: In this spear phishing attack, an attacker uses a list of GitHub employee email addresses to send employees a fraudulent virus scan link.
The label "Spear phishing" appears above an email and a group of eight people. The email is from "GitHub security team" to "GitHub employee." The subject is "Virus scan." The body of the email says, "Hello, A recent remote scan detected possible malware on your computer. Log in here to view scan results and remove the malware. Your GitHub security team."
Step 2: In this whaling attack, an attacker sends an email to a CEO with a fraudulent Zoom link. The attacker has researched the CEO's meeting schedule to make the email seem credible.
The label "Whaling" appears above an email and one person. The email is from "Rowan, CFO" to "Lynn,

CEO." The subject is "Today's meeting." The body of the email says, "Today's 10 am meeting will now be at the following link: https://zoom.us/j/93541734. Looking forward to your presentation. Rowan, CFO."

Animation captions:

1. In this spear phishing attack, an attacker uses a list of GitHub employee email addresses to send employees a fraudulent virus scan link.
2. In this whaling attack, an attacker sends an email to a CEO with a fraudulent Zoom link. The attacker has researched the CEO's meeting schedule to make the email seem credible.

PARTICIPATION ACTIVITY 1.7.4: Spear phishing and whaling.

Select the term to describe each phishing attack.

1) An attacker posing as Venmo sends an email to randomly-generated email addresses that reports suspicious account activity. The email includes a link to a fraudulent Venmo login page.
   - ○ General phishing
   - ○ Spear phishing
   - ○ Whaling

2) An attacker poses as a company's human resources manager. The attacker sends an email to the company's chief operating officer requesting employee payroll records.
   - ○ General phishing
   - ○ Spear phishing
   - ○ Whaling

3) An attacker obtains a real estate agent's client list. The attacker emails the clients wire transfer instructions to wire mortgage closing costs.
   - ○ General phishing
   - ○ Spear phishing
   - ○ Whaling

Disinformation

In social-based attacks, misinformation and disinformation are used to influence targets. ***Misinformation*** *is false or misleading information that is spread without a deliberate intention to harm.* ***Disinformation*** *is false information that is intentionally created and spread to mislead targets.*

Disinformation is used in phishing attacks and malvertising, an attack that convinces a target to click on a malicious advertisement, leading to the infection of the target device with malware or redirection to malicious websites.

1.8 Malware

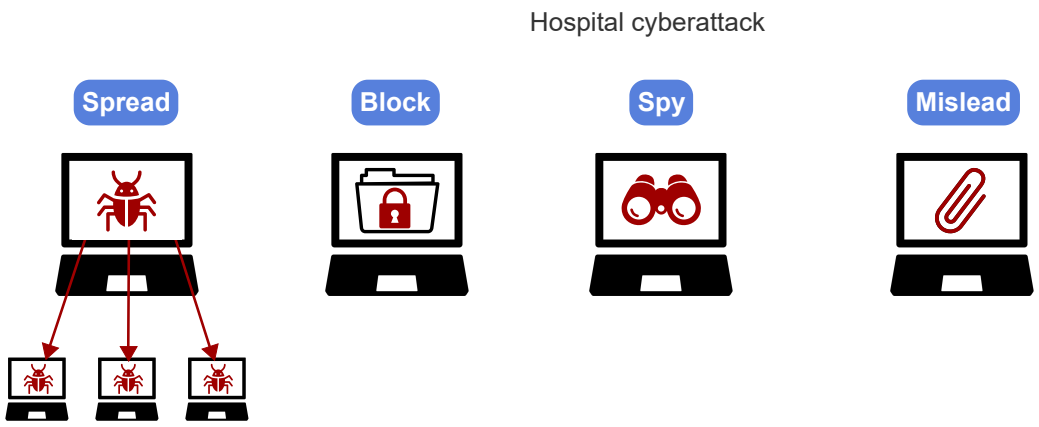
Malware

An attacker may infect a target's device with malware. ***Malware*** (**mal**icious soft**ware**) is any software developed to compromise the confidentiality, integrity, or availability of data. Malware can be used to steal data, modify files, or deny user access. Malware is often spread through phishing emails.

Malware can be classified by the malware's attack method.

- Spread - Malware that infects a device and spreads to other devices.
- Block - Malware that prevents a user from accessing data on the infected device.
- Spy - Malware that collects information from the infected device.
- Mislead - Malware that seems like legitimate software such as a game.
- Hide - Malware that evades detection or conceals other malware.

PARTICIPATION ACTIVITY | 1.8.1: Hospital malware attack.



Animation content:

Static figure: Five computers with icons representing different types of malware.
Step 1: An attacker uses spreading malware to expand an attack. The attacker first infects a vulnerable medical device, and then the spreading malware replicates and spreads to computers and servers.
The label "Spread" appears above a computer with a red bug and three smaller computers. The bug spreads to the three smaller computers.
Step 2: An attacker uses blocking malware to block access to patient files, halting hospital operations. The attacker demands a ransom to release the files.
The label "Block" appears above a computer with a file icon. A red lock appears on the file.

Step 3: An attacker uses spying malware to monitor an infected device so that the attacker can gain patients' personal information.
The label "Spy" appears above a blank computer. Red binoculars appear on the computer.
Step 4: An attacker uses misleading malware to present the malware as an email attachment containing a patient's medical records. When the target downloads the attachment, the device is infected with malware.
The label "Mislead" appears above a computer with a black attachment icon. The icon attachment changes to red.
Step 5: An attacker uses hiding malware to prevent an infected device from recognizing that the device has been infected by spying malware. The attacker can then continue to gain confidential information without detection.
The label "Hide" appears above a computer with a red bug. A red-outlined ghost appears and covers the red bug.

Animation captions:

1. An attacker uses spreading malware to expand an attack. The attacker first infects a vulnerable computer, and then the spreading malware replicates and spreads to other computers and servers.
2. An attacker uses blocking malware to block access to patient files, halting hospital operations. The attacker demands a ransom to release the files.
3. An attacker uses spying malware to monitor an infected device so that the attacker can gain patients' personal information.
4. An attacker uses misleading malware to present the malware as an email attachment containing a patient's medical records. When the target downloads the attachment, the device is infected with malware.
5. An attacker uses hiding malware to prevent an infected device from recognizing that the device has been infected by spying malware. The attacker can then continue to gain confidential information without detection.

PARTICIPATION ACTIVITY | 1.8.2: Real-life malware.

Select the attack method used by each malware example.

How to use this tool

Block **Spread** **Hide** **Spy** **Mislead**

	Pegasus has been used to remotely monitor the cell phones of journalists and political leaders.
	LockerGoga was used to shut down a Norwegian aluminum plant's manufacturing equipment for a full week, costing the company more than $50 million.
	SQL Slammer infected thousands of computers within 10 minutes.

	Stuxnet was used to target Iran's nuclear industrial control systems. Centrifuges kept failing, but Iranian engineers could not identify what caused the failures.
	Emotet has been disguised as a Word document attached to a phishing email.

Reset

Exploring further:

- Pegasus
- LockerGoga
- SQL Slammer
- Stuxnet
- Emotet

1.9 Malware: Spread, block, and spy

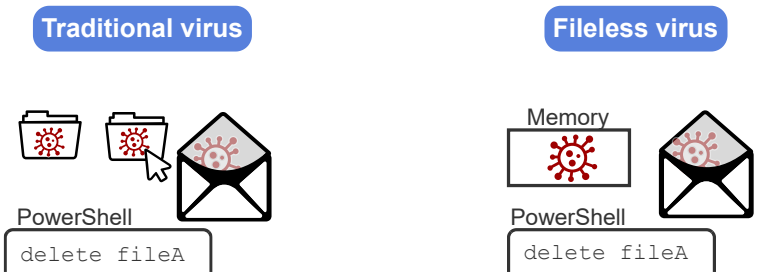
Spread: Virus and worm

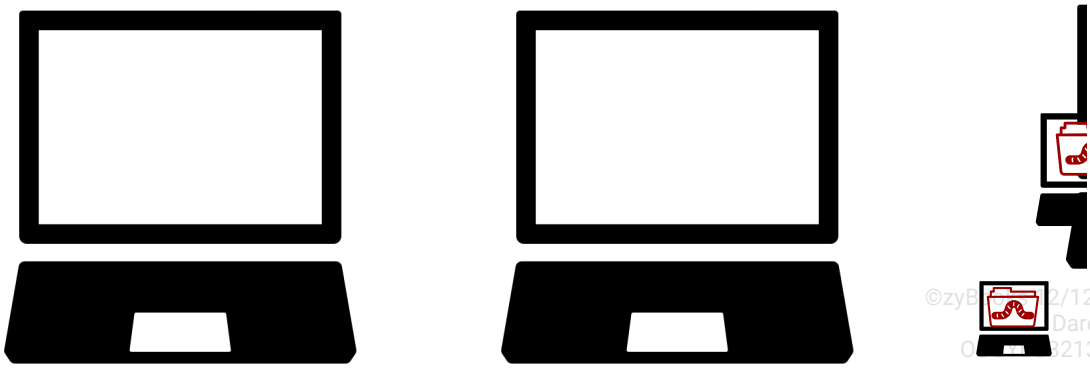
A ***virus*** is a type of malware that self-replicates and spreads within an infected device. An infection mechanism, such as an email, is used to initially infect a device with a virus. The virus then spreads and consumes system resources. An attacker may use a virus to delete, corrupt, alter, or steal data.

Most viruses attach to a file or a program. However, a fileless virus does not require a host. A ***fileless virus*** is a virus that exists in memory only, making the virus impossible to detect by scanning for infected files. A fileless virus is injected directly into memory and corrupts a program like PowerShell to run malicious commands.

A ***worm*** is a type of malware that self-replicates and spreads to other devices over a network. A worm spreads by exploiting a vulnerability. When a device becomes infected, the worm scans for connected devices with the vulnerability. The worm spreads to the vulnerable devices found. An attacker may use a worm to deliver other malware, steal data, or open a backdoor on the infected device.

PARTICIPATION ACTIVITY 1.9.1: Spreading malware through email.





Animation content:

Static image: Three images showing a traditional virus, a fileless virus, and a worm. Step 1: A traditional virus spreads to vulnerable files or programs on a computer.
The label "Traditional virus" appears above a computer with two file icons and a box labeled "PowerShell." An envelope appears and flies into the computer. The envelope opens and a virus icon comes out of the envelope. The virus moves onto one of the files. A copy of the virus moves from the first file onto the second file.
Step 2: When a user activates an infected file, the virus runs. Here, the virus executes malicious commands in PowerShell.
A cursor appears and moves onto the first file. The text "delete fileA" appears inside the PowerShell box.
Step 3: When a user clicks a malicious link, a fileless virus is injected directly into memory and runs immediately.
The label "Fileless virus" appears above a computer with a box labeled "Memory" and a box labeled "PowerShell." An envelope appears and flies into the computer. The envelope opens and a virus icon comes out of the envelope. The virus moves into the Memory box. The text "delete fileA" appears inside the PowerShell box.
Step 4: A worm is a standalone application that runs without user activation. Once a device is infected, the worm can spread to other vulnerable devices through a network.
The label "Worm" appears above a blank computer. An envelope appears and flies into the computer. The envelope opens and a worm on a file comes out of the envelope. Two blank computers appear below the first computer. Copies of the worm on a file fly to the two computers. Four computers appear below the row of two computers. Copies of the worm on a file fly from the two computers down to each computer in the row of four computers.

Animation captions:

1. A traditional virus spreads to vulnerable files or programs on a computer.
2. When a user activates an infected file, the virus runs. Here, the virus executes malicious commands in PowerShell.
3. When a user clicks a malicious link, a fileless virus is injected directly into memory and runs immediately.
4. A worm is a standalone application that runs without user activation. Once a device is infected, the worm can spread to other vulnerable devices through a network.

PARTICIPATION ACTIVITY | 1.9.2: Virus vs. worm.

Which type of malware is described in each statement?

1) Can spread through a network

- Traditional virus
- Fileless virus
- Worm

2) Attaches to a legitimate file or program

- Traditional virus
- Fileless virus
- Worm

3) May be removed by shutting down the infected device

- Traditional virus
- Fileless virus
- Worm

Real world examples

- *Virus - The Michelangelo virus would infect a device and then lay dormant until March 6th. On March 6th, the virus would overwrite the storage device's first one hundred sectors with zeros so that the device could no longer boot.*
- *Fileless virus - Operation Cobalt Kitty targeted a global corporation using a fileless virus. Employees received a spear phishing email with a link to a fake Flash installer that executed malicious commands through PowerShell.*
- *Worm - The ILOVEYOU worm spread to over ten million computers through a malicious email attachment. When a target opened the attachment, the worm damaged files and spread by copying itself to all of the user's Outlook contacts.*

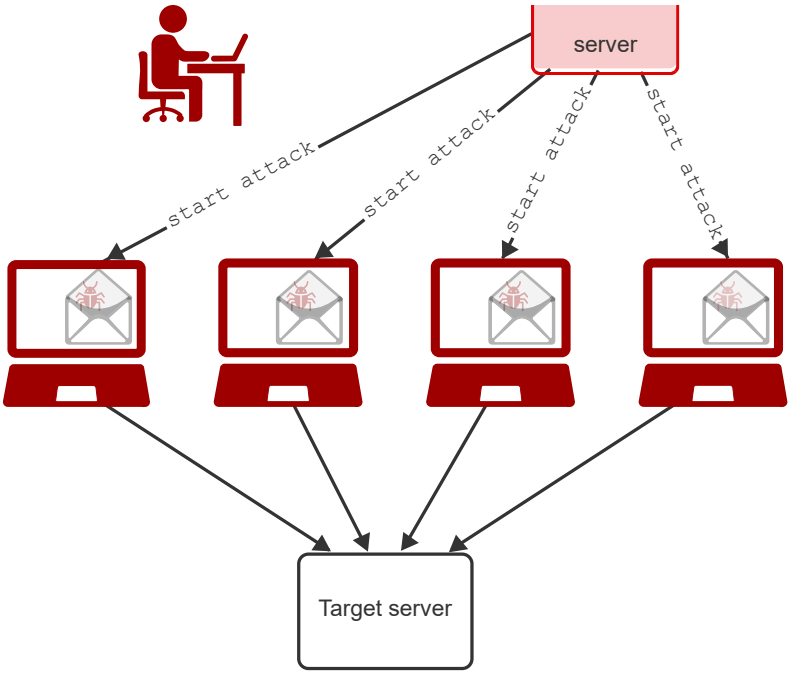
Spread: Bots

A ***bot*** is a device infected with malware that enables an attacker to remotely control the device. A bot communicates with a command and control (C&C) server to receive instructions or send back information. A group of bots, called a botnet, can be used to coordinate large-scale attacks.

Cryptomalware is a type of malware that uses a target computer's computing resources to mine cryptocurrency. Cryptocurrency mining is resource-intensive, so an attacker may deploy cryptomalware to a large botnet. The attacker can then use computing resources across the botnet for a larger payoff.

PARTICIPATION ACTIVITY 1.9.3: Botnet DDoS attack.

Command



Animation content:

Static image: An attacker icon with an arrow labeled "start attack" pointing toward a box labeled "Command and control center." The command and control center has four arrows labeled "start attack" pointing toward four computers. Each computer has an open envelope with a bug inside the envelope. Each computer has an arrow pointing to a single box labeled "Target server."
Step 1: An attacker spreads bot malware through spam email. When a user opens the email, the computer is infected with the malware and becomes a bot. Each bot is connected to a C&C server.
An attacker, a box labeled "Command and control center," and four black computers. An envelope appears near the attacker. A bug appears and moves from the attacker's computer into the envelope. The envelope closes. Four copies of the envelope fly onto each black computer. The first envelope opens and a bug comes out of the envelope. The first computer turns red and a line appears between the first computer and the command and control center. The third envelope opens and a bug comes out of the envelope. The third computer turns red and a line appears between the third computer and the command and control center. The second and fourth envelopes open and bugs come out of each envelope. The second and fourth computers turn red and lines appear between each computer and the command and control center.
Step 2: The attacker wants to attack a target server by flooding the server with traffic. The attacker controls the bots through the C&C server.
A box labeled "Target server" appears below the line of computers. An arrow labeled "start attack" appears pointing from the attacker to the command and control server. Four more arrows labeled "start attack" appear pointing from the command and control server to each of the red computers.
Step 3: The bots send requests to the target server. The flood of traffic overloads the server.
Arrows appear pointing from each computer to the Target server box.

Animation captions:

1. An attacker spreads bot malware through spam email. When a user opens the email, the computer is infected with the malware and becomes a bot. Each bot is connected to a C&C server.

2. The attacker wants to attack a target server by flooding the server with traffic. The attacker controls the bots through the C&C server.
3. The bots send requests to the target server. The flood of traffic overloads the server.

PARTICIPATION ACTIVITY 1.9.4: Botnets.

1) In a botnet, a bot is _____.
   - an attacker's device
   - a target
   - a tool

2) Kala's computer is part of a botnet. From Kala's perspective, the computer's performance is _____.
   - better
   - the same
   - worse

3) Cryptomalware is often used within a botnet because _____.
   - bot malware and cryptomalware are the same thing
   - cryptomalware requires a C&C server
   - mining cryptocurrency is resource-intensive

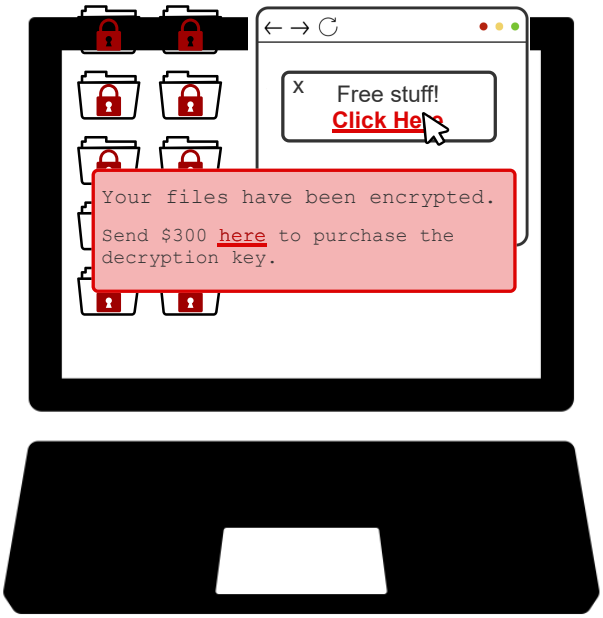
Real world examples

- *Botnet - In 2009, the spam botnet Cutwail contained 1.5 million bots and sent 51 million spam emails every minute.*
- *Cryptomalware botnet - In 2017, the Smominru botnet was used to mine $2.3 million in cryptocurrency.*

Block: Ransomware

Ransomware is a type of malware that denies access to computer files and then demands a ransom to release the files.

PARTICIPATION ACTIVITY 1.9.5: Ransomware attack.



Animation content:

Static image: A computer with ten folders, a browser window, and a red pop-up window. Each folder has a red lock. The browser window has a pop-up that says "Free stuff! Click Here" with a cursor over "Click Here." The red pop-up window says, "Your files have been encrypted. Send $300 here to purchase the decryption key."
Step 1: A user clicks a malicious link. The computer is infected with ransomware and the user's files are encrypted.
A computer appears with ten folders and a browser window. The browser window has a pop-up that says "Free stuff! Click Here." A cursor appears and flies onto "Click Here." Red locks appear on each folder.
Step 2: The computer displays a ransom message from the attacker. The attacker demands $300 in exchange for the decryption key.
A red pop-up window appears that says, "Your files have been encrypted. Send $300 here to purchase the decryption key."

Animation captions:

1. A user clicks a malicious link. The computer is infected with ransomware and the user's files are encrypted.
2. The computer displays a ransom message from the attacker. The attacker demands $300 in exchange for the decryption key.

PARTICIPATION ACTIVITY | 1.9.6: Ransomware.

1) An attacker uses ransomware to gain _____.

- information
- money

2) Jesse's computer has been infected with ransomware. Jesse can gain access to the blocked data by ____.

- decrypting the data with a key
- rebooting the computer

Real world example

The WannaCry ransomware encrypted user data and then displayed a message demanding $300 worth of bitcoin within three days. WannaCry infected 230,000 computers and the attackers received around $400,000 in ransom payments.

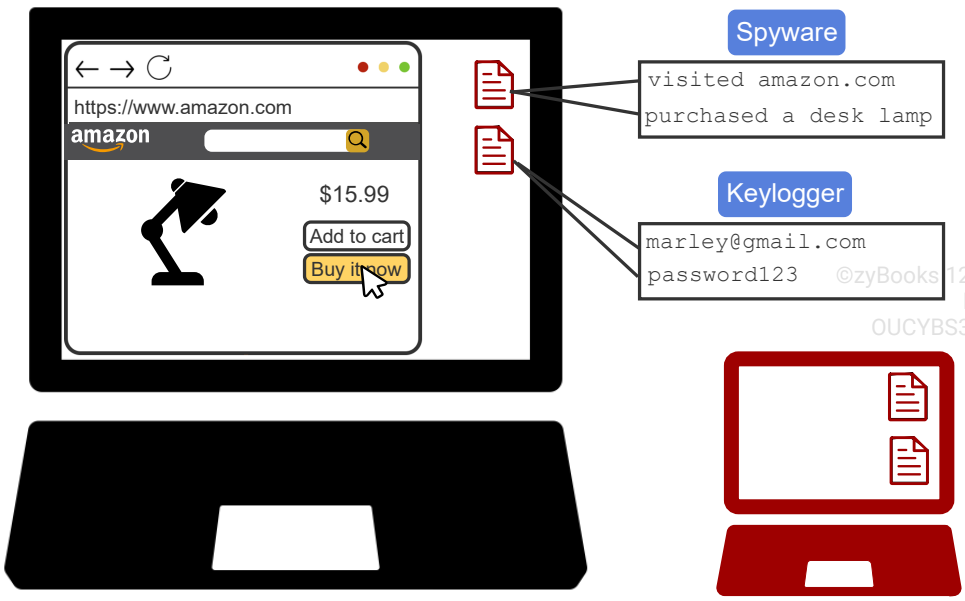
Spy: Spyware and keylogger

Spyware is a type of malware that collects user data without the user's consent. Spyware can be used to collect a user's browsing habits or shopping trends for targeted advertising. Spyware can also be used for nefarious purposes like gaining financial information or remotely accessing a webcam.

Spyware may be included in bloatware. ***Bloatware*** is unwanted software that is preloaded onto a new device by the device's manufacturer. Aside from potentially including spyware, bloatware consumes resources and can introduce vulnerabilities to the device.

A ***keylogger*** is a type of malware that records keystrokes on a keyboard. A keylogger can be used to gain a user's personal information such as passwords or credit card numbers. A keylogger is usually spread through a malicious link or email attachment.

PARTICIPATION ACTIVITY 1.9.7: Recording online purchases.



Animation content:

Static image: A black computer with a browser window and two red file icons. The browser window has a webpage with the URL "https://www.amazon.com." The webpage includes a desk lamp icon and a cursor over a button that says "Buy it now." Each red file icon connects to a box. The first box is labeled "Spyware." The Spyware box has the text "visited amazon.com" and "purchased a desk lamp." The second box is labeled "Keylogger." The Keylogger box has the text "marley@gmail.com" and "password123." A small red computer with two red file icons is next to the black computer.
Step 1: Marley's computer is infected with a keylogger and spyware. The keylogger and spyware record information in hidden files.
A black computer appears. Two red file icons appear on the computer.
Step 2: Marley visits amazon.com on a web browser. The spyware records the visit.
A browser window appears with the URL "https://www.amazon.com." The webpage has "Sign in," two input boxes, and a "Sign in" button. A box labeled "Spyware" appears connected to the first red file icon. The text "visited amazon.com" appears in the Spyware box.
Step 3: The keylogger records Marley's Amazon username and password when Marley logs in.
A box labeled "Keylogger" appears connected to the second red file icon. The text "marley@gmail.com" appears in the first input box and a copy of the text flies into the Keylogger box. Several black dots appear in the second input box and the text "password123" flies into the Keylogger box. A cursor appears and flies onto the Sign in button.
Step 4: Marley buys a desk lamp on amazon.com. The spyware records the purchase.
The webpage fades out. A desk lamp icon, "$15.99," and "Add to cart" and "Buy it now" buttons appear on the webpage. A cursor appears and flies onto the "Buy it now" button. The text "purchased a desk lamp" appears in the Spyware box.
Step 5: Marley's information is sent to the attacker.
A red computer appears next to the black computer. Copies of the red file icons fly onto the red computer.

Animation captions:

1. Marley's computer is infected with a keylogger and spyware. The keylogger and spyware record information in hidden files.
2. Marley visits amazon.com on a web browser. The spyware records the visit.
3. The keylogger records Marley's Amazon username and password when Marley logs in.
4. Marley buys a desk lamp on amazon.com. The spyware records the purchase.
5. Marley's information is sent to the attacker.

PARTICIPATION ACTIVITY | 1.9.8: Spyware.

1) An attacker uses spyware to gain _____.
   - information
   - money

2) Using _____ can limit the impact of a keylogger.
   - a password manager
   - multi-factor authentication (MFA)

- strong passwords

Real world examples

- *Spyware - Hermit spyware targets Android and iOS phones. Hermit can track calls and location, read text messages, access photos, and record audio.*
- *Keylogger - The Snake keylogger is spread through a malicious PDF email attachment. When a user opens the attachment, the Snake keylogger is installed and records the user's keystrokes.*
- *Bloatware - The Superfish VisualDiscovery bloatware, installed on some Lenovo PCs in 2015, was vulnerable to on-path attacks through HTTPS spoofing.*

CHALLENGE ACTIVITY 1.9.1: Malware.

581480.4344582.qx3zqy7

Start

Select the attributes of a worm.

- [ ] Runs malicious commands
- [ ] Requires a host
- [ ] Injected directly into memory
- [ ] Spreads to other devices
- [ ] Standalone application
- [ ] Spreads over a network

©zyBooks 12/12/24 17:58 2172291
Daren Diaz
OUCYBS3213FreezeFall2024

1 2 3

Check Next

1.10 Malware: Mislead and hide

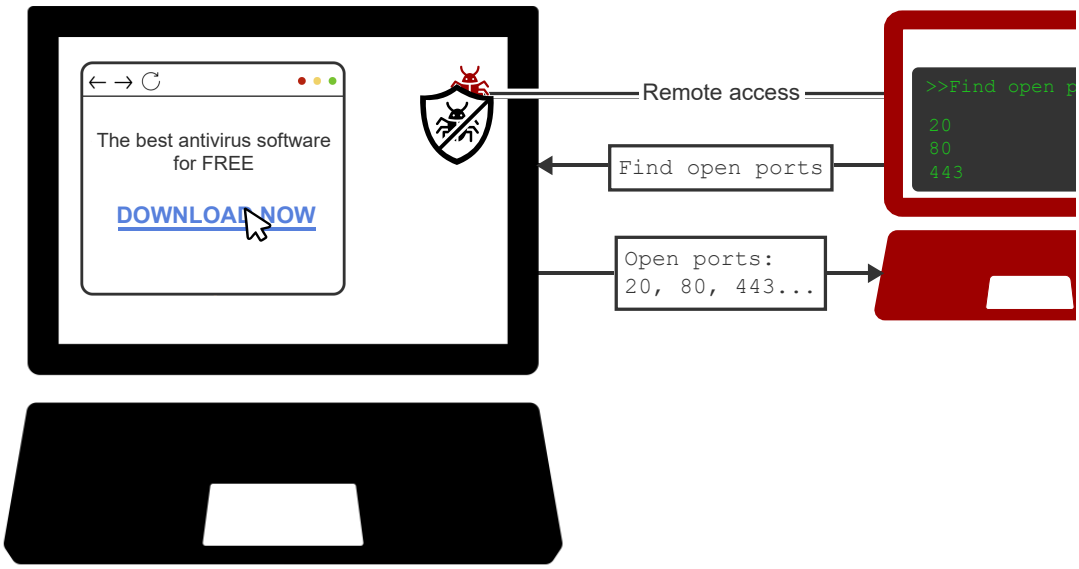
Mislead: Trojan, remote access trojan (RAT), and potentially unwanted program (PUP)

A ***trojan*** is a type of malware disguised as legitimate software such as a game or a utility application. A trojan performs the legitimate functions, so a user may not realize that the trojan is also stealing information or causing damage. Ex: The Xafecopy trojan infected Android devices through battery optimization apps and then subscribed users to unwanted paid services.

One type of trojan, called a ***remote access trojan (RAT)***, gives an attacker remote access to an infected device. A RAT can be used to gain information, change device settings, or install other malware. Ex: The DarkComet RAT was used by the Syrian government to spy on Syrian citizens. DarkComet was distributed as a PDF file. When a user opened the file, DarkComet infected the user's device.

A ***potentially unwanted program (PUP)*** is a type of software that a user considers unnecessary but does not intentionally cause damage. A PUP is usually installed with other software. Ex: A user installs a Chrome extension that searches for digital coupons. The extension also installs adware that displays popup ads when the user visits certain sites.

PARTICIPATION ACTIVITY | 1.10.1: RAT.



Animation content:

Static image: A black laptop on the left and a red laptop on the right. The black laptop has a browser with the text "The best antivirus software for FREE" and a link to download. A cursor hovers above the download link. The black laptop also has an antivirus icon on the desktop. A red bug peeks out from behind the antivirus icon. A connection labeled "Remote access" connects the red bug with the red laptop on the right. An arrow labeled "Find open ports" points from the red laptop to the black laptop. An arrow labeled "Open ports: 20, 80, 443" points from the black laptop to the red laptop. The red

laptop has a console with the text ">>Find open ports" and a list showing 20, 80, and 443.
Step 1: A user downloads free antivirus software.
A black laptop appears. A browser appears on the laptop screen. The browser has the text "The best antivirus software for FREE" and a link to download. A cursor appears and moves onto the download link. An antivirus icon appears on the download link and moves onto the laptop's desktop.
Step 2: The software includes hidden malware that gives an attacker remote access to the infected device.
A red bug peeks up from behind the antivirus icon. A red laptop appears on the right, and a connection labeled "Remote access" connects the red bug and the red laptop.
Step 3: The attacker can remotely command the infected device to scan for open ports. The list of open ports is returned to the attacker. The attacker can then use an open port to hack the system.
A console appears on the red laptop. The text ">>Find open ports" appears in the console. An arrow labeled "Find open ports" appears pointing from the red laptop to the black laptop. An arrow labeled "Open ports: 20, 80, 443" points from the black laptop to the red laptop. A list with 20, 80, and 443 appears in the console on the red laptop.

Animation captions:

1. A user downloads free antivirus software.
2. The software includes hidden malware that gives an attacker remote access to the infected device.
3. The attacker can remotely command the infected device to scan for open ports. The list of open ports is returned to the attacker. The attacker can then use an open port to hack the system.

PARTICIPATION ACTIVITY 1.10.2: Misleading malware.

1) Cary installed a new computer game and noticed a browser toolbar was installed at the same time. The browser toolbar is a _____.
   - PUP
   - RAT
   - trojan

2) A RAT can be seen as a trojan containing _____.
   - bot malware and ransomware
   - bot malware and spyware
   - spyware only

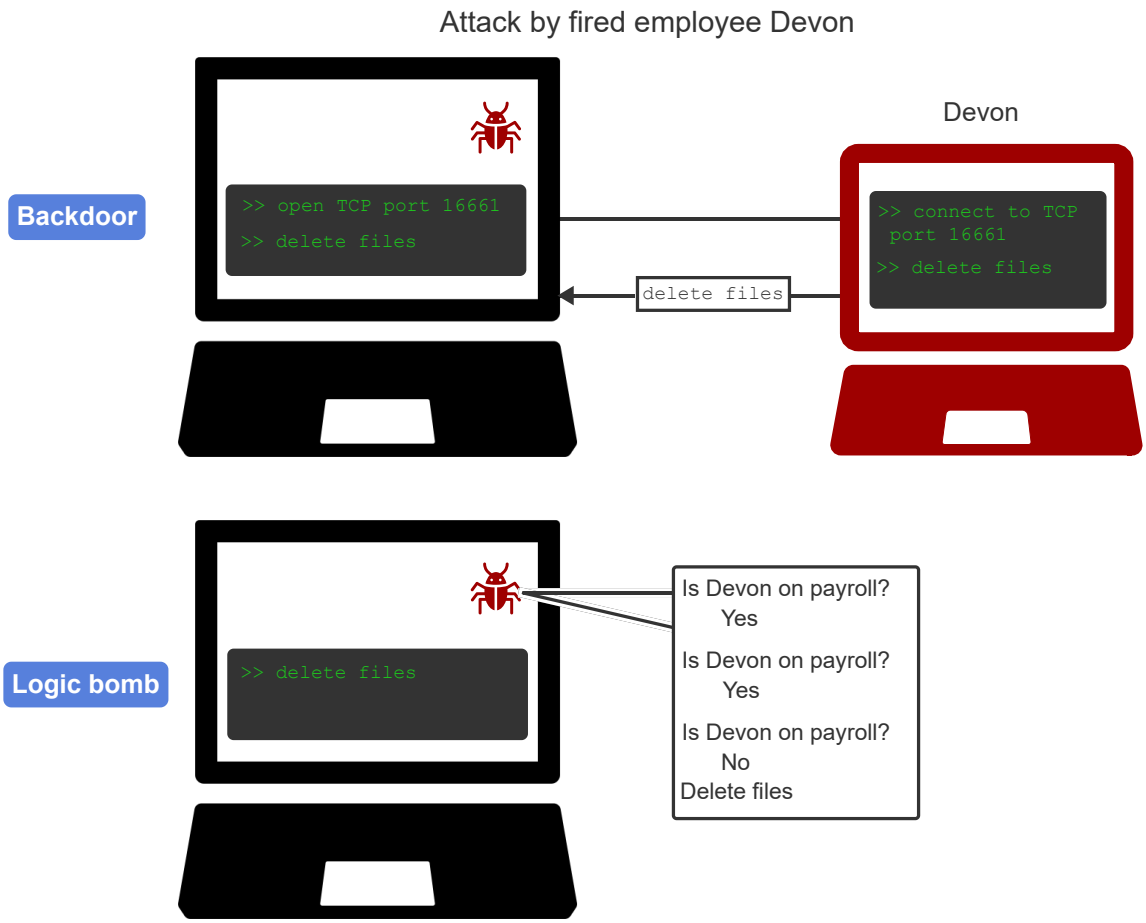
3) Dana wants to download a new photo editing app. Dana can avoid infecting the smartphone with a trojan by _____.
   - downloading the app to see what happens
   - reading the app's description
   - researching the app's developer

Hide: Backdoor and logic bomb

A ***backdoor*** is a type of malware that enables unauthenticated access to a device. A backdoor allows an attacker to bypass regular authentication procedures. A backdoor is usually included as part of a larger malware package. Ex: XcodeSpy is used to attack iOS app developer systems. When XcodeSpy infects a device, a backdoor called EggShell is also installed. The attacker can use the EggShell backdoor to control the target developer's microphone, camera, and keyboard.

A ***logic bomb*** is a type of malware that activates an attack when specified conditions are met. Ex: A Siemens contractor inserted logic bombs on Siemens's system so that Siemens would have to hire the contractor to fix the system. The logic bomb damaged the Siemens's spreadsheets on certain specified dates.

PARTICIPATION ACTIVITY | 1.10.3: Backdoor and logic bomb.



Animation content:

Static image: A general label "Attack by fired employee Devon." Representations of a backdoor and a logic bomb. The backdoor representation has a black computer and a red computer. The black computer has a red bug icon and a terminal with two lines of text: ">> open TCP port 16661" and ">> delete files." A line connects the black computer to the red computer. The red computer is labeled "Devon" and has a terminal with two lines of text: ">> connect to TCP port 16661" and ">> delete files." An arrow labeled "delete files" points from the red computer to the black computer. The logic bomb representation has a black computer with a red bug and a terminal. The red bug is connected to a text box with the text "Is Devon on payroll? Yes. Is Devon on payroll? Yes. Is Devon on payroll? No. Delete files." The terminal has the text ">> delete files."
Step 1: While employed, Devon installs a backdoor on a company computer. The backdoor opens

TCP port 16661. A "Backdoor" label and a black computer appear. A red bug appears on the computer. A terminal appears, and the text ">> open TCP port 16661" flies from the bug to the terminal.
Step 2: When Devon is fired, Devon can connect to TCP port 16661 and send a command to delete important files. A red computer labeled "Devon" appears with a terminal. The text ">> connect to TCP port 16661" appears in the terminal, and a line connecting the black and red computers appears. The text ">> delete files" appears in the terminal and a copy of the text flies to an arrow that appears from the red computer to the black computer. The text ">> delete files" appears in the terminal on the black computer.
Step 3: Alternatively, Devon could install a logic bomb. Every day, the logic bomb checks whether Devon is on the company payroll. A "Logic bomb" label and black computer appear. A red bug appears on the computer. A text box appears connected to the red bug. The text "Is Devon on payroll?" appears in the box. The text "Yes" appears on the line below. The text "Is Devon on payroll?" appears on the next line. The text "Yes" appears on the next line.
Step 4: If Devon is not on the payroll, the logic bomb executes the attack and deletes important files. In the text box, the text "Is Devon on payroll?" appears. The text "No" appears on the line below. The text "Delete files" appears on the next line. A terminal appears on the black computer, and the text ">> delete files" flies from the text box to the terminal.

Animation captions:

1. While employed, Devon installs a backdoor on a company computer. The backdoor opens TCP port 16661.
2. When Devon is fired, Devon can connect to TCP port 16661 and send a command to delete important files.
3. Alternatively, Devon could install a logic bomb. Every day, the logic bomb checks whether Devon is on the company payroll.
4. If Devon is not on the payroll, the logic bomb executes the attack and deletes important files.

PARTICIPATION ACTIVITY | 1.10.4: Backdoor and logic bomb.

1) A _____ automatically executes an attack.
   - backdoor
   - logic bomb

2) The use of _____ has become a point of conflict between law enforcement and tech companies.
   - backdoors
   - logic bombs

3) Logic bombs are often used by disgruntled employees because an employee has more _____ than an external attacker.
   - insider knowledge
   - monetary resources
   - technical training

Hide: Rootkit

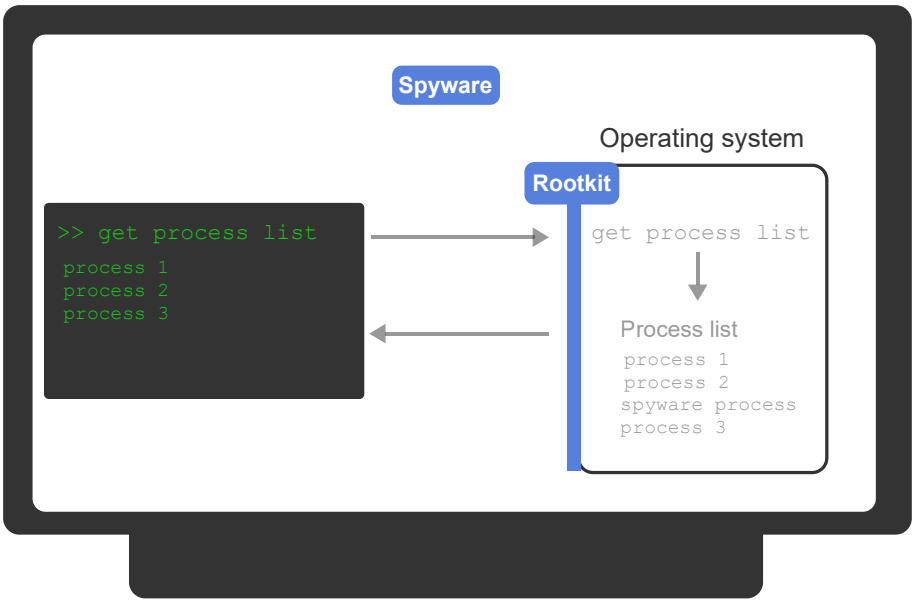
A ***rootkit*** is a type of malware that provides administrative, or root access to a computing device without permission or detection. A rootkit may be designed to:

- install, hide, or prevent the removal of other malware.
- allow an attacker to use the device to attack other devices.
- create a backdoor that allows an attacker to access confidential data.

Ex: The Sony BMG rootkit was used to enforce copyright protection. The rootkit was installed on a computer when a Sony CD was inserted. The rootkit modified the operating system to interfere with CD copying and hide the rootkit's presence.

Several rootkit types exist. A rootkit is classified by the injection location. Ex: A kernel rootkit targets a device's operating system (OS) and an application rootkit alters an application's executable file so that the rootkit runs when the application is started.

PARTICIPATION ACTIVITY | 1.10.5: Kernel rootkit.



Animation content:

Static image: A computer with bash terminal, a box labeled "Operating system," and a "Spyware" box. A "Rootkit" label is in the top-left corner of the Operating system box with a long rectangle extending from the "Rootkit" label to the bottom of the Operating system box. The text "$ get process list" is in the bash terminal with an arrow pointing to the text "get process list" in the operating system box. An arrow points from "get process list" in the operating system box to a list of processes also in the Operating system box. The process list includes process 1, process 2, spyware process, and process 3. An arrow points from the process list in the Operating system box to a process list in the bash terminal. The process list in the bash terminal includes process 1, process 2, and process 3.
Step 1: Malware is installed on a computer after a user clicks on a malicious link.
A computer outline. A box labeled Malware package appears and flies into the computer outline. The malware package box contains two elements labeled Spyware and Rootkit.
Step 2: The rootkit embeds itself in the operating system and monitors commands to the operating

system.
A box labeled "Operating system" appears. Malware package outline and label fade out. The spyware element moves to the top of the computer outline. The rootkit element moves to overlap with the top-left corner of the Operating system box. A highlight box appears below the rootkit element and runs along the left side of the Operating system box.
Step 3: The user requests a process list to search for malware. The rootkit intercepts the incoming request and alters the returned process list to hide the spyware while the spyware continues to run.
A bash terminal appears. "$ get process list" appears in the bash terminal. It moves to the Operating system box. An arrow appears below "Get process list." Below the arrow, a list called Process list appears with elements: process 1, process 2, spyware process, process 3. The process list moves toward the bash terminal and stops in the highlight box below the rootkit element. The "spyware process" text changes to red and then fades out. The "process 3" text moves up. The process list now contains: process 1, process 2, process 3. The process list moves to the bash terminal.

Animation captions:

1. Malware is installed on a computer after a user clicks on a malicious link.
2. The rootkit embeds itself in the operating system and monitors commands to the operating system.
3. The user requests a process list to search for malware. The rootkit intercepts the incoming request and alters the returned process list to hide the spyware while the spyware continues to run.

PARTICIPATION ACTIVITY 1.10.6: Rootkits.

1) What type of system account enables a rootkit to avoid detection?
   - user
   - privileged
   - guest

2) Anti-malware software is not effective at rootkit detection because _____.
   - a rootkit can alter OS operations to hide itself
   - a rootkit is not malware
   - a rootkit attacks a network

3) Which type of rootkit runs before the operating system?
   - Application rootkit
   - Kernel rootkit
   - Firmware rootkit

Exploring further:

- Xafecopy trojan
- DarkComet RAT

- XcodeSpy
- Siemens contractor logic bomb
- Investment bank logic bomb
- Michelangelo virus
- Sony BMG rootkit

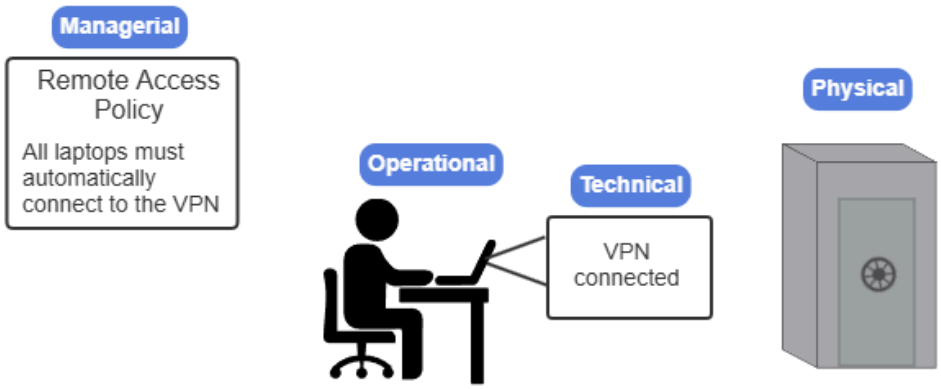
1.11 Security control types

Security control categories

A ***security control*** is a mechanism used to protect the confidentiality, integrity, and availability of an organization's systems and data. Security controls are separated into the following categories:

- ***Technical control*** - A control that is performed by a system. Ex: A firewall rule blocks all incoming traffic from a certain IP address.
- ***Managerial control*** - A control that addresses risk management and governance through established procedures. Ex: An organization's password policy states that employees must change passwords every 90 days.
- ***Operational control*** - A control that is performed by employees. Ex: An employee conducts security awareness training for new employees.
- ***Physical control*** - A control that secures the physical environment. Ex: A security camera that records people entering and exiting an office building.

PARTICIPATION ACTIVITY 1.11.1: Security control categories.



Animation content:

Static figure: A safe labeled "Physical". A VPN policy labeled "Managerial" that says, "All laptops must automatically connect to the VPN." The label "Operational" above an employee sitting at a desk with a laptop. The laptop screen is labeled "Technical" and says "VPN connected."

Animation captions:

1. A laptop is issued to a new employee. The laptop is stored in a locked safe - a physical security control.
2. Company remote access policy states that all laptops must automatically connect to the company's VPN server. The policy is a managerial control.
3. The IT employee sets the laptop to automatically connect to the VPN. Performing the task is an operational control.
4. The automatic VPN connection is a technical control.

PARTICIPATION ACTIVITY | 1.11.2: Security control categories.

Select the category of each security control.

How to use this tool

Physical **Operational** **Managerial** **Technical**

	Email security awareness training
	Door locks
	Employee offboarding procedures
	Encryption

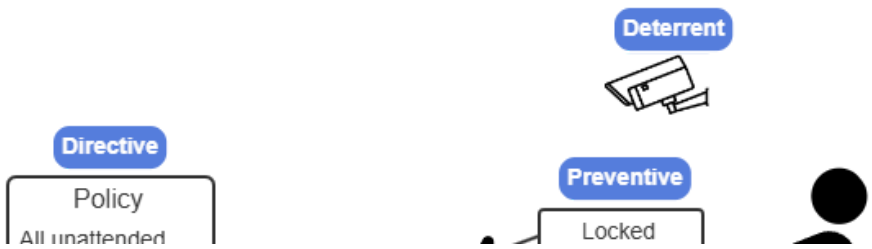
Reset

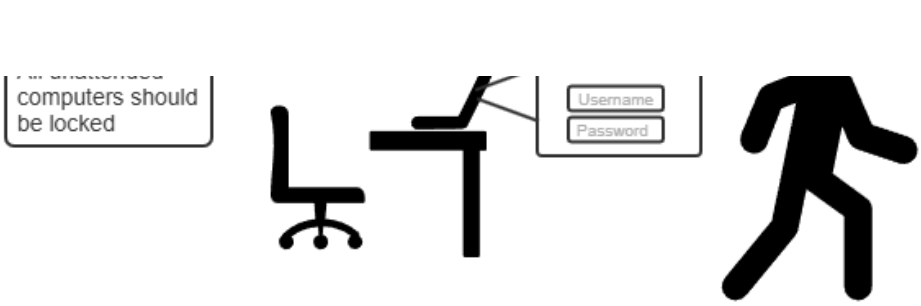
Passive security controls: Preventive, deterrent, and directive

A security control is also classified by the control's purpose. A passive security control aims to minimize the occurrence of security issues rather than actively responding to security issues. Passive security controls include:

- ***Preventive control*** - A control that prevents a security issue. Ex: A locked door to prevent unauthorized individuals from entering a sensitive area.
- ***Deterrent control*** - A control that deters an individual from violating security policies. Ex: Adequate lighting placed at all building entrances.
- ***Directive control*** - A control that gives direction. Ex: An organization's laptop Acceptable Use Policy (AUP).

PARTICIPATION ACTIVITY | 1.11.3: Preventive, deterrent, and directive controls.





Animation content:

Static figure: A person walking away from a laptop on a desk. The label "Deterrent" is above a security camera. The label "Directive" is above the policy "All unattended computers should be locked." The label "Preventive" is above the locked computer screen.

Animation captions:

1. Security controls are used to protect against unauthorized access when an employee leaves a computer unattended.
2. The deterrent control is the security camera pointed towards the desk.
3. The directive control is a policy stating that an employee must lock a computer when leaving the computer unattended.
4. The preventive control is the requirement of a user login to access the computer.

PARTICIPATION ACTIVITY 1.11.4: Passive security controls.

1) Preventive, deterrent, and directive security controls are used to _____ a security issue.
   - avoid
   - respond to
   - report

2) A scheduled risk assessment is a _____ security control.
   - deterrent
   - directive
   - preventive

3) A fence is a _____ security control.
   - deterrent
   - directive
   - preventive

4) The strongest passive security controls are _____ security controls.
   - deterrent
   - directive

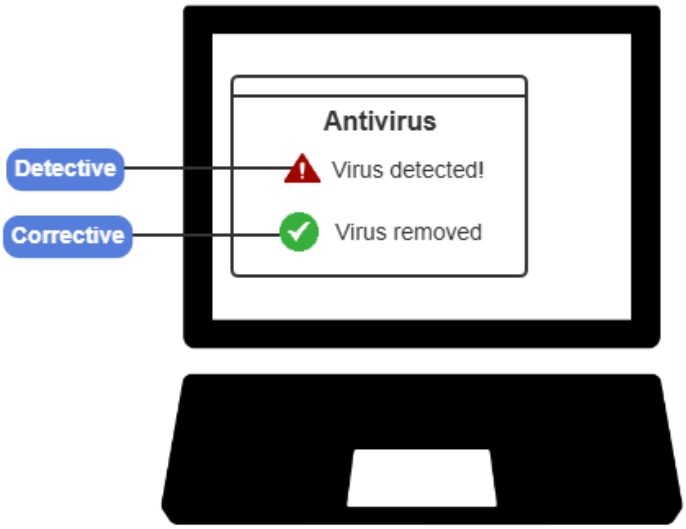
- preventive

Active security controls: Detective and corrective

Detective and corrective security controls actively respond to a security issue.

- ***Detective control*** - A control that detects a security issue. Ex: Door alarms and motion detectors.
- ***Corrective control*** - A control that restores normal operations after a security issue occurs. Ex: Restoring backup data after a ransomware attack.

PARTICIPATION ACTIVITY 1.11.5: Detective and corrective controls.



Animation content:

Static figure: A computer showing antivirus software.
Step 1: An employee opens a malicious file in an email and the employee's laptop is infected with a virus.
A black laptop with a window labeled "Antivirus". An envelope flies onto the laptop screen and opens. A red bug moves from the envelope onto the laptop screen. The laptop turns red.
Step 2: The antivirus software is a detective control because the software detects the virus and alerts the user.
"Virus detected!" appears in the Antivirus window. The label "Detective" appears and points to "Virus detected!"
Step 3: The antivirus software is also a corrective control because the software removes the virus from the laptop.
"Removing virus" appears in the Antivirus window. The red bug disappears. The laptop turns black.
"Virus removed" appears in the Antivirus window. The label "Corrective" appears and points to "Virus removed".

Animation captions:

1. An employee opens a malicious file in an email and the employee's laptop is infected with a virus.
2. The antivirus software is a detective control because the software detects the virus and alerts the user.
3. The antivirus software is also a corrective control because the software removes the virus from the laptop.

PARTICIPATION ACTIVITY 1.11.6: Detective and corrective controls.

Select each security control's type.

1) Intrusion detection system
   - Detective
   - Corrective

2) File integrity monitoring (FIM)
   - Detective
   - Corrective

3) Backup power generator
   - Detective
   - Corrective

Compensating security controls

A compensating security control addresses weaknesses of existing controls or compensates for the inability to meet specific security requirements. Ex: An organization requires separation of duties but does not have enough employees to implement separation of duties. Two-person integrity is implemented for sensitive tasks as a compensating control.

1.12 LAB: Basics (Walkthrough)

IT-Labs are not printable at this time.

1.13 LAB: Malware (Walkthrough)

IT-Labs are not printable at this time.

1.14 LAB: Credential harvesting using email phishing (Walkthrough)

IT-Labs are not printable at this time.

1.15 LAB: Basics (Scenario)

IT-Labs are not printable at this time.