CYBER SECURITY

Comp Sci 3: Introduction to Computer Systems

A basic understanding of information security can help you avoid unnecessarily leaving your software and systems insecure and vulnerable to weaknesses that can be exploited for financial gain or other malicious reasons. You should be aware of the role and importance of security throughout the use and development of software and networked systems.

The classic model for information security defines three objectives of security: maintaining confidentiality, integrity, and availability. Known as the CIA model. Each objective addresses a different aspect of providing protection for information.

Confidentiality

Confidentiality refers to protecting information from being accessed by unauthorized parties. In other words, only the people who are authorized to do so can gain access to sensitive data. Imagine your bank records. You should be able to access them, of course, and employees at the bank who are helping you with a transaction should be able to access them, but no one else should. A failure to maintain confidentiality means that someone who shouldn't have access has managed to get it, through intentional behavior or by accident. Such a failure of confidentiality, commonly known as a *breach*, typically cannot be remedied. Once the secret has been revealed, there's no way to un-reveal it. If your bank records are posted on a public website, everyone can know your bank account number, balance, etc., and that information can't be erased from their minds, papers, computers, and other places. Nearly all the major security incidents reported in the media today involve major losses of confidentiality.
So, in summary, a breach of confidentiality means that someone gains access to information who shouldn't have access to it.

Integrity

Integrity refers to ensuring the authenticity of information—that information is not altered, and that the source of the information is genuine. Imagine that you have a website and you sell products on that site. Now imagine that an attacker can shop on your web site and maliciously alter the prices of your products, so that they can buy anything for whatever price they choose. That would be a failure of integrity, because your information—in this case, the price of a product—has been altered and you didn't authorize this alteration. Another example of a failure of integrity is when you try to connect to a website and a malicious attacker between you and the website redirects your traffic to a different website. In this case, the site you are directed to is not genuine.

Availability

Availability means that information is accessible by authorized users.

Vulnerability Categories

A vulnerability is a weakness in a system that can be exploited to negatively impact confidentiality, integrity, and/or availability. There are many ways in which vulnerabilities can be categorized. This article uses three high-level vulnerability categories: software flaws, security configuration issues, and software feature misuse. These categories are described below.

Software flaw vulnerability

A *software flaw vulnerability* is caused by an unintended error in the design or coding of software. An example is an input validation error, such as user-provided input not being properly evaluated for malicious character strings and overly long values associated with known attacks. Another example is a race condition error that allows the attacker to perform a specific action with elevated privileges.

A security configuration setting is an element of a software's security that can be altered through the software itself. Examples of settings are an operating system offering access to control lists that set the privileges that users have for files, and an application offering a setting to enable or disable the encryption of sensitive data stored by the application. A*security configuration issue vulnerability* involves the use of security configuration settings that negatively affect the security of the software.

A software feature is a functional capability provided by software. A *software feature misuse vulnerability* is a vulnerability in which the feature also provides an avenue to compromise the security of a system. These vulnerabilities are caused by the software designer making trust assumptions that permit the software to provide beneficial features, while also introducing the possibility of someone violating the trust assumptions to compromise security. For example, email client software may contain a feature that renders HTML content in email messages. An attacker could craft a fraudulent email message that contains hyperlinks that, when rendered in HTML, appear to the recipient to be benign but actually take the recipient to a malicious web site when they are clicked on. One of the trust assumptions in the design of the HTML content rendering feature was that users would not receive malicious hyperlinks and click on them.

Software feature misuse vulnerabilities are introduced during the design of the software or a component of the software (e.g., a protocol that the software implements). Trust assumptions may have been explicit—for example, a designer being aware of a security weakness and determining that a separate security control would compensate for it. However, trust assumptions are often implicit, such as creating a feature without first evaluating the risks it would introduce. Threats may also change over the lifetime of software or a protocol used in software. For example, the Address Resolution Protocol (ARP) trusts that an ARP reply contains the correct mapping between Media Access Control (MAC) and Internet Protocol (IP) addresses. The ARP cache uses that information to provide a useful service—to enable sending data between devices within a local network. However, an attacker could generate false ARP messages to poison a system's ARP table and thereby launch a denial-of-service or a man-in-the-middle attack. The ARP protocol was standardized over 25 years ago, and threats have changed a great deal since then, so the trust assumptions inherent in its design then are unlikely to still be reasonable today.

It may be hard to differentiate software feature misuse vulnerabilities from the other two categories. For example, both software flaws and misuse vulnerabilities may be caused by deficiencies in software design processes. However, software flaws are purely negative—they provide no positive benefit to security or functionality—while software feature misuse vulnerabilities occur as a result of providing additional features.

There may also be confusion regarding misuse vulnerabilities for features that can be enabled or disabled—in a way, configured—versus security configuration issues. The key difference is that for a misuse vulnerability, the configuration setting enables or disables the entire feature and does not specifically alter just its security; for a security configuration issue vulnerability, the configuration setting alters only the software's security. For example, a setting that disables all use of HTML in emails has a significant impact on both security and functionality, so a vulnerability related to this setting would be a misuse vulnerability. A setting that disables the use of an antiphishing feature in an email client has a significant impact on only security, so a vulnerability with that setting would be considered a security configuration issue vulnerability.

The Presence of Vulnerabilities

No system is 100% secure: every system has vulnerabilities. At any given time, a system may not have any known software flaws, but security configuration issues and software feature misuse vulnerabilities are always present. Misuse vulnerabilities are inherent in software features because each feature must be based on trust assumptions—and those assumptions can be broken, albeit involving significant cost and effort in some cases. Security configuration issues are also unavoidable for two reasons. First, many configuration settings increase security at the expense of reducing functionality, so using the most secure settings could make the software useless or unusable. Second, many security settings have both positive and negative consequences for security. An example is the number of consecutive failed authentication attempts to permit before locking out a user account. Setting this to 1 would be the most secure setting against password guessing attacks, but it would also cause legitimate users to be locked out after mistyping a password once, and it would also permit attackers to perform denial-of-service attacks against users more easily by generating a single failed login attempt for each user account.

Because of the number of vulnerabilities inherent in security configuration settings and software feature misuse possibilities, plus the number of software flaw vulnerabilities on a system at any given time, there may be dozens or hundreds of vulnerabilities on a single system. These vulnerabilities are likely to have a wide variety of characteristics. Some will be very easy to exploit, while others will only be exploitable under a combination of highly unlikely conditions. One vulnerability might provide root-level access to a system, while another vulnerability might only permit read access to an insignificant file. Ultimately, organizations need to know how difficult it is for someone to exploit each vulnerability and, if a vulnerability is exploited, what the possible impact would be.

Threat

A *threat* is any circumstance or event with the potential to adversely impact data or systems via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. Threats may involve intentional actors (e.g., attacker who wants to access information on a server) or unintentional actors (e.g., administrator who forgets to disable user accounts of a former employee.) Threats can be local, such as a disgruntled employee, or remote, such as an attacker in another geographical area.
A *threat source* is the cause of a threat, such as a hostile cyber or physical attack, a human error of omission or commission, a failure of organization-controlled hardware or software, or other failure beyond the control of the organization. A *threat event* is an event or situation initiated or caused by a threat source that has the potential for causing adverse impact.

Many threats against data and resources are possible because of mistakes—either bugs in operating system and applications that create exploitable vulnerabilities, or errors made by end users and administrators.

Network traffic typically passes through intermediate computers, such as routers, or is carried over unsecured networks, such as wireless hotspots. Because of this, it can be intercepted by a third party. Threats against network traffic include the following:

- **Eavesdropping.** Information remains intact, but its privacy is compromised. For example, someone could learn your credit card number, record a sensitive conversation, or intercept classified information.
- **Tampering.** Information in transit is changed or replaced and then sent on to the recipient. For example, someone could alter an order for goods or change a person's resume.
- **Impersonation.** Information passes to a person who poses as the intended recipient. Impersonation can take two forms:
  - **Spoofing.** A person can pretend to be someone else. For example, a person can pretend to have the email address jdoe@example.net, or a computer can identify itself as a site called www.example.net when it is not. This type of impersonation is known as spoofing.
  - **Misrepresentation.** A person or organization can misrepresent itself. For example, suppose the site www.example.net pretends to be a furniture store when it is really just a site that takes credit-card payments but never sends any goods.

Security Controls

Sensitive data should be protected based on the potential impact of a loss of confidentiality, integrity, or availability. Protection measures (otherwise known as *security controls*) tend to fall into two categories. First, security weaknesses in the system need to be resolved. For example, if a system has a known vulnerability that attackers could exploit, the system should be patched so that the vulnerability is removed or mitigated. Second, the system should offer only the required functionality to each authorized user, so that no one can use functions that are not necessary. This principle is known as *least privilege*. Limiting functionality and resolving security weaknesses have a common goal: give attackers as few opportunities as possible to breach a system.

There are three types of security controls, as follows:

- *Management controls*: The security controls that focus on the management of risk and the management of information system security.
- *Operational controls*: The security controls that are primarily implemented and executed by people (as opposed to systems).
- *Technical controls*: The security controls that are primarily implemented and executed by the system through the system's hardware, software, or firmware.

All three types of controls are necessary for robust security. For example, a security policy is a management control, but its security requirements are implemented by people (operational controls) and systems (technical controls). Think of phishing attacks. An organization may have an acceptable use policy that specifies the conduct of users, including not visiting malicious websites. Security controls to help thwart phishing, besides the management control of the acceptable use policy itself, include operational controls, such as training users not to fall for phishing scams, and technical controls that monitor emails and web site usage for signs of phishing activity.

A common problem with security controls is that they often make systems less convenient or more difficult to use. When usability is an issue, many users will attempt to circumvent security controls; for example, if passwords must be long and complex, users may write them down. Balancing security, functionality, and usability is often a challenge. The goal should be to strike a proper balance: provide a reasonably secure solution while offering the functionality and usability that users require.

Another fundamental principle with security controls is using multiple layers of security—*defense in depth*. For example, sensitive data on a server may be protected from external attack by several controls, including a network-based firewall, a host-based firewall, and OS patching. The motivation for having multiple layers is that if one layer fails or otherwise cannot counteract a certain threat, other layers might prevent the threat from successfully breaching the system. A combination of network-based and host-based controls is generally most effective at providing consistent protection.

TCP/IP Security

TCP/IP is widely used throughout the world to provide network communications. TCP/IP communications are composed of four layers that work together. When a user wants to transfer data across networks, the data is passed from the highest layer through intermediate layers to the lowest layer, with each layer adding information. At each layer, the logical units are typically composed of a header and a payload. The *payload* consists of the information passed down from the previous layer, while the *header* contains layer-specific information such as addresses. At the application layer, the payload is the actual application data. The lowest layer sends the accumulated data through the physical network; the data is then passed up through the layers to its destination. Essentially, the data produced by a layer is encapsulated in a larger container by the layer below it. The four TCP/IP layers, from highest to lowest, are shown below.

- **Application Layer.** This layer sends and receives data for particular applications, such as Domain Name System (DNS), HyperText Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP).

- **Transport Layer.** This layer provides connection-oriented or connectionless services for transporting application layer services between networks. The transport layer can optionally assure the reliability of communications. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are commonly used transport layer protocols.

- **Network Layer.** This layer routes packets across networks. Internet Protocol (IP) is the fundamental network layer protocol for TCP/IP. Other commonly used protocols at the network layer are Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP).

- **Data Link Layer.** This layer handles communications on the physical network components. The best-known data link layer protocol is Ethernet.
  Security controls exist for network communications at each layer of the TCP/IP model. As previously explained, data is passed from the highest to the lowest layer, with each layer adding more information. Because of this, a security control at a higher layer cannot provide protection for lower layers, because the lower layers perform functions of which the higher layers are not aware. Security controls that are available at each layer include:

- **Application Layer.** Separate controls must be established for each application. For example, if an application needs to protect sensitive data sent across networks, the application may need to be modified to provide this protection. While this provides a very high degree of control and flexibility over the application's security, it may require a large resource investment to add and configure controls properly for each application. Designing a cryptographically sound application protocol is very difficult, and implementing it properly is even more challenging, so creating new application layer security controls is likely to create vulnerabilities. Also, some applications, particularly off-the-shelf software, may not be capable of providing such protection. While application layer controls can protect application data, they cannot protect TCP/IP information such as IP addresses because this information exists at a lower layer. Whenever possible, application layer controls for protecting network communications should be standards-based solutions that have been in use for some time. One example is Secure Multipurpose Internet Mail Extensions (S/MIME), which is commonly used to encrypt email messages.

- **Transport Layer.** Controls at this layer can be used to protect the data in a single communication session between two hosts. Because IP information is added at the network layer, transport layer controls cannot protect it. The most common use for transport layer protocols is securing HTTP traffic; the Transport Layer Security (TLS) protocol is usually used for this. (TLS is the standards-based version of SSL version 3. More information on TLS is available in RFC 4346, *The TLS Protocol Version 1.1*, available at https://www.ietf.org/rfc/rfc4346.txt. Another good source of information is NIST SP 800-52, *Guidelines on the Selection and Use of Transport Layer Security*, available from https://csrc.nist.gov/publications/nistpubs/.) The use of TLS typically requires each application to support TLS; however, unlike application layer controls, which typically involve extensive customization of the application, transport layer controls such as TLS are much less intrusive because they do not need to understand the application's functions or characteristics. Although using TLS may require modifying some applications, TLS is a well-tested protocol that has several implementations that have been added to many applications, so it is a relatively low-risk option compared to adding protection at the application layer. Traditionally TLS has been used to protect HTTP-based communications and can be used with SSL portal VPNs.

- **Network Layer.** Controls at this layer can be applied to all applications; thus, they are not application-specific. For example, all network communications between two hosts or networks can be protected at this layer without modifying any applications on the clients or the servers. In some environments, network layer controls such as Internet Protocol Security (IPsec) provide a much better solution than transport or application layer controls because of the difficulties in adding controls to individual applications. Network layer controls also provide a way for network administrators to enforce certain security policies. Another advantage of network layer controls is that since IP information (e.g., IP addresses) is added at this layer, the controls can protect both the data within the packets and the IP information for each packet. However, network layer controls provide less control and flexibility for protecting specific applications than transport and application layer controls. SSL tunnel VPNs provide the ability to secure both TCP and UDP communications including client/server and other network traffic, and therefore act as network layer VPNs.

- **Data Link Layer.** Data link layer controls are applied to all communications on a specific physical link, such as a dedicated circuit between two buildings or a dial-up modem connection to an Internet Service Provider (ISP). Data link layer controls for dedicated circuits are most often provided by specialized hardware devices known as *data link encryptors*; data link layer controls for other types of connections, such as dial-up modem communications, are usually provided through software. Because the data link layer is below the network layer, controls at this layer can protect both data and IP information. Compared to controls at the other layers, data link layer controls are relatively simple, which makes them easier to implement; also, they support other network layer protocols besides IP. Because data link layer controls are specific to a particular physical link, they cannot protect connections with multiple links, such as establishing a VPN over the Internet. An Internet-based connection is typically composed of several physical links chained together; protecting such a connection with data link layer controls would require deploying a separate control to each link, which is not feasible. Data link layer protocols have been used for many years primarily to provide additional protection for specific physical links that should not be trusted. Because they can provide protection for many applications at once without modifying them, network layer security controls have been used frequently for securing communications, particularly over shared networks such as the Internet. Network layer security controls provide a single solution for protecting data from all applications, as well as protecting IP information. Nevertheless, in many cases, controls at another layer are better suited to providing protection than network layer controls. For example, if only one or two applications need protection, a network layer control may be excessive. Transport layer protocols such as SSL are most commonly used to provide security for communications with individual HTTP-based applications, although they are also used to provide protection for communication sessions of other types of applications such as SMTP, Point of Presence (POP), Internet Message Access Protocol (IMAP), and File Transfer Protocol (FTP). Because all major Web browsers include support for TLS, users who wish to use Web-based applications that are protected by TLS normally do not need to install any client software or reconfigure their systems. Newer applications of transport layer security protocols protect both HTTP and non-HTTP application communications, including client/server applications and other network traffic. Controls at each layer offer advantages and features that controls at other layers do not.

SSL is the most commonly used transport layer security control. Depending on how SSL is implemented and configured, it can provide any combination of the following types of protection:

- **Confidentiality.** SSL can ensure that data cannot be read by unauthorized parties. This is accomplished by encrypting data using a cryptographic algorithm and a secret key—a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.

- **Integrity.** SSL can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a keyed cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.

- **Peer Authentication.** Each SSL endpoint can confirm the identity of the other SSL endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host. SSL authentication is typically performed one-way, authenticating the server to the client, but it can be performed mutually.

- **Replay Protection.** The same data is not delivered multiple times, and data is not delivered grossly out of order.

Unauthorized Access and Control Systems

Encryption - decryption

Firewall is a type of security system that creates a wall that checks all incoming and outgoing messages to ensure only authorized traffic goes through. There are many different forms of this application such as Norton and Windows Security Essentials. Another way to protect your information is through **encryption**. Encryption basically scrambles and makes any message sent unreadable to anyone who does not have a key. The key is then used to decrypt the scrambled message into the original format. Whenever you go to a website that has an 'S' after the HTTP that means it is a secure web page, meaning the entire web page is encrypted. Therefore, people hacking to your web browser cannot get you credit card number or SSN. One question that arises is, "Can't you just make every website a secure web page?". The simple answer is money, a site owner needs to pay someone to encrypt the site. Then to send the data takes up more bandwidth, and slows down traffic in general. Cheaper web hosts may provide secure security features and backup services but have limitations. Another form of protection is a VPN (Virtual Private Network). A VPN creates a link between the user and some other destination. In order to access the VPN you will need a username and password, in order to keep it more secure and to block out hackers.

Firewalls can work in a number of ways, but a couple types of firewalls are more widely used over others. The two most common firewalls are packet-filtering and proxy.

Figure 1-Firewall

Packet-Filtering Firewall

- Advantages

  1. A packet-filter simply examines each packet to determine whether it is safe or not. After examining a packet, the filter will either allow in or block out the packet depending on if it’s safe or not.
  2. Packet-filters are common among routers, switches, wireless access points, etc.

- Disadvantages

1. A disadvantage of using a packet-filter firewall is that some packets that are safe may be blocked by accident. This means that it is possible that parts of information could be missing due to a packet being blocked.

Proxy Firewall

- Advantages

1. Most Secure - direct connections are limited by packets being sent from one computer to the proxy, and then mirrored over to the computer on the receiving end.
2. More secure decisions are able to be made in Application settings through strong analysis.

- Disadvantages

1. A disadvantage of a proxy firewall is that it can slow down the transfer speed of packets. Although decrease in speed or functionality is a disadvantage, it is important to remember key advantages.
2. While using a proxy firewall it is difficult for someone to figure out the location of where packets were sent from.

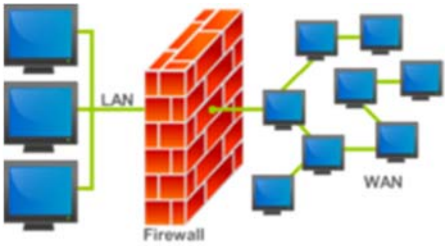
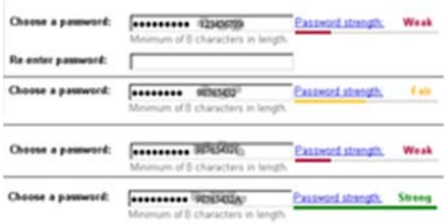


Figure 2-Firewall

The Internet was created as an open system for the free exchange of information. Due to the openness of an ideology, the Internet provides to “bad guys” the significantly greater opportunities for the penetration into information systems. Firewalls make it possible to filter incoming and outgoing traffic that flows through your system. The Firewall uses one or more sets of rules to check the network packets as they enter or exit through a network connection, it either allows the traffic through or blocks it. The Firewall could be applied for protection a single host as well as to protect the entire network. A computer Firewall may be built-in into the Operation System or installed separately. The network Firewalls are the more complicated systems, combined hardware and software. These days, there is no single, the universally accepted classification of firewalls. But according to the methods of deploying it is possible to identify three following types of them. Filtering routers are the routers or a servers running on a program configured to filter incoming and outgoing packets. The Packet filtering is carried out on the basis of information contained in TCP- and IP-packet headers. Firewalls based on Session layer gateways. This class of routers is a repeater TCP-connection. Gateway receives a request from authorized client for specific services and after validation of the requested session establishes a connection to the destination. Firewalls based on Application layer gateways. In order to protect a number of vulnerabilities inherent filtering routers, firewalls should be used by applications to filter connections with services such as Telnet and FTP. This application is called proxy-service. This gateway eliminates the direct interaction between the client and authorized external host. The gateway filters all incoming and outgoing packets at the application layer. Application Layer Gateways are good for protection; since the interaction with the outside world is realized through a small number of authorized applications, fully control all incoming and outgoing traffic. Note that application-level gateways require a separate application for each network service.These categories can be considered as the basic components of real firewalls. However, these components reflect the key features that distinguish firewalls from each other.

Figure 3- Retinal Scanner

Biometric Access Systems identify an individual based on their fingerprint, iris, or facial features or other unique physiological characteristic. Keystroke Dynamics recognize an individual's personal typing pattern to authenticate the user as s/he types a username or password. Biometric readers allow access based on the persons physical characteristics. Fingerprint readers and retinal scanners isolate an unchangeable property in an individual in order to identify them and offer high security based on these measures. They are typically used to control access to high risk facilities such as government property, prisons, and corporate headquarters. Fingerprint scanners have also been equipped into laptops in order to offer a higher standard of protection in securing personal files. In the same way, a person can download face recognition software onto their laptop as well. Because biometrics are entirely unique to the user, they are extremely accurate. In the same way no two people will have the same fingerprint, a persons facial features and iris' are as equally unique. In fact, the odds of another person having the same features as another is about 1 in 10^78 power.



Choose a password: ●●●●●●●●● 123456789 Password strength: Weak
Minimum of 8 characters in length.
Re enter password:

Choose a password: ●●●●●●●● 98765432 Password strength: Fair
Minimum of 8 characters in length.

Choose a password: ●●●●●●●●● 987654321 Password strength: Weak
Minimum of 8 characters in length.

Choose a password: ●●●●●●●●● 98765432A Password strength: Strong
Minimum of 8 characters in length.

Figure 4-Password Strength

Identification Systems are a type of Access Control System that reassures whoever wants to access your system has authorization. Along with this, Authentication Systems makes sure the person is who they say they are. Possessed Knowledge Access Systems use passwords using information only the user should know. Downsides to this system would be the ability to forget this information or for it to be found out by someone who should not know. Cognitive Authentication Systems require users to think of their answers to certain personal questions such as their first pet, where they were born, where they have been on vacation, etc. The disadvantages to this system are the same as Possessed Knowledge Access Systems; with a lapse of time a person is more likely to forget their answer to a security question, especially if it had multiple answers. Lastly, Possessed Object Access Systems are a way to identify you with a physical object such as a keycard or badge. Access Control Systems link up to different types of readers that have the ability to hold data and retrieve it when needed. Some may even have function buttons that let them collect different data used for timing and attendance purposes. Identification Systems are a great tool to ensure the safety and privacy of users and are useful for everyday computers and accounts, business accounts, and much more.

Figure 5-Wireless Connection

Many WI-FI connections are unfortunately left unsecured. This allows for any individual with a WI-FI compatible device to potentially piggy back the network. Once an individual is connected to a network, most devices connected to that network become available for a skilled hacker to view. This leaves an opening for many possible risks, especially if that network has a high traffic of sensitive information or data. Some war driving software exists which allows a user, usually with a portable device, to identify many unsecured networks in a short amount of time. This gives a hacker to identify a large number of potential targets. Cyber-Crime has become increasingly prevalent over the years. Hackers are notorious for the various crimes they commit. Using malicious software, a skilled hacker is capable of stealing credit card numbers, bank account numbers, and other personal information, some of which make it possible for them to even steal identities. Using a program such as a keylogger, a hacker can monitor keystrokes without the individual knowing, allowing them to acquire sensitive information such as a credit card number, social security number, bank account, or password. A skilled hacker with an understanding of web design can create a phishing website and acquire account information from unsuspecting website visitors.

Public Hotspot Safety

Figure 6 - Public Wifi

Public hotspots are public networks, usually found within buildings such as restaurants, airports, and hospitals that allow a free or fee-based wi-fi connection to nearby users. Because these hotspots are public, it is beneficial to take certain precautionary measures when using them. Some of these safety measure include, disabling your computer automatic wi-fi connection feature. Many modern computers will automatically connect to any available wi-fi networks and it is important to be aware of this. Also, using a firewall can protect connections from working in the opposite direction. Instead of your computer connecting to the wi-fi, there is a chance that other softwares or devices that are perhaps malicious will try to access your computer through the network. Also, you should avoid viewing or inputting personal information while using a public hotspot. Avoid online shopping which requires a credit card as well as using passwords which can link to sensitive accounts. If you are viewing and inputting personal information, then try using a virtual private network through the public hotspot which will avoid others from accessing your data. Other precautions include turning off file sharing, using antivirus software, and watching to see if others are trying to look at your computer screen within the public area.

Computer Sabotage

Malware

Malware is a term for unwanted software that gets installed on a user's computer and performs malicious tasks. It can be as simple as pop-up windows containing advertising, otherwise known as Adware, or it can cause significant damage in the form of a Virus. A Virus is a program that can replicate itself and spread to other computers by inserting its own code, wreaking havoc along the way. There are different types of computer viruses that can cause different kinds of damages to a computer. Another form of Malware is Spyware. Spyware can track a computer user's web browsing habits, obtain private information, and transmit that information to advertisers without the user's knowledge.

Figure 7- Monitor padlock

Unfortunately, without adequate protection, it is rather easy for a user to inadvertently allow malware installation. It can be as simple as clicking the wrong box in a pop-up window on a website. Protection from malware is available through various security software programs. When first purchasing a computer, it may have security programs already installed or you will automatically receive notifications on your computer to purchase spyware for an additional fee. Some are even available for free download,. Often times, if a computer is already infected, it can block anti-malware apps. One of the benefits of Malwarebytes is that it can be installed even a PC already has malicious programs on it.

Botnets and Computer Viruses

A botnet is a large group of computers that are ran on multiple bots that have been taken over; botnets are a serious threat to computer users because of their devious ways of taking over computers. At the time, computer owners did not know their computers were being altered. Botnets are commonly used for DDoS attacks, click-fraud, phishing campaigns, key logging,and host malicious web sites. There are warning signs a computer user should be aware of if he or she's computer is apart of a botnet. For example, the computer will be extremely slow, one will receive emails accusing he or she of spam, and the computer user will have email messages in his or her's outbox that was never sent. botnets can be controlled by using command and control software. Also, a malware is any type of deleterious software. A computer virus is a common type of malware that ruins computers. A virus

Figure 8-Protect Your Computer

can attach itself to programs so when the program runs, the virus will also run. There are many harmful effects that could come with a computer virus. For example, a virus could delete important data, send out fake emails, and could possibly delete the information that contains on the hard drive. Therefore, it is important for a computer user to buy an anti virus system for his or her's computer to avoid these terrible malfunctions that are very common in computers. If a computer does becomes infected, you are able to remove it with antivirus softwares. It is not impossible to remove viruses, but it is beneficial to have the software before the problem occurs.

Figure 9-Security Software is a Computer's Doctor

Although computer viruses in the past were sometimes designed to create confusion and mischief, more recent viruses have been designed to inflict much more serious damage. The perpetrators of creating such viruses are more often working for foreign governments or intelligence agencies. In recent years there have been several viruses that have become well known due to the large amount of damage they caused. One such virus was called Conficker Virus and affected Windows-based Pc's in 2009. This worm crawled through millions of computers which created an immense botnet that was able to steal financial information and data. The virus is still affecting computers today. Another well known virus was called agent.btz and occurred in 2008. This virus spread through infected thumb drives and was found on Pentagon computers. It was believed to be the work of foreign spies, and lead to the creation of U.S. Cyber Command, an agency created to battle cyber war. PoisonIvy, another computer virus launched in 2005, allowed the attacker to control the infected user's computer. This malware is known as remote access Trojan. It allows the hacker complete control of a computer. Once control is gained, the hacker could manipulate files and even get access to the computers speaker and webcam. PoisonIvy affected both defense and chemical industries in the West. Computer viruses are a serious threat. With the world relying on computers for everything from personal use to national defense, it is vital that computers be safeguarded against viruses. The next section goes on to describe security software.

Data, Program or Website Alteration

Figure 10-Facebook Logo

Alteration attacks could take many different forms and occur when someone makes unauthorized modifications to code or data, attacking its integrity. Alteration attacks have a range of consequences such as altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. For example, students are changing grades, employees are altering or deleting corporate data as well as hackers changing social networking accounts and posting statuses on victim's behalf. Many politicians like French President Nicolas Sarkozy whose Facebook page was hacked in 2011 are under website alteration attack. Alteration attacks can happen to anyone even the Government. In 1996 U.S. Central Intelligent Agency's website was altered by Swedish hacker and in 1998 The New York Times' website was hacked. Although people may feel helpless against these attacks, victims of sabotage have the law on their side. A person who knowingly, willfully and without authorization creates, alters or deletes any data, information, image, program, signal or sound contained in any computer, system or network which, if done on a written or printed document or instrument is guilty of forgery. In 2012, the IC3 (receives, develops, and refers criminal complaints of cybercrime) received and processed 289,874 complaints, averaging more than 24,000 complaints per month. Also, unverified losses reported to IC3 rose 8.3 percent over the previous year.

Security Software

Security software (also called as antivirus) is a program that runs alongside other programs on a computer to try and prevent viruses from penetrating into the system. If security software does not prevent the virus with its defensive properties, then it can detect a virus and detect the user. Most viruses can be removed by security software, but if there is one that cannot be removed, the software will “corner” the virus so that it cannot ruin any other areas in the computer system. Viruses are a big problem for every computer that uses the internet, no matter what type of activity is done on the internet. Viruses can be used for theft, corruption of data, destruction of data, or system failure. The way to get security software is to download it digitally or through a DVD-ROM. According to the Anti-Virus Software website, the top ten anti-virus softwares are the following, respectively: McAfee, BullGuard, Trend Micro, Kaspersky, Norton by Symantec, BitDefender, ESET, ZoneAlarm, ParetoLogic, and VIPRE. These softwares provide web browsing protection, protection against Phishing scams, and parental control in addition to the basic anti-virus features. The way to choose the best anti-virus software is to check out all of the details and features to determine what extra characteristics are really necessary and what price range is suitable for personal circumstances. When purchasing a new computer, you will, most likely, automatically be offered security software that comes with your computer. The computer software is usually has a free trial, so you will have to pay for it eventually.

If you do not want to use the suggested/trial security software, you do not have to. Remember that Windows 8 onwards includes its own built-in anti-virus called as Windows Defender which provides similar features and is free. It is automatically enabled if you do not install any other antivirus.

Online Theft and Fraud

Identity theft is when someone identity in order to gain access to their bank accounts and possibly rent apartments or take out loans in that persons name. They then use their credit cards to make purchases. It usually begins when someone gets the name, address, and social security of someone from thrown a discarded document, usually mail. They can also get people’s information form the Internet. Identity theft is typically grouped into two subcategories. One is true name identity theft and that is when the thief uses another person’s information to open new accounts. The other kind is account takeover, which is when the thief uses

Figure 11-Credit Cards

someone else’s personal information to gain access to their existing accounts. There are different techniques such as skimming and social engineering.

- Skimming is when the thief uses a device that reads and stores credit and debit card numbers and stores them for later retrieval by the thief.
- Social engineering is when you pretend to work at a place (say at a telecommunication company or bank) and ask people for their information.
- Thieves rummage through garbage, trash in business, public dumps to get what they are looking which is someone’s personal information.

Some good indicators that your account identity has been stolen are if there are withdrawals that you can’t explain, not getting bills in the mail, refused checks, IRS contacting you, bills received that you are not aware of, and if your health plan will not cover you. All of these are big indicators that your identity has been stolen. It is important to be aware of bank transactions to be cautious of these thieves. There are certain types of Identity theft as well. Tax related would be one of them. If a Social Security number is stolen that can be used to get a tax refund or job. If you get paid by someone you do not know or find more than one tax return those would be big indicators that someone stole from you. Contacting the right people immediately would be the first thing to do in any situation dealing with identity theft. The IRS can help if a Social Security number has been stolen and they can protect the account. Children can also have their Social Security number stolen so it is important to keep that information private and on file.

Phishing

Phishing is when a thief sends out an e-mail that looks like it is from a legitimate site and then they steal your information. They are typically sent to a large group of people and they include an urgent message. It usually says that they need to update their banking information or something to that affect. Phishing attempts can occur anywhere, including Twitter, MySpace, or Ebay. Something that is becoming more targeted is spear phishing. Spear phishing e-mails are personalized. It is often targeted to social media sites because it is easier to find personal information on people.

Figure 12-twitter logo

Pharming, Drive-by Pharming, and Online Auction Fraud

Many people today are victims of identity theft. Another type of fraud or scam is called **Pharming**. Pharming is usually a fraudulent domain name intended to redirect a website’s traffic to another “trick” website. Pharming can be conducted either by changing the hosts file on a victim’s computer, or by the exploitation of a vulnerability in DNS server software. Sometimes this happens via email. The hacker gets ahold of the user’s email address and sends the code or website to the specific user. Once the user receives and opens the email, the hacker can receive the user’s information. Pharming usually happens most often with DNS servers at a company with a common and well-known Web site. The hacker can change IP addresses intended for the company URL. Then the company URL is routed to the “poisoned” URL, which then takes over the Web server. This method of pharming is useful to the hacker because the “poisoned” Web site is usually made to look exactly like the company Web site. Once the user logs in, the hacker captures the username and password for the first time. The user receives a login message error and is then returned to the original company Web site.

Drive-by Pharming is a little more recent. This method is used by logging into the user’s personal routers by using a common password that a script within a website can run. When it is accessed, the information on the router can be modified to suite the hacker.

Online auction fraud happens when a payment online goes to the seller, but the item is never delivered. For instance, if a buyer wants to make a bid online and buy tickets to a show or a concert, the buyer pays the seller for the tickets, and the seller never sends them. Many people are scammed each year and need to be careful with who they are trusting over the Internet.

Ransomware

Ransomware are programs that are designed to encrypt a user's PC and demand payment for the access of the files. Often these come into the user's PC through means described earlier in this article. The user will be forced to pay the ransom demanded by the program author (generally) though a virtual currency like Bitcoin which makes it hard for police to track the criminal.

Unfortunately the hopes of recovery in such cases are slim; not for many ransomwares have a free decryptor been released. Bleeping Computer is the best place to go for help if you have been infected by one.

The problem is especially acute for corporates: many have paid over $50,000 to restore vital information affected by the ransomware. The best way to protect against ransomwares is to take frequent backups; that way, if you do get infected, you can easily restore from your backups.

Protecting Against Online Theft and Fraud

Protecting Against Identity Theft

The key to internet safety is always being self aware.

Just as the Internet is always evolving for good, there are also constantly scheming e-criminals hoping to take advantage of those who aren't careful with their online identities. Identity Theft is one of the scariest things that can happen to a person, especially if they don't have a strong friend or family base to help convince the proper authorities of their true identity. There is not one universal way to protect yourself from identity theft; instead, there are a number of steps you should take to keep yourself fully protected. The first thing you can do is be responsible with your bank accounts and credit cards. If you're checking your balance every day, you will be quick to see if there are any suspicious discrepancies occurring. It is essential to download your bank's mobile application, so you can get alerts on all of your transactions. The next important step to protect against identity theft seems simple but can be easily overlooked: do not give out your personal information on the internet. This includes phone numbers, addresses, or anything else that hackers could potentially trace back to something you hold valuable. Some individuals can be targeted by thieves through fake emails and text messages who urge them to give up their information. You can protect yourself from identity theft is being wary of your mail. It is very easy for an e-criminal to send you a destructive link in an email that looks like it came from one of your friends, where one small click will lead you into a world of pain. Just follow these few rules and you will be doing fine online. One of the most easiest ways to protect yourself is to create a long, strong password. Creating a difficult password will prevent thieves from hacking into your personal information.

Avoiding Phishing E-mails

Most e-mail programs will automatically disable links in e-mail messages identified as questionable.

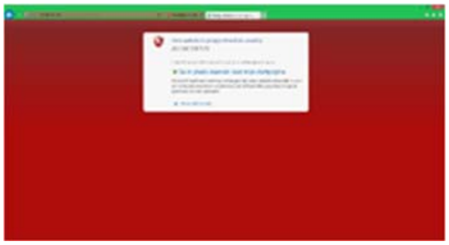


Figure 13-Phishing Emails

Due to the advantage taken of today's improving technology, phishing has emerged as one of the most damaging forms of identity theft. Using very convincing and persistent language, e-criminals are able to trick millions of users into revealing confidential information over the Internet. As mentioned earlier, to lure people in to clicking an attached link, e-criminals tend to steal the identity of a legitimate and well-known company to write a very "important-sounding" e-mail, solely for the purpose of tricking the reader into thinking the contents of the e-mail really are significant. Nonetheless, however urgent the e-mail may seem, it is actually designed to steal your money! A typical phishing e-mail will usually consist of: spelling errors, links, threats to make the content seem urgent, and a popular company name to sound reliable. If examined carefully, some phishing expeditions may be fairly easy to spot, due to the poor spelling and grammar used, making it obvious that the message is not from a *legitimate* company. The link in the e-mail is used by the cybercriminals to install malicious software on your computer, ultimately enabling them to steal personal and sensitive information off of your computer. The e-mail could also even ask you to provide personal information, such as your bank account number, credit card number, or your Social Security Number; this should automatically be a red flag for the recipients because an authentic business would never request such information in any way other than in person. Therefore, if one is alert and careful about the content they receive in an e-mail, they can ultimately help protect their identity and their money, even if the e-mail seemed rather urgent.

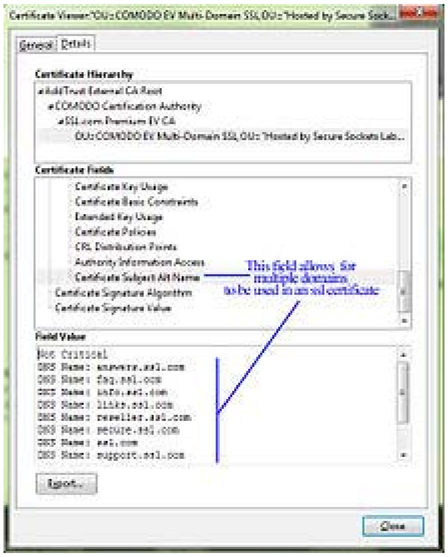
Don't take the bait. Protect your financial information.
We need to verify your credit card number.

Figure 14-Phish

The act of a phisher setting up a Web site that appears to look like the legitimate business is an act called Web site spoofing. Phishing emails can be sent to a wide group of people or can be personalized and sent to one person. This more targeted trend of phishing is called spear phishing because it targets a specific individual. A phisher may gather personal information from a networking site and send an email to a particular individual in order to convince the recipient that personal login information or account information is needed. Phishers may also do something that is called typosquatting, which is setting up spoofed Websites with addresses slightly different from legitimate sites in the hopes that a user would supply login information via the spoofed site when they arrive. Another form of online threats include pharming. Pharming is another type of scam that uses spoofing. With pharming, the criminal reroutes traffic intended for a commonly used Web site to a spoofed Web site set up by the pharmer. The pharmer makes changes to the DNS server. The DNS server is the computer that translates URLs in to the needed IP addresses to display the Web page corresponding to a URL. A pharmer will usually target company DNS servers. Lastly, online action fraud can also be a concern for Internet users. This threat occurs when an online auction buyer pays for merchandise that never is delivered.

Digital Certificates

One way of protecting yourself from online thefts or frauds is by looking for a digital certificate when browsing the Web or looking through e-mails. A digital certificate is granted by Certificate Authorities, which prove to the person that the website they are accessing is secure. A digital certificate binds the owner of a website to a specific pair of electronic keys, one being public and the other private. This allows the owner of the certificate to encrypt their files and e-mails and provides the user with the knowledge that their actually is an owner to the website that they are on. A digital certificate tracks who sends an email and who receives an email. This can protect users from giving away their credit card numbers to unprotected websites that try to scam people of their money. A digital certificate can either be an SSL or EV (Extended Version) SSL. The SSL digital certificate is the ordinary certificate that still requires an application and verification process while the EV SSL requires a more in-depth verification process. For users, an EV SSL digital certificate indicates that it is more secure than just an SSL digital certificate, while both of them are considered to be safe. This can be represented by the fact that when you enter an EV SSL webpage, the Address bar turns green and for an SSL webpage it doesn't change color at all. A digital certificate, in general, is definitely a good security advisor for users on the Internet.



Certificate Viewer:"OU=COMODO EV Multi-Domain SSL,OU="Hosted by Secure Sock...

Certificate Hierarchy

- AddTrust External CA Root
  - COMODO Certification Authority
    - SSL.com Premium EV CA
      - OU=COMODO EV Multi-Domain SSL,OU="Hosted by Secure Sockets Lab...

Certificate Fields

- Certificate Key Usage
- Certificate Basic Constraints
- Extended Key Usage
- Certificate Policies
- CRL Distribution Points
- Authority Information Access
- Certificate Subject Alt Name
- Certificate Signature Algorithm
- Certificate Signature Value

Field Value

```
Not Critical
DNS Name: answers.ssl.com
DNS Name: faq.ssl.com
DNS Name: info.ssl.com
DNS Name: links.ssl.com
DNS Name: reseller.ssl.com
DNS Name: secure.ssl.com
DNS Name: ssl.com
DNS Name: support.ssl.com
```

General
Details
This field allows for multiple domains to be used in an ssl certificate
Export...
Close

Figure 15 - Digital certificates

The Safety of Using PayPal

Figure 16-Credit Cards

Internet users have to be very cautious of the information they put on the internet. PayPal seems to be a popular e-commerce business that many people use and willing give their private information to. Is this payment processor to be trusted? PayPal makes the lives of everyday internet consumers much easier. Its secure server stores your credit card information so payment over the internet is more efficient. Not much effort has to be put in by the individuals that use this payment processor. Other accounts require a vast amount of paper work to be signed beforehand. One drawback to using PayPal is that there is a long list of rules the users must abide by, and if a user breaks any of these rules their money could be locked for up to six months while under investigation. An interesting feature that was added to PayPal in 2006 was an additional security option. Instead of only entering a login id and password, PayPal users can choose to type a six-digit number code in as well. This lowers the risk of malware bots trying to hack into the account. There is a fee associated with this added security measure. Users might be discouraged to protect their accounts because of this additional fee. They should still take caution when it comes to entering personal information into PayPal. Users should also be cautious when placing orders online using PayPal because they're at a greater risk for their credit card information to be stolen.

The Safety of Digitally Storing Cards

Figure 17-Apple Pay

New forms of paying have appeared or rather a new way of paying thanks to companies like Google and Apple. Apple Pay and Android Pay are ways of paying wherein the user puts their credit cards or debit cards into their phones and can then use their phones or smartwatches to use their credit cards instead of bringing the physical cards with them. You can also use in app purchases by using your fingerprint on the latest Apple phone. With the phone's it uses biometrics to make sure the owner is using Apple Pay and with smartwatches they use passcodes. But the real question is this new way of paying secure? Apple claims that it is so. In fact, they claim that it is actually more secure and that they will never upload the details on your cards to their servers. In fact, if your smartphone or smartwatch was ever stolen, you have the ability to revoke the information on your smartphone or smartwatch. Also Apple creates a Unique Device Account Number in order to protect your purchases when making transactions. However, there are those who do believe that this may not be safe. The best way to not have to deal with the risk is to not use Apple Pay. There are also applications like Snapchat and Venmo in which you can send money using your credit card information. This is a fast way to receive money but can be risky. A thief can login to your account and steal your information. All in all, it is not safe to store any personal information

Basic Home Network Security

Figure 18-Wireless Router

Many people have wireless networks in their homes, but they may not necessarily keep these networks as safe as they can or should. If somebody else accesses your network without your knowledge or consent, then they may do things on that network that you do not desire, they can use up your allotted data usage, and, most concerning, they may be able to get your personal information. Therefore, people with wireless home networks should take precautions to keep them secure. First, networks should always have some sort of a password to keep them safe; a network should never, *ever* be left unsecured, because then absolutely anybody within range can go on it. Typing any password at all is better than nothing, since it'll deter people from mooching, but—as is always the case—it is not wise to go with a predictable password such as the network name, 'password', 'Internet', etc. Something that is meaningless on the surface level but has a deeper meaning for you is a better way to go; for example, the first letters of words in an individual phrase that only you will remember. Also, to add yet another layer of security, you can make it so that your network is not available to other users by default but instead they must know the network name; this way, for a hacker to gain access, they would have to guess both the ID of the network *and* the password, which is highly unlikely. With these incredibly simple steps, one can make their network incredibly secure compared to one that has absolutely no measures preventing access from anybody within a certain physical proximity.

Personal Safety

Cyber-bullying

This is a new way of bullying especially for the amount of social networks and how it has influenced our society today. Unfortunately, it happens 24 hours of the day and anything can be posted or distributed anonymously in which it could be difficult to track where the bullying is coming from. And as everyone is informed these days, once something is on the internet, there is no way to permanently delete the comment after it has been sent. It happens when individuals are bullied through electronic technology. For example, you can cyber bully over text message, emails, rumors send through any type of social networks. There's no way to prevent an individual from making a comment that could be known as the start of cyber bullying, but simply ignoring or reporting the comment to either a parent, friend or any type of guidance person could benefit you most in not having the bullying continue. To elaborate, you can simply block the individual that had started the commenting and keep any type of evidence of the bullying for future documents in case it gets worse. A last important note is to recognize the signs of attitudes if a student were to be cyber bullied; some reactions are abusing drugs and alcohol, skip school, receive poor grades and have lower self-esteem.

Activity: Delete Cyberbullying - Preventing Cyberbullying

Cyberstalking

Cyberstalking is the use of the internet, email, or other electronic communications to stalk another person. This occurs when there is a continuous pattern of malicious or threatening activity from an individual. Cyberstalking is considered the most dangerous form of harassment over the internet and is punishable by law. Depending on the state, punishments can range from misdemeanors to felonies. Victims of cyberstalking can be targeted by strangers online who find personal information somewhere on the web or by more personal colleagues or individuals who know the person they are targeting well. Unfortunately, cyberstalking can move beyond the computer and become a problem in the real world if the stalker discovers or knows how to find the individual personally. This is a very serious issue and should be brought to law enforcement agencies or even the FBI. It is important to not give away any personal information that can be used to stalk you and to ensure that you trust anyone or anywhere that you may be giving personal information to online. The best solution to stop cyberstalking is to not respond at all or to change the information on whatever resource the cyber stalker is using to harass you.

Protecting Against Cyberbullying, Cyberstalking, and Other Personal Safety Concerns

Safety Tips

While it may seem unnecessary to state, the Internet is accessed by not only those with good intentions but also those who can pose a threat in a variety of ways. It is important to be aware of this fact because it is quite easy to forget how vast of an entity the Internet is and countless masses who use it daily. This makes for the task of safeguarding information from those who mean harm an important responsibility. Some of the ways one can prevent cyberbullying, cyberstalking and other issues are by using names that are gender-neutral. This hides the identity of the user, and this is important for female users because unfortunately they are more likely to be targets compared to male users. Also, one should not give phone numbers, addresses and other personal information to strangers for obvious reasons. A way to prevent cyber bullying is to not be a cyber bully yourself. Bullying people online is not only unethical but it will increase the number of users targeting you.

Safety Tips for Children and Teens

Monitoring how children and teenagers use the Internet through the computer, smartphone, game console, etc. is the most important step in protecting them. It is recommended to place certain restrictions on how they use the Internet so that they do not access certain sites that might make them more susceptible to dangerous individuals or certain sites (e.g. adult sites). There are certain softwares parents can download to monitor what their children are doing online. There are also softwares to block innapropriate websites which is more common to find in children's schools. It is also important for older teens to understand the potential ramifications, including not only personal but also legal issues, that can arise from sending explicit messages or pictures via text messaging. Although teenagers may think that they have deleted text message or a picture, someone can still obtain the image.

Using Your Computer In A Safe Way

One of the best ways to stay safe online is to make sure you have your computers operating system and antivirus / anti-malware software update and set scanning schedules however the most important part of protection is **user awareness**. A recent blog post from Antivirus Talk details a list of good computer rules. Remember the majority of the time the user has allowed a virus onto the system.

- Always run antivirus software (at least the built-in Windows Defender)
- Don’t go To Websites You don’t Know
- Don’t open Emails if you don’t know where they are from
- Use A different password for everything
- Keep your system up-to-date
- Don’t install unknown programs
- Don't send/give out your passwords
- Lock your computer when you are not by it in a public area
- Don't leave your computer in your car or lying around

By just following these rules you have the best chance of a safe journey online.

Network and Internet Security Legislation

New legislation is frequently introduced to address new types of computer crimes. Unfortunately, it's difficult to keep pace with the rate at which the technology changes. Along with this, there are both domestic and international jurisdictional issues because many computer crimes affect people in geographical areas other than one in which the computer criminal is located. Regardless, computer crime legislation continues to be proposed and computer crimes are being prosecuted. Some of the most important and impactful laws follow: Computer Fraud and Abuse Act of 1984- Makes it a crime to break into computers owned by the federal government. Identity Theft and Assumption Deterrence Act of 1998- Makes it a federal crime to knowingly use someone else's means of identification, Social Security number, or credit card, to commit any unlawful activity. Homeland Security Act(2002)- Includes provisions to combat cyberterrorism. One of the most famous cases of a cyber crime happened quite recently, the criminals charged in 2013. Five cyber criminals were responsible for a hack that targeted companies more than $300 million. They did this by stealing usernames and passwords, personal identification information, credit card and debit card numbers

Figure 19-DC3 Seal

through secure computer networks. The criminals were sentenced up to 20 years in prison, depending on the amount stolen and involvement with the hacking group.

Review

Important Terms

1. **antivirus software**:]Software used to detect and eliminate computer viruses and other types of malware.
2. **biometric access system**: An access control system that uses one unique physical characteristic of an individual (such as a fingerprint, face, or voice) to authenticate that individual.
3. **bot**: A program/service that does tasks which would be tedious to do do manually. However, it can also be used for criminal activities, like for DDoS purposes.
4. **botnet**: A group of bots that are controlled by one individual.
5. **computer crime**: Any illegal act involving a computer.
6. **computer sabotage**: An act of malicious destruction to a computer or computer resource.
7. **computer virus**: A software program installed without the user's knowledge and designed to alter the way a computer operates or to cause harm to the computer system.
8. **computer worm**: A malicious program designed to spread rapidly to a large number of computers by sending copies of itself to other computers.
9. **cyberbullying**: Children or teenagers bullying other children or teenagers via the Internet.
10. **cyberstalking**: Repeated threats or harassing behavior between adults carried out via e-mail or another Internet communications method.
11. **denial of service (DDoS) attack**: An act of sabotage that attempts to flood a network server or a Web server with so much activity that it is unable to function.
12. **digital certificate**: A group of electronic data that can be used to verify the identity of a person or organization; includes a key pair that can be used for encryption and digital signatures.
13. **digital signature**: A unique digital code that can be attached to a file or an e-mail message to verify the identity of the sender and guarantee the file or message has not been changed since it was signed.
14. **dot con**: A fraud or scam carried out through the Internet.
15. **encryption**: A method of scrambling the contents of an e-mail message or a file to make it unreadable if an unauthorized user intercepts it.
16. **firewall**: A collection of hardware and/or software intended to protect a computer or computer network from unauthorized access.
17. **hacking**: Using a computer to break into another computer system. (I bet you need this for class.)
18. **identity theft**: Using someone else's identity to purchase goods or services, obtain new credit cards or bank loans, or otherwise illegally masquerade as that individual.

19. **malware**: Any type of malicious software.
20. **online auction fraud**: When an item purchased through an online auction is never delivered after payment, or the item is not as specified by the seller.
21. **password**: A secret combination of characters used to gain access to a computer, computer network, or other resource.
22. **pharming**: The use of spoofed domain names to obtain personal information in order to use that information in fraudulent activities.
23. **phishing**: The use of spoofed e-mail messages to gain credit card numbers and other personal data to be used for fraudulent purposes.
24. **possessed knowledge access system**: An access control system that uses information only the individual should know to identify that individual.
25. **possessed object access system**: An access control system that uses a physical object an individual has in his or her possession to identify that individual.
26. **private key encryption**: A type of encryption that uses a single key to encrypt and decrypt the file or message.
27. **public key encryption**: A type of encryption that uses key pairs to encrypt and decrypt the file or message.
28. **secure Web page**: A Web page that uses encryption to protect information transmitted via that Web page.
29. **security software**: Software, typically a suite of programs, used to protect your computer against a variety of threats.
30. **spear phishing**: A personalized phishing scheme targeted at an individual.
31. **Trojan horse**: A malicious program that masquerades as something else.
32. **two-factor authentication**: Using two different methods to authenticate a user.
33. **unauthorized access**: Gaining access to a computer, network, file, or other resource without permission.
34. **unauthorized use**": Using a computer resource for unapproved activities.
35. **virtual private network (VPN)**: A private, secure path over the Internet that provides authorized users a secure means of accessing a private network via the Internet.
36. **war driving**: Driving around an area with a Wi-Fi-enabled computer or mobile device to find a Wi-Fi network to access and use without authorization.
37. **Wi-Fi piggybacking**: Accessing an unsecured Wi-Fi network from your current location without authorization.