Introduction

"identity" is licensed under CC0 1.0

Information security refers to the protection of computers and other digital devices, information systems, data, and information against unauthorized access, use, manipulation, or destruction.

Information security is a growing concern as increasing amounts of important and private information are stored digitally on systems connected to public networks and wireless private networks. From bank account and credit account access codes, to personal medical records, to secret business strategies, to national defense initiatives, to email sent to a friend, people trust information systems to keep their most valuable and secret information safe and secure. But can information systems be trusted?

To understand how much the world is impacted by computer security issues, all one has to do is access the daily news. Consider these recent headline stories:

- Massive Cyberattack Triggers Recalls and Serious IoT Concerns
- Yahoo says 500 million accounts stolen
- FBI Warns of Possible State Election-System Hacks
- Major U.S. Hotels Hit by Point-of-Sale System Breach
- Quadrooter Bug Affects 900 Million Android Devices
- Study Finds Ransomware Hits Almost 40 Percent of Enterprises
- HummingBad Malware Infects 85 Million Android Devices
- Millions of Health Records Appear for Sale on Dark Web
- LinkedIn Passwords from 117M Accounts Hacked and Up for Sale
- Google Says Ad Injectors Infect Millions of Users
- U.S. Government Suffers Massive Cyberattack
- Russians Reportedly Hacked White House Computers Last Year
- IRS Hacked, Info on 100,000 Americans Stolen
- Adult Dating Site Hack Exposes Personal Data of Millions
- Massive Security Flaw Puts 600 Million Samsung Smartphones at Risk
- Hackers stole 21.5 million Social Security Numbers in government breach
- Fiat Chrysler recalls 1.4 million cars over remote hack vulnerability
- Over 225,000 Apple iPhone Accounts Hacked by New Malware

Cyberattacks of one kind or another are occurring continuously on the Internet, causing concern over information at every level: personal, business, and government. Consider the information of concern to you that is stored on your computer, on web servers, and in the systems of every business and organization with which you have interacted. What damage could be inflicted on you if that information was stolen, altered, or destroyed? What types of businesses are at the biggest risk of cyberattack? Why? How do cyberattacks against businesses impact you and the country? What should the government do to protect its citizens from cyberattacks? Should the government force businesses to adopt tighter security measures? Who should incur the costs of increased national cybersecurity?

Corporate and government networks and home computers are under attack, and the Internet is the battlefield. Automated criminal systems probe Internet-connected computers owned by individuals, businesses, and governments, continuously seeking security holes that might allow a hacker to infiltrate the system. The casualties of this war include your privacy, information, property, and money. Crimes that take place online, called cyber crimes, can impact personal information, corporate information, and governmental information. Valuable information and many forms of intellectual property can be compromised or stolen. Computer systems, automated industrial systems, and critical national infrastructure, such as the power grid, can be attacked and derailed. An increasing percentage of criminal activity now takes place online.

Cyber crime takes place on many levels. Pirates illegally download copyright-protected music, movies, and software. Plagiarists copy portions of online articles and claim ownership of others' ideas. Criminal hackers illegally access computer systems to steal information, to cause problems or embarrassment for a business or organization, or to utilize hacked network resources for criminal activity. Cyber spies take part in cyberwarfare to steal government secrets or to disrupt a nation's critical infrastructure. These represent examples of intentional crimes. Others may be unintentional. Sometimes, damage to computer systems and information occur through negligence. For example, a user may unintentionally delete files, enter incorrect and misleading data, lose archived data stored on removable media, or fail to take safety precautions like backing up data.

Total information security refers to securing all components of the global digital information infrastructure from mobile phones to PCs to automobiles, to smart home appliances, to business and government networks, to Internet routers and wireless networks. The figure shows the layers of information security and illustrates how you, the computer user, are at the heart of information security. Your recognition of security risks and the actions you take to secure the systems with which you interact are the most important components of total information security. As a computer user, you must learn about security risks at three levels: the machine level, the network level (including wireless networks), and the Internet level. As you move from the machine level toward the Internet level, you face increasing exposure and risk.

When it comes to state-affiliated cyberespionage, China and Russia have been blamed for many attacks against the U.S. but both deny all charges. The nature of cyberattacks makes it difficult to trace an attack to its exact origin. President Obama signed a cybersecurity executive order to protect the country's critical and vulnerable infrastructure. A new branch of the Pentagon was created to focus on cyberwarfare. A legal review on the use of America's growing arsenal of cyber weapons concluded that the president has the power to order a preemptive cyber strike if the United States detects credible evidence of a major digital attack looming from abroad. Clearly things are heating up in what has been called cyber cold wars with China and Russia.

Meanwhile the international community is working to create rules for cyberwarfare engagement similar to the Geneva Convention, which governs traditional warfare. The NATO Cooperative Cyber Defense Center of Excellence has created a set of rules named the Tallinn Manual to protect civilian targets such as hospitals, dams, and nuclear power stations from state-sponsored cyberattacks.

What steps do you think world powers should take to rein in damaging cyberattacks and prevent global cyberwarfare? How can the U.S. better protect its critical infrastructure?

Lesson 16.1: Data Loss Prevention

Lesson 16.1 Introduction

"phone security" by stockcatalog is licensed under CC BY 2.0

Machine-level security refers to actions taken to protect information on a computer that may or may not be connected to a computer network or the Internet.

Information security is implemented at multiple levels: the individual machine level, the computer network level, and the Internet level. This section examines security from the perspective of the individual machine and discusses security precautions for personal computers that may or may not be connected to a network or the Internet. While it may not be practical to lock your computer in a vault to protect your data, there are methods available to provide nearly the same level of protection. By learning how to protect stand-alone PCs, you also learn about the first line of defense for the networks to which those PCs may be connected.

The greatest threat to information on a computer is through network connections. However, information on computers not connected to a network is also at risk from people who might access that computer physically rather than remotely. The only way to fully protect a computer is to eliminate access to the machine by anyone other than the owner. Many businesses take this approach by keeping important computer systems behind locked doors, accessible only to authorized users granted access with a card swipe. Other methods of protecting data on a machine include the use of passwords and encryption. Keeping backups is essential for protecting data in case all defenses fail.

Reading: Authentication

Authentication is a security process in which the identity of a person is verified.

Why This Matters

Deciding who should have access to information and who should not is the foundation of information security. There must also be a method of determining that persons attempting to access the data are who they claim to be. That is the purpose of authentication. There are several forms of authentication, some stronger than others. Implementing authentication properly is important in protecting computers and mobile devices.

Essential Information

Access to today’s PCs is typically guarded with a username and password. In security terms, this is called authentication, which confirms the identity of a user. The table below shows the three common forms of authentication:

Forms of Authentication

Form of Authentication	Description
Something you know	Information such as a password or personal identification number (PIN)
Something you have	An item such as a phone, computer, ID card, smart card, badge, keychain fob, or other item designed to be used to authorize access to secure areas and systems
Something about you	Unique physical characteristics such as fingerprints, retinal patterns, and facial features that can be scanned and used for authentication

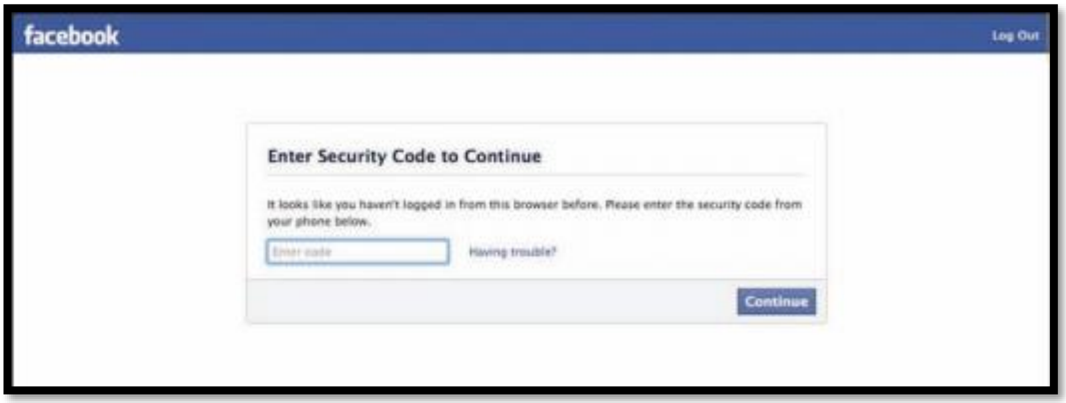
A username identifies a user to the computer system. Varying levels of computer access and environmental preferences are associated with a username. Although usernames can act as a form of “something you know” authentication, they are not very strong because they are typically not kept secret. Usernames can often be accessed from email addresses. A password is a combination of characters known only to the user that is used for authentication when gaining access to systems. Passwords can be an effective form of authentication if they are difficult to guess, kept confidential, and changed regularly. However, passwords are considered a weak form of authentication because they can be guessed by others to access systems without your knowledge. It is important to create passwords that are strong—that is, difficult, if not impossible, to guess. For example, johnnyb and nycjohnny would be weak passwords for John Baily from New York City. The password 92Tpo5#cCw is very strong but nearly impossible to remember. The password nyKOOLB@Y might make a good password for John, since it is strong and is also easy to remember.

It is equally important to use different passwords for different accounts and to change your passwords regularly, at least twice a year. This will thwart hackers who may already be accessing your account without your knowledge.

The large number of passwords most users have to remember is becoming problematic. Password manager software is one way to deal with it. Password manager software like 1Password, LastPass, and DashLane securely stores all of your online passwords and automatically enters them when needed. The only password the user needs to remember is the password for the password manager. Most web browsers also have the capacity to remember and auto-enter passwords, but don't have the full functionality of password manager software. Many companies, including Google, are developing new methods of authentication that will no longer require passwords.

A number of physical devices are used in corporations and organizations to identify users and provide access to restricted areas and computer systems. These technologies make use of the "something you have" form of authentication. Sometimes, they are combined with a password to increase the security level. The most popular of these devices are ID cards and tokens that sometimes take the form of a keychain fob. ID cards may contain forms of identification in a magnetic strip or in a microchip, as is found in a smart card. A token is an object like a smart card or key fob that contains a microchip that stores ID information. The user holds the token against a reader device to gain access to a location or information systems.

A token can also take electronic form on a computer. For example, a bank may require its members to install a special bookmark in their browsers to use when logging into their online bank accounts. The bookmark is used as a token to identify the computer as an approved device for a member's account. If the account is accessed from a different computer, the user is required to enter more detailed information to authenticate his or her identity.



Enter Security Code to Continue

It looks like you haven't logged in from this browser before. Please enter the security code from your phone below.

Courtesy of Facebook. Fair Use

Facebook, Google, PayPal, and other online services offer a higher level of security using 2-step verification. 2-step verification requires a combination of a password with a verification code sent to the user's phone. Typically, the 2-step verification is only required if the account is accessed from an unrecognized computer. These systems also use digital tokens to identify and recognize approved computers. They may notify a user by email when someone attempts to access the user's account from an unrecognized computer.

Biometrics is the science and technology of authentication by scanning and measuring a person’s unique physical features (“something about you”). Fingerprints, facial characteristics, retinal patterns, and voice patterns are commonly used in biometrics. A fingerprint scan uses the pattern of a fingerprint to authenticate a user. Fingerprint scans are an increasingly common method of authentication for access to secure areas, for validating credit card purchases, and for logging onto or unlocking devices.

Apple Inc. Fair Use

Facial pattern recognition is a form of biometrics that uses a mathematical technique to measure the distances between points on the face. Taking a weighted sum of these measurements, software can quickly scan a database of known faces and come up with a match if one exists. Law enforcement agencies and airport security agents use facial pattern recognition software in efforts to catch criminals and terrorists. Facial pattern recognition is also being used to secure PCs and mobile devices that include cameras. Another form of biometrics, retinal scanning, analyzes the pattern of blood vessels at the back of the eye (see figure). As the field of biometrics expands, other physical characteristics, such as speaking patterns, are also being explored for use in authentication.

Reading: Encryption

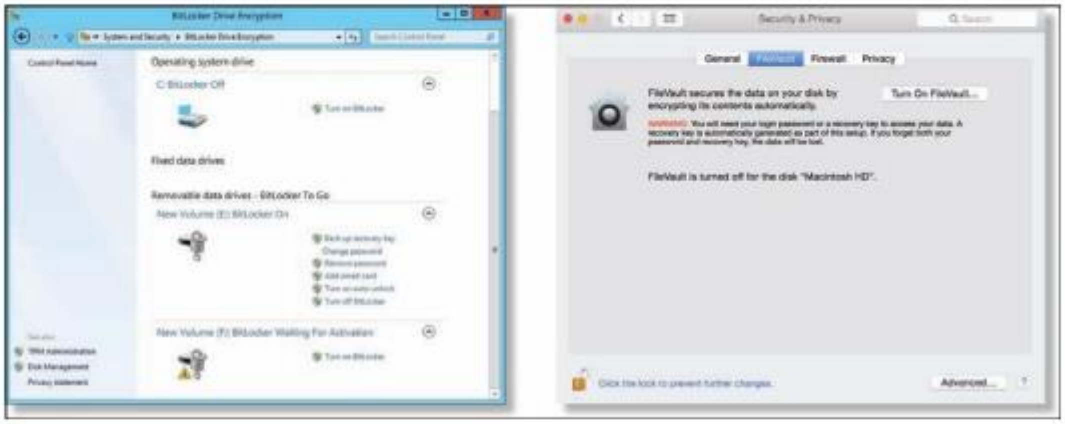
Encryption is a security technique that uses high-level mathematical functions and computer algorithms to encode data so that it is unintelligible to all but the sender and recipient.

Why This Matters

With the increase in mobile computing, the possibility of losing a computer or having it stolen is very real. Data can also be stolen from computers by hackers who break through network security. Sometimes, the data stored on a mobile device is more valuable than the device itself. If that data is encrypted, it will be unintelligible to hackers and thieves who have stolen it. Data can also be stolen while it is in transit over a computer network. An increasing number of users have become concerned about government spying on telecom networks and mobile phones. Encryption techniques help safeguard data that is stored or traveling over a network.

Essential Information

Today’s PCs include security tools that can encrypt files stored on disks and flash drives. This is useful in situations where the information you are storing is confidential or valuable, and there is a possibility that your computer can be accessed by others, lost, or stolen.



C: BitLocker Off

New Volume (E:) BitLocker On

New Volume (F:) BitLocker Waiting For Activation

FileVault secures the data on your disk by encrypting its contents automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned off for the disk "Macintosh HD".

Apple Inc and Microsoft Corporation. Fair Use

Files can be encrypted “on the fly” as they are being saved and decrypted as they are opened. To open encrypted files, you must enter a password. Encryption and decryption (the process of decoding encrypted data) tends to slow down a computer slightly when opening and saving files, so encryption is not typically turned on by default. Instead, the user manually selects the files or folders that contain confidential information and marks them for encryption.

Mac OS uses the FileVault system for file encryption. FileVault uses the latest U.S. government security standard, AES-128 encryption, to safeguard confidential documents. Microsoft Windows uses BitLocker Drive Encryption, which is machine-level data encryption that can secure the entire hard drive and protect the data even if the PC is stolen. Some Windows PCs include an embedded security subsystem that stores passwords and encryption keys on a dedicated security chip on the motherboard. Storing security information in a dedicated chip rather than in a file on the hard drive offers perhaps the strongest method of personal computer security.

In addition to protecting data on storage media, encryption is also used to protect data that travels over a network. By sharing an encryption key, the sender and receiver can send encrypted data over a network and the Internet. Encryption is particularly important for wireless networks, where data can be easily intercepted. Several wireless encryption protocols exist. Wi-Fi Protected Access (WPA) is a common encryption protocol. WPA2 is the most recent and most secure version. Even with encryption, it is dangerous to send passwords and other private information over public wireless networks.

When sending confidential data over the web, users are wise to make sure the browser is using a secure connection, which can be indicated by https:// in the address bar, a green color in the address bar, and a closed lock icon in the address bar or at the bottom of the browser screen. HTTPS is a secure form of HTTP that encrypts the data submitted by users, such as passwords, credit card numbers, and other data submitted using forms on webpages.

Due to the revelations about government-surveillance-provided leaked NSA documents, encryption has become more important to many U.S. citizens. Many online services, including email, now apply encryption by default. The iPhone and Android phones provide options for encrypting data stored on the phone. If the phone is stolen, the data cannot be accessed without the owner’s PIN code. This caused controversy in 2016 when the FBI asked Apple to retrieve encrypted data from a terrorist’s iPhone, and Apple refused. Ultimately, the FBI discovered how to hack the iPhone to get at the data.

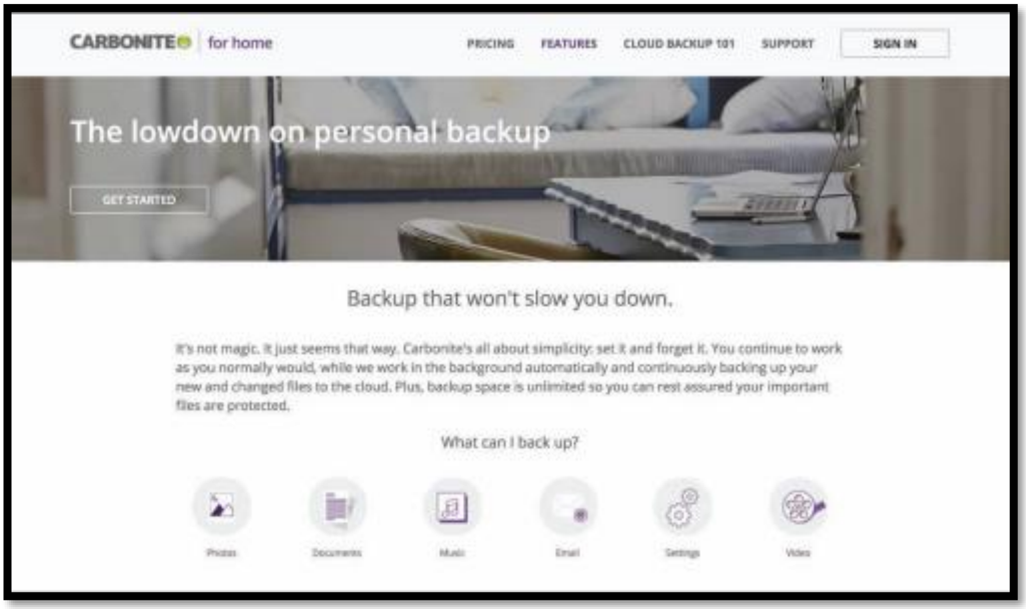
Encryption and other forms of information security, used alone, do not safeguard data 100 percent. Maximum information security is accomplished through the implementation of all computer security tools combined with safe computing practices.

Reading: Data Backup

Data backup is a process in which copies of important computer files are stored in a safe place to guard against data loss.

Why This Matters

Data may be lost due to hardware failure, human error, software corruption, hackers, malware, or natural disasters. The only method that provides protection for data against all of these disasters is to back it up! Still, many computer users do not have a regular backup procedure in place. Today's backup technologies make backing up important data and system files easier than ever.



The lowdown on personal backup

Backup that won't slow you down.

It's not magic. It just seems that way. Carbonite's all about simplicity: set it and forget it. You continue to work as you normally would, while we work in the background automatically and continuously backing up your new and changed files to the cloud. Plus, backup space is unlimited so you can rest assured your important files are protected.

What can I back up?

Carbonite. Fair Use

Essential Information

When you purchase a new computer, it typically comes with a system recovery disk. If operating system files become corrupted, either due to failure of the hard drive or a virus, your computer may simply not start. A system recovery disk, sometimes called a rescue disk, is used to regain access to a computer that has lost its ability to boot normally. The disk includes utility software that can be used to attempt to repair the damaged system files, recover data files, or prepare the computer for a reinstall of the operating system. Operating systems typically provide a way for users to create a system recovery disk if one is not provided by the manufacturer.

Windows PC users who find their system damaged but can start the computer can benefit from the System Restore (up to Windows 10) or File History (Windows 10) utilities. These utilities allow you to restore files that have been lost or corrupted, or to roll back the operating system to a time when the computer was without problems. Apple Mac OS provides a similar tool called Time Machine, which backs up not only system files but also data files.

In addition to backing up important system files, it is important for computer users to back up data files. Businesses typically have regular backup procedures to back up corporate data to disk drives, tape, or online storage media. Individuals typically back up their personal data files to an external drive or remote online storage.

Operating systems usually provide a backup utility for data files. Typical backup software collects the files you wish to back up into a compressed file called an archive. Some backup software provides the ability to encrypt the archive and password-protect it. Backup software typically provides the following options:

Select the files and folders you wish to back up.

Choose the location to store the archive file.

Choose whether to back up all files (a full backup), or just those that have changed since the last backup (an incremental backup).

Most backup utilities also provide a scheduling option that allows you to automatically run backup routines at specified dates and times.

Rather than creating an archive, some users prefer to create an exact copy of their data files, using a technique called mirroring. Some software provides real-time mirroring for home users. As the user saves a file, a second copy is saved to a drive connected to the home network. Businesses sometimes use a technology called redundant array of independent disks (RAID) to keep a mirror copy of all data on the system. Should the primary system fail, the RAID kicks in, allowing uninterrupted operation.

Internet-based backup services are becoming popular as more users have high-speed Internet connections. Services like Remote Data Backups, Dropbox, Mozy, SugarSync, and Carbonite provide automated backup of data continuously or periodically over an Internet connection for a monthly or yearly fee. Files that are backed up to the cloud may be accessed from any computer by the owner or by individuals the owner chooses to share the files with. Some of these services allow users to make folders or files accessible to the general public—a useful feature for sharing photos on the web. An important feature of an online backup service is that it allows you to back up your data off-site in a different location from your computer. It is smart to keep backups off-site, as keeping them on-site may expose them to the same destructive forces that wipe out the original data: fire, flood, a power surge, and so on.

With the advent of cloud computing, users are storing increasing amounts of data on Internet servers. Email, calendars, documents, photos, and other data are being saved in services provided by Google, Amazon, Microsoft, Flickr, Facebook, and other cloud apps. Google, Amazon, Microsoft, and Apple offer remote data storage for backing up files, sharing files, and accessing data from any Internet-connected computer. Microsoft offers free online storage and sharing of Microsoft Office documents with OneDrive while Apple's iCloud provides backup options and the ability to share apps and data across Apple devices.

As data moves to the cloud, the responsibility for backing it up falls on the shoulders of the service providers. Before trusting a service provider to back up your data, make sure to read the disclaimers. The providers do not typically ensure against data loss. Ultimately, it falls to the users to keep backup copies of everything for 100 percent assurance.

Lesson 16.2: Network Security

Lesson 16.2 Introduction

Network security is concerned with addressing vulnerabilities and threats in computer networks that may or may not be connected to the Internet.

When a computer becomes connected to a network, security risks increase a hundredfold. If the network happens to be a wireless network, it is all the more vulnerable. If the network is connected to the Internet, risks increase a million times that of a stand-alone computer. In fact, for information of highest security, government agencies use computers that are not connected to agency networks or the Internet. As long as there is a network connection, there is an increased risk of unauthorized access. The primary challenge in securing a computer network is keeping user data private and accessible only by authorized persons.

This lesson discusses threats, considerations, and security for computers connected to wired and wireless networks. A later section on Internet security deals specifically with security measures for computers connected to the Internet.

Networked computers may be in a government agency; a large, medium-sized, or small business; a college campus or campus housing; an apartment building; or a home. Whenever people share computing resources remotely over a network, a system administrator assumes the responsibility of establishing which resources should be accessible to each user. A system administrator may be a person or persons hired by a corporation to manage a large computer network, or it could be a person like you, managing a home network. The topics in this section discuss the threats posed to computer networks—both wired and wireless—and the tools available to system administrators to protect the network.

Reading: Permissions

Permissions, or file system permissions, refers to the specific access privileges afforded to each network user and each system resource in terms of which files, folders, and drives each user can read, write, and execute.

Why This Matters

A multiuser system is a computer system, such as a computer network, where multiple users share access to resources. When sharing resources, users are naturally concerned about the privacy and protection of their data files. System administrators are concerned with protecting the system from intentional and unintentional damage. If a corporation owns the network, corporate management is concerned about the security and privacy of corporate information. The network administrator can control which network resources—files, folders, drives, network connections, systems, and software—each user can access and edit, by defining specific permissions for each resource and user on the network.

Essential Information

Operating systems such as Microsoft Windows, Mac OS, and Linux provide methods for associating permissions with each user account and each system resource. As each user logs on to a computer connected to the network, the permission policies are applied, and the user can access only the resources defined by those policies.

To control user access to system resources such as files, folders, and disk drives, access policies must be defined for both the resources and the users. For example, a user may be restricted to accessing only files that he or she created. Files and folders on the system must carry information that identifies their creator. This is referred to as file ownership. Users are the owners of the files they create.

The system administrator is responsible for setting the access rights of users and for setting the permissions on system resources. The system administrator can also assign permissions to groups of users. Users have the power to set permissions for the files they own.

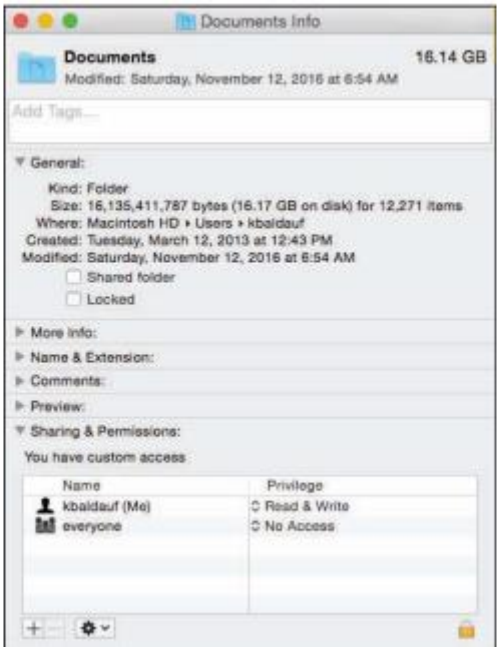
The system administrator is typically the only user who has full access to the system. The system administrator can also define the type of access allowed. Access to files and folders can be classified as read, write, and execute. Execute permission can be applied to programs (.exe) and folders in order to control access to folders. Data files make use of read and write permissions. The following table illustrates settings for a system resource, such as a file stored on a web server accessible from the web.

File Permissions Example

	Read	**Write**	**Execute**
Owner	X	X	X
Group	X		
World	X		

The ability to carry out system commands can also be restricted through user permissions. For example, Windows uses three classifications for user accounts: Administrator, Standard, and Guest. Those with Standard access can only change their own account password and associated icon. A Guest account is for someone who does not have a permanent account and needs to temporarily access computer or network resources. Guests can't change settings, install hardware or software, or create passwords. An Administrator has full access to system commands and resources.

Home users can set permissions on their own files so that others on the network can access them or not. By default, the personal files and folders on Windows and Mac OS computers are off limits to others on a network. You can adjust file permissions for a specific file or folder by accessing its properties. On a Windows PC, you right-click and choose Properties; on a Mac, select Get Info from the File menu (see figure). Some OSs designate a special folder for sharing documents with others on the network.



Documents 16.14 GB
Modified: Saturday, November 12, 2016 at 6:54 AM

▼ General:

Kind: Folder
Size: 16,135,411,787 bytes (16.17 GB on disk) for 12,271 items
Where: Macintosh HD ▸ Users ▸ kbaldauf
Created: Tuesday, March 12, 2013 at 12:43 PM
Modified: Saturday, November 12, 2016 at 6:54 AM
☐ Shared folder
☐ Locked

▼ Sharing & Permissions:

You have custom access

Name	Privilege
kbaldauf (Me)	Read & Write
everyone	No Access

Apple Inc. Fair Use

User permissions provide a second layer of security for computer networks. Usernames and passwords and the login process are the primary way of keeping unregistered users out of the system. User permissions provide registered users with access to the files they need while restricting access to private resources. User permissions become even more important for files accessible on the Internet. Webpage files, for example, exist on a web server with permissions set to allow the world to read but not write.

Reading: Interior Threats

"IMG_20140814_144219" by Robert is licensed under CC BY 2.0

Interior threats are network security threats that originate from within a network, typically from registered users.

Why This Matters

Interior threats can be intentional or unintentional. Unintentional threats can occur when users make mistakes or exceed their authorization. Intentional threats come from registered users who desire to do the system harm or steal information. Interior threats can be as troublesome for corporations and organizations as hackers, malware, and other exterior threats.

Essential Information

Network users can become security threats through intentional or accidental behavior. There are many situations where innocent human mistakes result in monumental problems. Take, for example, the Taiwan stock trader who mistakenly bought $251 million worth of shares due to a typing error, causing her company a paper loss of more than $12 million. In another error, the U.S. Defense Department, Internal Revenue Service (IRS), and Justice Department have misplaced hundreds of government notebook computers, many of which contain classified government documents. In more common acts of negligence, many users provide hackers with easy access to computer systems by visiting websites designed to spread malware, downloading infected files, using passwords that are easy to guess, or storing passwords and other private information where others can access them.

People's mistakes can lead to problems with security, accuracy, or reliability of computer systems and information. The major types of human errors include those shown in the following table.

User Mistakes That Threaten Computer Security

Type of mistake	Example
Data-entry errors	A military commander might enter into the computer the wrong GPS position for enemy troops. This data-entry error might cause friendly troops to be killed.
Errors in computer programming	A payroll program might multiply a person's pay rate by 1.5 instead of 2 for overtime. This programming error results in a lower paycheck than the employee should receive for overtime work.
Improper installation and setup of computer systems	A person may neglect to properly set the necessary security settings to secure a wireless network.
Mishandling of computer output	A medical office might send lab results to the wrong person, so the person receiving the results has access to another person's private medical information.
Uninformed dangerous computer activity	An employee might write down his or her password for others in the office to find, download an infected file, visit an infected website, or use an infected USB drive.

Type of mistake	Example
Inadequate planning for and control of equipment malfunctions	An individual's hard drive might fail. If the person has not backed up important files recently, he or she will lose important information and have to redo work.
Inadequate planning for and control of electrical problems, humidity problems, and other environmental difficulties	A power outage could shut down an organization's computer system. Without a backup power supply and protection from electrical surges, information and data might be lost, and equipment might be ruined.

Individuals and organizations can take a number of actions to prevent computer-related mistakes. Smart businesses and organizations automate data entry whenever possible to cut down on typing errors. For example, scanning RFID chips or bar codes rather than typing in item numbers during inventory is more accurate. Database management systems and spreadsheets can be programmed to validate data entry. Businesses typically have data backup policies and procedures as well as backup power supplies and surge protection. Businesses also employ technology experts to set up and maintain computer systems so that both the hardware and the software are safe and secure.

It is not uncommon for a business to include policies that outline how employees are to use information systems and handle data in soft and hard copy. For example, a business may have a policy that calls for employees to shred all documents that contain private information. To avoid viruses, most organizations do not allow users to install software on their corporate PC. To keep corporate data secure, some businesses don't allow removable storage devices like USB drives. Just as today's best businesses employ smart and thorough information security practices, individuals should do the same when managing their own personal computers and information.

Besides accidents and careless mistakes, inside threats can be intentional. Disgruntled employees pose a serious threat to computer systems and information. There have been many cases where employees expecting layoffs have taken malicious revenge on data. Those with technical expertise might create software time bombs that destroy data after they have left the organization. Consider the global impact of the leaked documents that NSA (National Security Agency) IT contractor Edward Snowden stole and exposed.

Financial gain is often the goal of internal system attacks. Employees may know of ways to transfer funds within a system or find other illegal means to benefit financially based on their knowledge of the system. Other employees might be bribed by outsiders to provide corporate secrets or database records. Whistle-blowers might want to expose injustices in the corporate or governmental system.

Reading: Network Usage Policy

A **network usage policy** is a document, agreement, or contract that defines acceptable and unacceptable uses of computer and network resources for a business or organization.

Why This Matters

Network usage policies are important for network owners in that they define what is permitted on the computer network and can provide legal protection for the network owner when a user breaks the law using the network. Network usage policies are important for users as they can prevent them from accidentally using the network in a way that was unintended by the network owner. It is important that network users and owners have a clear understanding of acceptable network behavior. This is particularly important in corporate networks, where using the network in inappropriate ways can be used as a basis for an employee's dismissal.

Essential Information

To safeguard against threats to a network's health and stability and to prevent information theft, businesses and organizations often implement network usage policies. New users are often asked to agree to the conditions of the policy before receiving a network account. Users are held liable for upholding the policies and can lose their network account or job if they violate the rules.

Employers are not legally responsible for notifying employees of network usage policies. If policies are not provided at the time of receiving network privileges, it is wise for the new user to ask what is and isn't allowed on the network. Corporate network administrators have the right to listen in on network communications, read employee email, and electronically monitor employees' web activities without giving notice to the employee. Employees enjoy very little legal protection with regard to privacy when using employer-owned networks. People have lost their jobs over activities that they thought were okay but that their employer thought were wrong.

Network usage policies typically warn against using the network for illegal activities. They also cover issues that may not be as obvious. For example, most college networks do not allow students to use their network account to run a business. Some businesses do not allow employees to use their business email account for personal correspondence. The following table lists some common corporate security and usage policies and examples.

Common Network Usage Policy Examples

Policy type	**Examples taken from actual company policies**
Network and computer use	• Users are responsible for maintaining the security of their password. • Users are responsible for using the network facilities in a manner that is ethical, legal, and not to the detriment of others. • It is against federal law and corporate policy to violate the license on computer software. • Users must request permission of system administration for the installation of software and provide proof of ownership of the software license.
Email use	• Employees shall use corporate email systems only for corporate business purposes. • Email systems shall not be used for transmission or storage of information that promotes discrimination. • Employees must use judgment on the type of information sent through email. • The use of network systems to send and forward chain letters and other inappropriate messages is prohibited. • The office may access an employee's email media.
Internet use	• The use of Internet access and the web should be restricted to corporate business purposes. • Users shall request the permission of system administration before installing web plug-in applications. • The use of peer-to-peer networks and file-sharing software is strictly forbidden.

Reading: Wireless Security

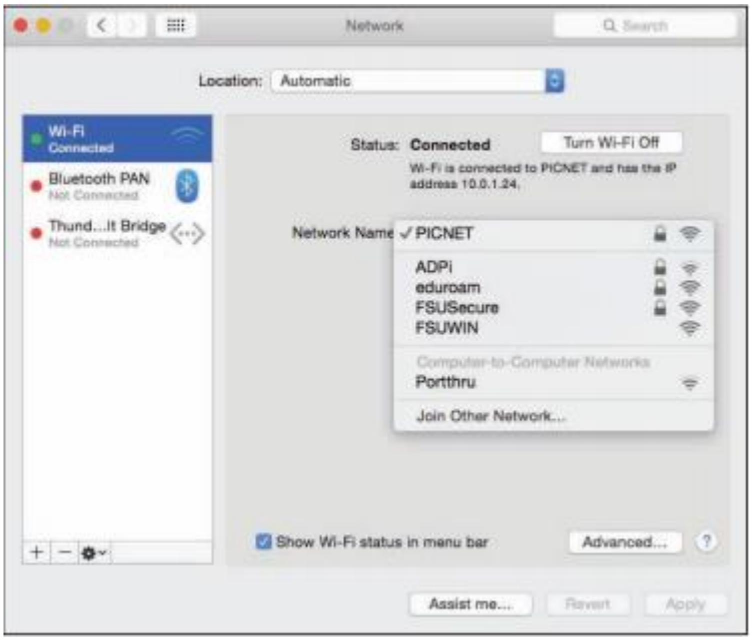
Wireless security refers to the unique threats and defenses associated with wireless computer networks.

Why This Matters

Wireless networks provide wonderful convenience, but, as is usually the case, with convenience comes security risks. With wireless technologies, an attacker no longer has to establish a wired connection to a network. Attackers located within the range of the wireless signal, perhaps on the floor above or in a car parked outside, can attack a wireless network to gain access.

Essential Information

Wi-Fi networks are centered on a telecommunications device called an access point. Access points are essentially routers with the capability of wirelessly connecting to Wi-Fi equipped devices. The access point sends and receives signals to and from computers on the wireless local area network or WLAN (pronounced W-lan). By default, access points are set to broadcast their presence. So, for instance, if you open up your notebook computer in a coffee shop, a message may pop up on your display, letting you know that the Starnet wireless network is within range and asking you if you would like to connect. Starnet is the SSID (service set identifier) of the wireless network. Clicking the Connect icon establishes your wireless connection with the access point. In the case of a commercial provider, you may then be asked for a credit card number to pay for the service. If an access point has no security enabled, clicking the Connect icon puts you on the network, no questions asked. By viewing the Network dialog box (see second figure), a user can view all wireless networks available and select one to connect to.



Location: Automatic

Status: Connected

Wi-Fi is connected to PICNET and has the IP address 10.0.1.24.

Network Name ✓ PICNET

☑ Show Wi-Fi status in menu bar

Courtesy of Apple, Inc. Fair Use

Consider the user in a small apartment who decides to set up a Wi-Fi network. Once the access point is set up, a dialog box appears on the owner's computer with the message, "Network available, would you like to connect?" Easy, right? At the same time, the wireless-enabled computers of neighbors on either side of the user, as well as those upstairs and downstairs from the user, get a similar message. Now there are five users connected to the "private" home Wi-Fi network without the owner's knowledge. This is a fundamental problem of Wi-Fi networks.

Neighbors may find it hard to resist free wireless network access when a pop-up message offers it. But there are other intruders who go out looking for open wireless networks. War driving is the act of driving through neighborhoods with a wireless notebook or handheld computer looking for unsecured Wi-Fi networks. Homemade war-driving kits include high-powered antennae attached to the vehicle roof, a long-lasting power supply for the computer, software such as NetStumbler that probes and scans for networks, and sometimes a GPS receiver to mark coordinates that can be shared with others over services on the web. The legality of war driving is questionable. While accessing unprotected wireless networks that owners have left open may be regarded as legal (but perhaps unethical), working to gain unauthorized access to a secured wireless network is definitely against the law.

Another common hacker trick is to set up a computer to masquerade as a free Wi-Fi network in a public space. When nearby users connect to the “network,” all of the data they send and receive can be accessed by the hacker, including passwords.

So, how can Wi-Fi network owners keep neighbors and war drivers off their private networks? Access points provide several settings that can all but bulletproof a wireless network. The access point configuration settings are accessed using an app or web browser on a network-connected computer. The web address and the password are provided in the access point’s owner’s manual. The following steps combine to offer sufficient protection for most wireless home networks:

- Change the default password for your access point to something unique.
- Add encryption to your network communications through settings on your router, preferably WPA2 encryption.
- Set your router to connect only to the MAC addresses of approved devices.
- Set your access point so it does not automatically broadcast its existence.
- When away from home, protect your wireless devices and the information they hold by following these tips:
- Avoid sending private information like passwords and credit card numbers over public Wi-Fi networks.
- Do not connect to unknown, unsecured access points in public places.
- Turn off any “auto-connect” option for connecting to wireless networks.
- Make sure that the data on your PC is not set to be readable to others on the network and that all sharing services are disabled.
- Do not accept network connection requests from users who may attempt to access your PC.
- Make sure that Bluetooth is set so that it is not “Discoverable” or “Visible” to others. Bluetooth can be used to hack onto smartphones and computers.

Lesson 16.3: Internet Security

Lesson 16.3 Introduction

"Security" by Got Credit is licensed under CC BY 2.0

Internet security refers to the unique threats and defenses associated with computers connected to the Internet.

The Internet is the most popular resource for information, communication, and digital services, and it is also the most dangerous. Criminals long ago discovered that it is much easier and safer to commit crimes in cyberspace than it is in physical space, and they have devised a wide array of traps, scams, and attacks. Internet threats and defenses become more advanced and complex every day. Internet users must learn how to protect themselves online for their own security, the security of the businesses they work for, and that of the countries in which they reside. It is likely that an unprotected PC, when connected to the Internet, will be attacked and infected within minutes.

Expanding a connection from a local area network to the Internet is akin to moving from a small town to downtown Manhattan. While your access to information is dramatically increased, so is your exposure to risk. When a computer is connected to the Internet, it becomes visible to billions of Internet users and a target to millions of attacks.

Internet connections are not a one-way street. Just as you can request information and services from servers, so too can intruders attempt to access information and services from your computer. On the Internet, everyone is just a number—an Internet (IP) address. An address such as 128.186.88.100 could be a web server, an email server, or your PC. Although you may be anonymous, your computer's IP address is registered and known to others.

Attacks against Internet-connected computers can come in the form of direct attacks by hackers (system penetration), through malware like viruses and worms, or via spyware obtained through email, the web, or downloaded files. Internet users are also at risk of being manipulated through scams.

The four pillars of Internet security are: 1) use a firewall, 2) install software updates 3) use security software, and 4) practice safe, cautious online behavior. The checklists below provide a more detailed list of safe and secure behaviors and can be used as a quick reference to the material in this section.

Applying Software Security Tools Checklist

- Set your operating system to update automatically.
- Install or activate antivirus and antispyware software.
- Install or activate firewall software.
- Make sure that all security, antivirus, firewall, and antispyware software is set to update automatically.
- Use backup software to back up important data files automatically on a regular schedule.
- Use a security suite, such as BitDefender, McAfee Total Protection, Norton Security, or Sophos Anti-Virus for Mac, to manage all of the above.
- Install web browser security updates as soon as they are released.
- Use encryption to protect private files stored on your computer, to secure web transactions, and to secure wireless networks.
- When connected to a network, make sure that user permissions are set to share only the files you wish to share.
- If you use a home wireless network, disable SSID broadcasting on the access point, change passwords on the access point, and set it to connect with only specific MAC addresses.
- Turn Bluetooth off (set to undiscoverable) unless using it.
- Windows users can consider using Windows cleaner software to maintain the Windows Registry.
- Use spam filters on your email.

Maintaining Safe and Vigilant Online Behaviors Checklist

- Don't type private information when connected to a public wireless network.
- Select strong passwords carefully and change them regularly.
- Do not open email attachments unless expected and scanned for viruses.
- Do not click links received in emails, text messages, or social network messages unless you are certain they are authentic and safe.
- Examine web addresses closely to make sure that they are legitimate and include https:// for forms.
- Avoid P2P file-sharing networks.

- Avoid websites set up for unethical, immoral, or indecent purposes.
- Do not allow websites to install software on your computer, unless you are certain the website is legitimate.
- Keep your computer system well organized and up to date using the housecleaning tips provided in this section.

Reading: Hacker

A **hacker** is an individual who subverts computer security without authorization.

Courtesy of Darren Kitchen. Fair Use

Why This Matters

In the battle between Internet users and those who attack them, it is valuable to understand the motivation of the enemy. Learning about criminal hackers, why they hack, and what tools they use enables Internet users to defend against attacks more effectively.

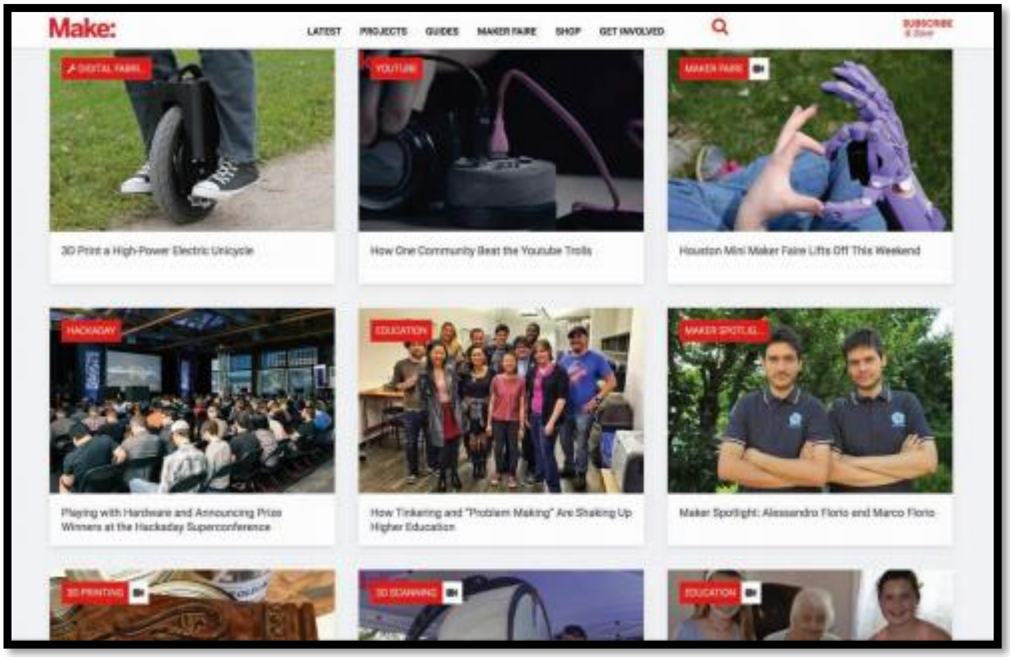
Essential Information

A hacker subverts computer security without authorization. Security professionals refer to this as system penetration. In reality, there are many names used to label those who unlawfully hack into secure computers and networks. The news media generally uses the term hacker. Hackers and others who wish to differentiate between law breakers and innocent techies use the term cracker, for criminal hacker, claiming that hackers do not necessarily break laws. Those in the information security industry tend to prefer the labels attacker and intruder.

Types of Hackers

Hacker	**Description**
Black-hat hacker	A hacker who takes advantage of security vulnerabilities to gain unlawful access to private networks for unethical purposes
White-hat hacker	An individual who considers himself/herself to be working for the common good by hacking into networks in order to call attention to flaws in security so that they can be fixed
Gray-hat hacker	A hacker of questionable ethics
Script kid or Kiddie	A person with little technical knowledge who follows the instructions of others to hack networks
Hacktivist	A hacker who hacks networks for a social cause or perceived greater good

Notice that there are ranges of ethics embraced by varying types of hackers. Not all hackers are considered unethical. Many hackers simply enjoy re-engineering technologies and gadgets so that they perform differently than originally intended. Make magazine is a publication geared toward this type of hacking. Other hackers experiment with cyberattacks and hacks so that they can better protect computer systems. This is the philosophy behind the popular hacking/security podcast Hak5. Often the line between hacking as an exploratory hobby and breaking the law is difficult to define. Some hackers are drawn over that line and face serious consequences for their crimes.



3D Print a High-Power Electric Unicycle

How One Community Beat the Youtube Trolls

Houston Mini Maker Faire Lifts Off This Weekend

Playing with Hardware and Announcing Prize Winners at the Hackaday Superconference

How Tinkering and "Problem Making" Are Shaking Up Higher Education

Maker Spotlight: Alessandro Florio and Marco Florio

Makezine. Fair Use

Over the history of the Internet, hacking migrated from a hobby to a money-making profession. Hackers have increasingly gained access to systems for the purpose of taking control and selling access to hacked computers for illegal activities, such as sending illegal spam or launching denial-of-service attacks. In 2011, that trend took a dramatic turn towards hacktivism. Hacker collectives like Anonymous began hacking systems for perceived righteous causes. They targeted businesses and government organizations perceived by the hackers as evil. They exposed large numbers of confidential records online through websites like WikiLeaks. They did not profit financially from their exploits, but instead embarrassed companies and governments and proved that no network is safe from hackers. In 2012 and 2013, global attention was turned to cyberwarfare and espionage, where one-fifth of all cyberattacks were government sponsored. Cyberwarfare and espionage have been a growing area of government investment ever since.

Hackers have many tools at their disposal for finding vulnerable computers and gaining access to them. Attacks may also be automated in the form of malware viruses, worms, and spyware. These methods of attack can achieve many of the goals of common attacks without the need for directly manipulating a system. The following table describes some tools in the hacker's arsenal.

Hacking Tools

Tool	**Description**
Key-logging software	Software installed on a computer to record all keystrokes and commands. The recording is later collected from a remote computer over the Internet and played back in order to spy on the user's actions and sometimes to steal usernames and passwords.
Packet-sniffing software	Software that captures and analyzes all packets flowing over a network or the Internet. It can be programmed to look for personal information such as passwords and credit card numbers.

Tool	Description
Wireless network scanning software	Software used to locate unprotected wireless networks. Once found, a hacker will try to connect to it. If unable to connect to it, wireless sniffing software can be used to capture the information being sent over the network. Encryption hacking software can be used to break common forms of encryption used on wireless networks.
Port-scanning software	Software that searches random IP addresses for open ports. Port-scanning software is allowed to run continuously, allowing the attacker to collect a list of IP addresses waiting to be hacked.
Social engineering	A technique that uses social interactions to manipulate individuals to give up personal information. For example, a social engineer might phone a person, pretending to be a system administrator in order to get that person to provide a password. A social engineer may even go dumpster diving—that is, rummaging through trash to steal credit card numbers or other personal information.

Reading: Firewall

"My Virus Infected Computer" by koolkat_one is licensed under CC BY 2.0

A **firewall** is network hardware or software that examines data packets flowing in and sometimes out of a network or computer in order to filter out packets that are potentially dangerous.

Why This Matters

Hackers attempt to access your computer dozens of times every day. Hacker tools allow them to continuously cruise the Internet, checking computers for an open port that can be used to gain access. A firewall slams the door in hackers' faces, turning away probes and hack attempts. A firewall can also prevent infected computers from operating under the control of a hacker. Using a firewall is one of the four pillars of information security, the others being installing software patches, using security software, and practicing safe, cautious online behavior.

Essential Information

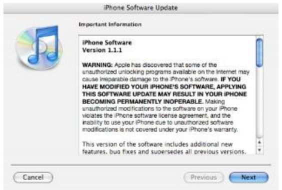
A firewall is implemented either through the software running on a computer or through hardware such as a network router. For personal computers, firewall software is typically used and can be enabled in system security settings. Networks typically use software as well, but some larger networks employ a hardware firewall—a device connected to the network at the point where it joins the Internet. Whether implemented through software or hardware, a firewall protects all the ports of a network or PC from intruders and guards against known methods of attack.

A standard firewall checks all incoming data packets and rejects packets that are defined as dangerous or undesirable. Microsoft Windows, Mac OS, and some Linux distributions include a firewall utility. Users not using a firewall should enable the firewall as soon as possible.

Users looking for a more powerful firewall can find plenty to choose from online. Some firewalls include the ability to check outgoing as well as incoming packets. The purpose of checking outgoing packets is to keep zombie computers from carrying out the will of hackers. Zombie computers are infected computers that are being used in a botnet to attack other computers or send spam. There are millions of zombie computers on the Internet today. Using firewalls that check outgoing packets reduces online infections and spam considerably.

It is even more important to use firewalls on networks than on PCs. A firewall is installed at the point that the network connects to the Internet to protect the entire network from infection and attacks. It is a good idea to use a firewall that checks both incoming and outgoing packets because infected computers are hard to identify on a network. Network firewalls also provide settings that allow the administrator to filter particular types of network activities. For example, a campus network administrator might use a firewall to block access to P2P networks. Firewalls are also used by some governments, Internet service providers, and businesses to censor data that may not be dangerous but may be undesirable.

Reading: Software Update



iPhone Software
Version 1.1.1

WARNING: Apple has discovered that some of the unauthorized unlocking programs available on the Internet may cause irreparable damage to the iPhone's software. **IF YOU HAVE MODIFIED YOUR IPHONE'S SOFTWARE, APPLYING THIS SOFTWARE UPDATE MAY RESULT IN YOUR IPHONE BECOMING PERMANENTLY INOPERABLE.** Making unauthorized modifications to the software on your iPhone violates the iPhone software license agreement, and the inability to use your iPhone due to unauthorized software modifications is not covered under your iPhone's warranty.

This version of the software includes additional new features, bug fixes and supersedes all previous versions.

"iPhone 1.1.1" by mysistersabarista is licensed under CC BY 2.0

A **software update**, sometimes called a security patch, fixes software bugs and flaws and is typically distributed to software users through online software updates.

Why This Matters

Although software vendors do their best to develop secure and bug-free software, the high degree of complexity in today's software makes it very difficult to achieve perfection. As flaws are discovered, software vendors provide updates to users that include patches to correct the bugs and flaws.

Essential Information

Software bugs in operating systems, web browsers, and other Internet software can create security holes that hackers may exploit to gain full control of a computer. These are called critical software flaws and should be patched as soon as possible to keep computers and data safe. Software updates are one of the four pillars of information security, the others being using a firewall, using security software, and practicing safe, cautious online behavior.

Most software companies offer free and regular software updates for their products. Software updates are distributed to customers over the Internet, and the process of applying them is typically automatic. Many programs use the Internet to check periodically to see if an update is available. When an update is discovered, it may be downloaded automatically or the user may be prompted to download it. In either case, the user is then asked to click to install the update.

One of the great benefits of cloud computing is that it removed the burden of software updates from users. For online software like Google Docs and Microsoft Office 365, the software company—Google or Microsoft in these cases— fixes software bugs as they are discovered, often without users ever noticing the bug.

Users are wise to set their operating system to update automatically, whenever updates become available. It takes hackers less than 24 hours after a security hole is identified, to design a method of exploiting the vulnerability. When an update is released, it becomes a race between users applying patches and hackers seeking to exploit the vulnerability.

Mobile devices including iPhones, iPads, Windows phones, and Android devices are also targets for hackers. Many Android phones have been infected with malware from free apps in Google Play and other app stores. It’s important to keep mobile device software updated to protect the devices from attacks.

It is particularly important to patch operating systems, web browsers, browser plug-ins, and other network and Internet software as soon as updates are available. The vast majority of hacker exploits take advantage of the security holes in Internet software. Keeping this software up to date and using firewall software are two of the most important steps to take to ensure information security.

Reading: Malware

"Rotes Wort MALWARE (Schadsoftware) in blauem Binärcode aus 1 und 0 auf Bildschirm" by verchmarco is licensed under CC BY 2.0

Malware is short for “malicious software” and includes any software designed to damage, corrupt, or illegally manipulate computer resources. Common forms include viruses, worms, and spyware.

Why This Matters

Cyberattacks can take the form of software that is distributed and executed on a computer without the user’s knowledge for the purpose of corrupting or disrupting systems, stealing information, or using the system to launch further attacks. The most common of these malware programs are viruses, worms, and spyware.

Essential Information

A virus is a program that attaches itself to a file, spreads to other files, and delivers a destructive action called a payload. The payload could be the corruption of computer data files or system files, resulting in the loss of data or a malfunctioning computer. There are many different types of viruses. A worst-case scenario for damage would be the total loss of data and software. Viruses do not harm computer hardware or cause users to have to buy a new computer. Recovery might involve wiping the hard drive of all files to remove all infection, reinstalling the operating system and all software, and restoring data files from backup.

Viruses are sometimes delivered through a technique called a Trojan horse, or just a Trojan. Like the Trojan horse in Greek mythology, these Trojan horses appear to be harmless programs, but when they run, they install other programs on the computer that can be harmful. A backdoor Trojan opens up ports (back doors) on the computer to allow access to intruders. This type of virus distribution is common on Android mobile devices. A hacker loads a virus in a legitimate and desirable-looking app, posts it in an app store, and just waits for gullible users to download and install it so the virus can infect the device. While Google works to minimize dangerous apps in its Play Store, there are many other sources for Android apps online where anyone can post apps for download.

One form of malware called ransomware uses encryption to hold the user’s data captive until a ransom is paid. For example, Ransom-A, one of the first ransomware Trojans, encrypted the user’s data files and demanded $10.95 to be paid through Western Union. It threatened to delete a file every 30 minutes until the ransom was received.

A worm does not attach itself to other programs but instead acts as a free agent, replicating itself numerous times in an effort to spread to other computers or overwhelm systems. For example, within 10 minutes of its introduction, the Slammer worm had attacked more than 75,000 computers. Thirty minutes later, some believe the worm had disrupted one in five data packets sent over the Internet.

In 2010, the world saw the first worm that experts believe was designed for cyberwarfare. The Stuxnet worm was an extremely sophisticated piece of code, designed to attack industrial software and equipment. More specifically, the worm appears to have been designed to attack the centrifuges used to enrich uranium at a nuclear power plant in Iran.

Spyware is software installed on a computer without the user’s knowledge, either to monitor the user or to allow an outside party to control the computer. Spyware is so prolific that any computer that spends time on the web, if not protected, has probably contracted it. Spyware differs from viruses and worms in that it does not self-replicate. Spyware is often used for commercial gain by displaying pop-up ads, stealing credit card numbers, distributing spam, monitoring web activity and delivering it to businesses for marketing purposes, and hijacking the web browser to show advertising sites.

Spyware is distributed by deceiving the user into installing it by hiding it in legitimate apps, email attachments, webpages, or other online resources. Spyware is often installed by a virus or worm. Once on a system, spyware runs in the background, unknown to the user, carrying out the wishes of its creator. Spyware can communicate with its creator over the Internet.

Google believes that more than 5 percent of all users have at least one ad injector knowingly or unknowingly installed on their operating systems, according to a research report from Google and the University of California-Berkeley. Often simply unwanted—but sometimes outright malware—ad injector software inserts additional or replacement advertising into sites during online browsing.

A computer that carries out actions (often malicious) under the remote control of a hacker, either directly or through spyware or a virus, is called a zombie. Thousands of computers are added to the ranks of zombies each week. Zombie computers can join together to form zombie networks, or botnet armies. Botnet armies apply the power of multiple PCs to overwhelm websites with distributed denial-of-service attacks, to crack complicated security codes, or to generate huge batches of spam. It has been estimated that a very high percentage of spam originates from zombie computers.

The goal of the malware engineer is to get the user to run the software that installs the malware. Although sending malware as email attachments used to be the preferred method of distribution, today most malware is spread from webpages. A common trick is to infect a website so that when users visit the site, a pop-up instructs them to install a software update. Instead of legitimate software, malware is installed on the user’s PC. Even worse, in drive-by downloads, users aren’t even prompted to download the software. Just visiting the site infects their computer. By distributing the link to an infected website through social media or email, millions of computers can be infected. Once infected, a PC can then act as the attacker and spread malware to other PCs, either over a network or through email, social networks, instant messaging systems, shared files, or webpages (if the infected machine is a web server). Good antivirus software protects a computer from the vast majority of these types of attacks.

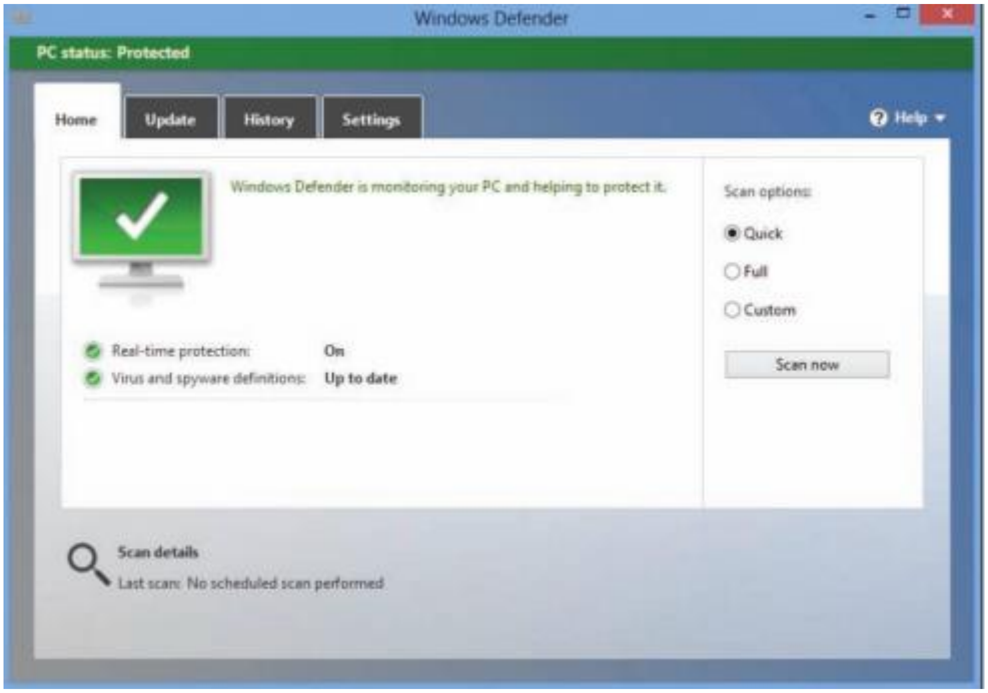
Sometimes, rumors of nonexistent viruses and virus hoaxes spread online. These may be an effort by hackers to get users to take unsafe actions in order to infect their devices. When you hear about a virus, it’s always a good idea to check it out online using Google and by visiting the websites below prior to taking any action. If a website pops up a message saying your computer is infected, it is most likely an effort to get you to download illegitimate “virus protection” software actually intended to infect your device.

Reading: Antivirus Software

Antivirus software, also known as virus protection software, uses several techniques to find malware on a computer system; remove it if possible; and keep additional malware from infecting the system.

Why This Matters

Implementing some form of virus protection is a necessity on all types of PCs: Windows and Macs. Without some form of virus protection, it is almost assured that an Internet-connected PC is—or will soon become—infected. Antivirus software is one of the four pillars of information security, the others being firewalls, software patches, and safe, cautious online behavior.



PC status: Protected

Windows Defender is monitoring your PC and helping to protect it.

Scan options:

● Quick
○ Full
○ Custom

Real-time protection: On
Virus and spyware definitions: Up to date

Scan details
Last scan: No scheduled scan performed

Courtesy of Microsoft Corporation. Fair Use

Essential Information

The number-one tool against malware, including viruses, worms, and spyware, is antivirus software. Antivirus software is only effective if it is continuously running to guard against attacks and if it is continuously updated with new virus information as it becomes available. For this reason, antivirus software, such as BitDefender, McAfee Total Protection, Norton Security, or Sophos Anti-Virus for Mac — which update automatically when necessary—are preferred. Antivirus software is often packaged with firewall software, backup software, and other security tools as a security software suite that covers all aspects of computer security. Most importantly, antivirus software can protect you from drive-by downloads and unsafe websites designed to infect your computer.

In addition to using antivirus software, knowledge and caution play a big part in protecting PCs against viruses and worms. Follow these practices to protect your PC from malware:

- Don’t open email or IM attachments that come from friends or strangers unless they are expected and inspected by antivirus software.
- Keep up with software patches and updates for your operating system, your web browser, your email software, and your IM software.

- Avoid clicking links sent to you through email or sent to you through text messages or social networks.
- Use caution when exploring websites created and maintained by unknown parties.
- Avoid downloading software or plug-ins from websites created and maintained by unknown parties.
- Avoid any software from untrusted sources.
- Be cautious if you use P2P file-sharing networks; they do not effectively protect users from dangerous files that are being swapped.
- Don't download antivirus software when prompted to do so in an email or on the web—it's often a ploy to get you to install malware.

Reading: Botnet

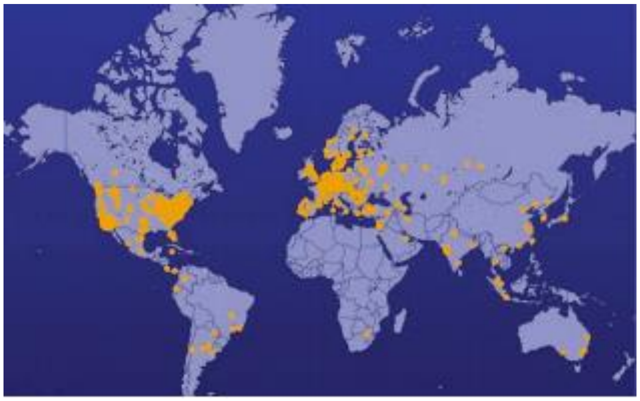
A **botnet, or botnet army,** refers to a collection of computers autonomously or automatically working together toward some goal; these are often zombie computers that are synchronized to perform illegal activities on the Internet.

Why This Matters

Botnets harness the power of hundreds of thousands of compromised computers to carry out monumental attacks over the Internet. Computers are drafted into botnet armies through the use of malware. It is possible that your computer is a soldier in a botnet army. Understanding botnets will help you to free your computer if it has been enslaved and protect your computer from becoming a zombie.

Essential Information

Millions of computers on the Internet are leading double lives. They service their users as usual without any indication that anything is amiss while they simultaneously live secretive second lives as zombie computers working in botnet armies. The Kraken botnet was one of the world's earliest and largest in 2008, with more than 400,000 zombies carrying out its commands. It is estimated that Kraken uses its zombies to crank out more than 9 billion spam email messages per day. Another botnet, Storm, at its height in early 2008, was believed to control as many as a million computers. The ZeroAccess botnet, sometimes known as Sirefef, infected more than 2 million computers and cost online advertisers an estimated $2.7 million per month in 2013. More recently, botnets progressed from utilizing people's computers to utilizing devices on the Internet of Things. In late 2016, a massive cyberattack took out huge swaths of the Internet throughout the U.S. by exploiting a security hole in Internet-connected devices such as security cameras.



The Shadowserver Foundation. Fair Use

Devices are drafted into botnet armies when they are infected with malware. A computer under the control of an outside party working in a botnet is referred to as a zombie computer. Botnet armies are controlled by botnet command and control (C&C) servers that disperse the commands of the hackers who created them. The Shadowserver Foundation maintains a map of C&C servers worldwide that is updated daily (see figure). Botnet armies are used to distribute spam, viruses, and worms. They are also used in distributed denial-of-service attacks (DDoS) in which many computers simultaneously access a web server, making it impossible for the server to respond to legitimate requests.

The power of a botnet can surpass that of today's most powerful supercomputers. With that kind of power, a botnet can be used to crack encryption codes and hack accounts through brute force methods. Botnet owners lease out their botnets for all kinds of online jobs. Botnet armies are a major tool in cyberwarfare. In 2007, a botnet was used to bring down the information infrastructure of the country of Estonia, in an act that the country viewed as a military attack. Since then, botnets have been behind many major outages in businesses and government agencies.

Reading: Cyberwarfare

"67718" by Catalyst Research Institute is licensed under CC PDM 1.0

Cyberwarfare extends traditional forms of warfare to the Internet and the web, including espionage, psychological warfare, and attacks.

Why This Matters

Heavy dependence on information technologies and the Internet creates a significant vulnerability for individuals, businesses, and governments. Those wishing to harm a population for political or ideological reasons may use information systems as tools in their quest and may target information systems in order to disrupt the lives of their enemies. In this manner, the Internet has become a primary tool for terrorism and international attacks.

Essential Information

Attacks over the Internet are a serious and well-known threat to nations. All of the major world powers invest significantly in guarding their online resources—including government servers that contain confidential information—and their critical national infrastructure, such as hospitals, utilities, transportation, and commerce. The U.S. Pentagon has stated that the United States reserves the right to retaliate with military force against a cyberattack and is working to sharpen its ability to track down the source of any breach. U.S. intelligence officials have accused China and Russia of systematically stealing American high-tech data for their own national economic gain. Attacks originating in China against the U.S. and its allies, and China's complaints of being attacked by Western governments, have become so numerous that some are calling it a cyber cold war.

Smaller countries, including North Korea and Iran, have turned to cyberwarfare as a primary offensive against the U.S. and other Western countries. When it comes to cyberwarfare, the physical size of a country and its armed forces doesn't matter.

Terrorist organizations such as al-Qaeda have made effective use of the Internet and the web for promoting their causes, recruiting new members, and terrorizing populations. There is no doubt that such terrorist organizations are also seeking to use the Internet to harm their enemies through hacking and attacking online. Cyberterrorism extends traditional forms of terrorism to the Internet and the web.

The United States Computer Emergency Readiness Team (US-CERT) was established to monitor the security of U.S. networks and the Internet and to respond to cyberwarfare and cyberterrorism. US-CERT is part of the National Cybersecurity Division of the United States Department of Homeland Security. The US-CERT website, www.us-cert.gov, gives network administrators and computer users up-to-date information on security threats and defenses. A new branch of the Pentagon has been established to defend the U.S. against cyberattacks. The Pentagon's Cyber-Security unit is the fastest growing unit in the U.S. Department of Defense, with plans to grow from 900 on staff to more than 4,000 over the next few years.

Fighting international cyberattacks is difficult as there are currently no global cybercrime laws. The laws of one country cannot be enforced in another without the cooperation of both governments. A computer attack may be designed by hackers in country A and launched in country B to attack computers in country C. Some countries are discussing the establishment of a global cyber-crime task force, similar to the INTERPOL international police network. One step in that direction was the Council of Europe's convention on cybercrime in 2001 and its more recent Dialogue on Internet Governance (EuroDIG). The convention on cybercrime produced a treaty that calls on countries to work together to create international laws that address cybercrime. Currently, over 49 countries have ratified the convention.

Just as traditional international warfare is governed by the Geneva Convention and other international treaties, cyberwarfare will soon be governed by its own set of international rules. The NATO Cooperative Cyber Defense Center of Excellence has produced a set of rules called the Tallinn Manual, named for the Estonian capital where it was compiled. The rules protect civilian targets such as hospitals, dams, and nuclear power stations. Hacking a dam's computer controls to release its reservoir into a river valley is just as serious as breaching it with explosives, the authors argue, and should have similar rules and responses. They argue as well that medical computer systems should get the same protection that brick-and-mortar hospitals do.

Reading: Identity Theft

"An online fraudster commits online fraud or identity theft wearing black gloves" by Patrick Cannon Tax Barrister is licensed under CC BY 2.0

Identity theft is the criminal act of stealing information about a person to assume that person's identity in order to commit fraud or other crimes.

Why This Matters

The U.S. Federal Trade Commission (FTC) receives hundreds of thousands of consumer fraud and identity theft complaints each year. Yearly losses to U.S. consumers total more than a billion dollars. Individuals between the ages of 18 and 29 are hardest hit by ID theft.

Essential Information

Using a person's Social Security number (SSN), birth date, or other personal identifiers, an identity thief can apply for a new credit card in the victim's name and have it delivered to a post office box. Identity thieves can make purchases on stolen credit card numbers, make bank withdrawals, apply for loans, or buy cars. The information could also be used for more serious crimes. For example, an illegal driver's license might be created for use by a non-U.S. citizen to gain access to services and benefits provided only to citizens. The damage caused can be quite serious. An identity thief can also do damage to a victim's reputation by perpetrating crimes under the victim's identity.

Identity thieves use several methods to steal personal information. In a technique called dumpster diving, personal information can be found by going through someone's trash. Store clerks and cashiers can steal customer credit card information when processing a sale. Phishing is a technique used to trick a person into providing personal information on a fake website that looks like a reputable website. Identity thieves might submit a change of address form for a victim in order to have personal information rerouted to their own post office box. Personal information is often stolen by stealing wallets and purses or by stealing database records from businesses. Social engineering is a technique that uses social interaction to manipulate individuals into giving up personal information. For example, a criminal may phone a system administrator, pretending to be someone else in order to get access to a network account. Criminals might also buy personal information from other thieves, using the dark web, sometimes referred to as the deep web—underground networks and marketplaces that exist on the Internet.

People can protect themselves from identity theft by being cautious with their personal information and by following these tips:

- Keep Social Security numbers private; be suspicious of anyone who asks for your SSN.
- Shred documents containing personal information prior to disposal.
- Use caution online and verify the ownership of websites that ask for personal information. Never trust links sent to you via email or other messaging services.
- Store personal information in secure locations, both in physical and digital formats.
- Use encryption to safeguard information that is stored on your computer and transmitted over networks.
- Opt out of services offered by online stores that want to store your personal information for faster checkout; each business that retains your credit card info is an additional target for hackers. Instead, utilize one central digital wallet to store your payment info such as PayPal, Apple Pay, Google Pay, or others.
- Be careful about storing digital copies of personal information on your own computer and in business and organization databases; keep these to a minimum.

Reading: Internet Fraud (3 min.)

"Wooden scrabble letters spell out fraud in a stock style photo" by Patrick Cannon Tax Barrister is licensed under CC BY 2.0

Internet fraud is the crime of deliberately deceiving a person over the Internet in order to damage them or to obtain property or services unlawfully.

Why This Matters

The FBI receives more than 200 million Internet fraud complaints each year. Hundreds of millions of dollars are stolen each year by online criminals. With increasing amounts of business taking place online, Internet fraud is more prevalent than ever. It is essential to be able to recognize common types of fraud in order to protect yourself against them.

Essential Information

The FBI and the Internet Crime Complaint Center collect data each year on cases of Internet-related fraud. A common form of Internet fraud is Internet auction fraud. Auction fraud involves being swindled by sellers or buyers on auction sites like eBay. Another common type of fraud is non-delivery of merchandise, which involves purchases from etailers that process the payment and never deliver the goods. There are numerous cases of credit card fraud and check fraud, where online customers use fraudulent checks or stolen credit card numbers to purchase items. There are also cases of phony loan company or bank websites that pretend to assist consumers with debt problems but really rob them blind.

The Nigerian letter fraud has been around for a long time. In this online scam, the victim receives an email from a prominent figure outside of the country asking for assistance, perhaps in the form of utilizing the victim’s bank account to store a large sum of money. Of course, the victim will be well compensated for the inconvenience. Although often the author of the message claims to be from Nigeria, there are many variations on the theme. Once the victim supplies a bank account number, that account is cleaned out.

Often, scammers set up fraudulent websites that appear legitimate but are actually covers for identity theft. Users may receive fraudulent emails inviting them to visit the phony website where they are asked to enter private information. Impersonating legitimate businesses on the web or in email is referred to as spoofing. Phishing scams utilize spoofed email and webpages to fool users into believing the source of the email is legitimate.

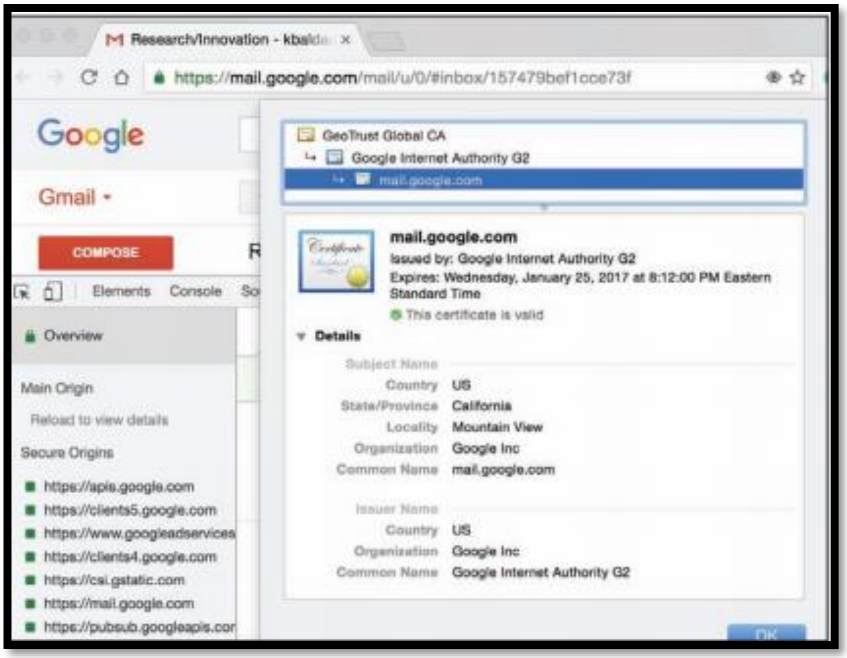
Facebook and other social networks have become major tools for fraudsters. Hacked accounts are used to trick friends into clicking links to fraudulent sites. Ads are also used to lure victims to fraudulent sites. Dating websites and Craigslist can also be used to lure victims into unsafe situations where fraud and even worse crimes are perpetrated.

Reading: Digital Certificate

A **digital certificate, also called an SSL certificate**, is a type of electronic business card that is attached to Internet transaction data to verify the sender of the data.

Why This Matters

Because so much of the information we send over the Internet is confidential, it is important that the identities of individuals, businesses, and organizations involved are positively verified. For example, consumers need to make sure that they are giving their credit card number to a legitimate and trustworthy business, and businesses need to confirm that the customer is the owner of the credit card being used. Transaction data must be accessed only by intended parties and not be intercepted by outsiders. Two technologies are available to assist individuals and businesses in meeting these goals: digital certificates and encryption.


Research/Innovation - kbald
https://mail.google.com/mail/u/0/#inbox/157479bef1cce73f
Google
Gmail
COMPOSE
Elements
Console
Overview
Main Origin
Reload to view details
Secure Origins
https://apis.google.com
https://clients5.google.com
https://www.googleadservices
https://clients4.google.com
https://csi.gstatic.com
https://mail.google.com
https://pubsub.googleapis.com
OK

GeoTrust Global CA
Google Internet Authority G2
mail.google.com

mail.google.com
Issued by: Google Internet Authority G2
Expires: Wednesday, January 25, 2017 at 8:12:00 PM Eastern Standard Time
This certificate is valid

Details

Subject Name

Country	US
State/Province	California
Locality	Mountain View
Organization	Google Inc
Common Name	mail.google.com

Issuer Name

Country	US
Organization	Google Inc
Common Name	Google Internet Authority G2

Google. Inc. Fair Use

Essential Information

Digital certificates are provided by certification authorities such as Symantec VeriSign and Thawte. They can be used to verify the sender of email and other forms of Internet communication. Digital certificates for use in encrypting web communications and credit card transactions cost the provider between $350 and $1,400, depending on the level of security and type of communications. Certificates cost more for ecommerce than for nonbusiness use. Digital certificates for personal email are provided by Thawte for free.

Digital certificate information can be accessed on any HTTPS page by clicking the lock icon in the status bar or by right-clicking the page and viewing its properties (Windows) or info (Mac). A digital certificate contains the owner’s name, a serial number, an expiration date, and a public key (see figure). The public key is used in encrypting messages and digital certificates. Encryption uses high-level mathematical functions and computer algorithms to encode data so that it is unintelligible to all but the intended recipient. Through the use of a public key (a large number) and a private key kept by the certification authority, an encrypted message can be decrypted back into its original state.

Digital certificates combined with Secure Sockets Layer (SSL) technology and a more recent version of SSL called Transport Layer Security (TLS) enable encrypted communications to occur between a web browser and web server. This combination of technologies is used to secure usernames, passwords, and credit card information when they are typed into a web form and sent to a web server. The presence of an SSL connection is usually indicated by a URL that uses https:// rather than http://. Also, a closed lock icon appears in the address line or status bar of the browser window when the connection is secure. New versions of browsers that support Extended Validation SSL go even further by showing a green background in the address bar for secure sites.

Reading: Phishing Scam

"Security-Stock-11078" by Hivint is licensed under CC BY 2.0

A **phishing scam** combines fraudulent email with faked websites in order to trick a person into providing private information that can be used for identity theft.

Why This Matters

There are many forms of Internet fraud designed to trick users into giving out private and valuable information. Phishing scams are some of the most difficult to detect. The more you know about the various types of phishing scams, the better protected you will be.

Essential Information

A phishing scam combines a spoofed email with a spoofed website in order to trick a person into providing private information. Spoofing is the act of impersonating a person, business, or organization on the web or through email. In a phishing scam, the hacker sends out mass emails (often using a botnet) that appear to come from a legitimate company, such as PayPal, a credit card company, or a bank. The email warns of some trouble with your account and provides a link that should be clicked to address the problem. The link may look safe—such as https://www.paypal.com/customer-service—but when you click it, it takes you to a different web address that looks just like the real PayPal login page, so you don't notice a slightly different URL in the address box. The page looks like the PayPal page because the hacker copied the page exactly from PayPal to his or her own web server.

From this point in the phishing scam, a number of things can occur. Most commonly, the user logs in as requested. The hacker has then attained his goal of stealing the user's login information. Then, the user may get a message like "Incorrect Password. Click here to try again." When the user clicks to try again, the software may send the user to the login screen of the real website, where the user can log in without any trouble. The victim is totally unaware of the fraud or identity theft that has occurred.

In addition to stealing login information, and depending on how long the user can be strung along, phishing pages can also install spyware on a computer. The website www.antiphishing.org receives thousands of phishing reports each month.

Phishing tactics are getting more sophisticated. In an attack called spear phishing, private or personal information is used to target a specific individual. The fraudulent email received can be so convincing that it is impossible to guess that it isn't a legitimate request.

In a bold scheme, several hacker tricks were combined to ultimately blackmail Monster.com users. Monster.com reported that information about 1.3 million job-seekers had been stolen from its servers. The usernames, email addresses, and other information stolen from Monster.com were used in a spear phishing scam. Each of the users received email that appeared to come from Monster.com, inviting the users to try a new "Monster Job Seeker Tool." Those who took the bait ended up downloading ransomware that encrypted their files and demanded $300 to unlock them.

To protect yourself from phishing scams, avoid clicking links received in emails. Instead, type URLs directly into your web browser. Examine web addresses closely to make sure that they are legitimate and include an https:// for forms or a closed lock icon or green background in the address bar.

In the criminal act of pharming, hackers hijack a domain name system DNS) server to automatically redirect users from legitimate websites to spoofed websites in an effort to steal personal information. In pharming, a user may type www.paypal.com into the web browser address bar; but when the request is received at the DNS server, rather than routing the packets to the PayPal server, they are hijacked to the hacker's web site. Pharming strikes a serious blow to the underlying architecture of the web as it is nearly impossible to detect. The ability of hackers to corrupt DNS computers could undermine the public's faith in ecommerce and the Internet altogether.

Reading: Information Security Laws

Information security laws seek to protect the civil rights of populations from abuses of information systems and the Internet.

Why This Matters

Securing networks and the information they store takes effort by individuals, businesses, and governments. Information security is so important that the United Nations has taken an interest in managing it. The U.S. Whitehouse has also developed a Comprehensive National Cybersecurity Initiative (CNCI) to establish a front line of defense against threats to the national infrastructure.

Essential Information

A number of U.S. laws have been created for the purpose of securing information and protecting privacy. The following table lists the most important such laws.

U.S. Information Security Laws

Law	Description
Consumer Internet Privacy Protection Act of 1997	Requires data collectors to alert people that their personal information is being shared with other organizations
Children's Online Privacy Protection Act of 2000	Gives parents control over what information is collected from their children online and how such information may be used
Information Protection and Security Act of 2005	Gives the Federal Trade Commission (FTC) the ability to regulate the sale of personal information
Notification of Risk to Personal Data Act of 2003	Requires businesses to notify individuals when their personal information is stolen
Identity Theft Protection Act of 2005	Requires businesses to secure sensitive data physically and technologically and to notify consumers nationwide when data is compromised
Health Insurance Portability and Accountability Act (HIPAA) of 1996	Requires those in the health industry to protect the privacy of health information and provides policies and procedures for doing so
Sarbanes-Oxley Act ("Sarbox") of 2002	Fights corporate corruption by imposing stringent reporting requirements and internal controls on electronic financial records and transactions
Gramm-Leach-Bliley Act (GLBA) of 1999	Requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information