THE INTERNET OF THINGS (IOT)

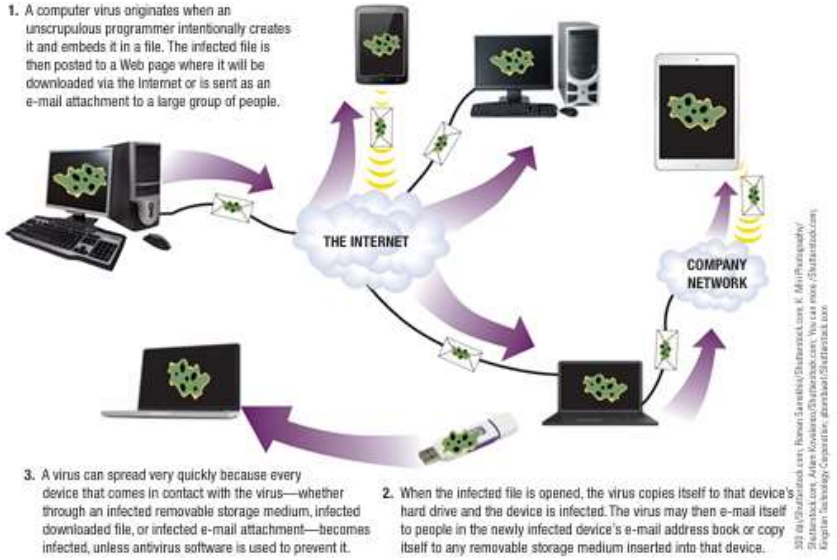
One of the hottest Internet topics today is the Internet of Things (IoT). The Internet of Things refers to a world where everyday physical objects are connected to, and uniquely identifiable on, the Internet so they can communicate with other devices. Also called Machine-to-Machine (M2M) because it involves primarily machines talking directly to one another, the IoT is expected to greatly impact our lives and the way we get information and control objects. Devices included in the Internet of Things can range from sensors in your shoes, to smart fitness devices, to healthcare monitors, to home automation systems (see the accompanying illustration), to smart farm equipment, to smart freeways and traffic lights. While still in the early stages, some aspects of the Internet of Things, such as smart homes and fitness PANs, exist today. As the Internet of Things matures, the connected smart devices will continue to make our lives more convenient, save us money, and provide us with other advantages. Businesses will benefit from getting feedback from equipment (being notified when a machine in the field needs service or refilling, for instance, without an employee having to physically monitor it), being able to automate more processes, and getting faster and more accurate feedback about point-of sale purchases. One concern about the Internet of Things is how best to protect the security and privacy of individuals from hackers and data leaks. That concern will likely need to be addressed before the Internet of Things becomes mainstream

COMPUTER VIRUSES AND OTHER TYPES OF MALWARE

Malware is a generic term that refers to any type of malicious software. Malware programs are intentionally written to perform destructive acts, such as damaging programs, deleting files, erasing hard drives, or slowing down the performance of computers. This damage can take place immediately after a device is infected (that is, the malware software is installed) or it can begin when a particular condition is met.

Computer viruses

A computer virus is a software program that is installed without the permission or knowledge of the computer user, is designed to alter the way a computer operates, and can replicate itself to infect any new media it has access to. Computer viruses are often embedded into program or data files (such as software, games, videos, and music files downloaded from Web pages or shared via a P2P service).



Computer worm

A computer worm is another common form of malware. A worm is designed to cause damage by creating copies of its code and sending those copies to other devices via a network. Although worms can be sent via an e-mail attachment and launched when the attachment is open, typically worms do not require any user action to infect the user's device. Instead, a worm scans the Internet looking for computers and other devices that are vulnerable to that particular worm and sends a copy of itself to those devices to infect them. Some worms are specifically written to take advantage of newly discovered security holes (vulnerabilities) in operating systems and e-mail programs before the security patch to correct that vulnerability is available; these types of attacks are called zero-day attacks. Unfortunately, the use of zero-day attacks is growing rapidly and the time required to release security patches to correct security holes is increasing. For example, a record 24 zero-day attacks were discovered in 2014 and it took 204 days, 22 days, and 53 days, respectively, to provide patches for the three most exploited vulnerabilities. Because of its distribution method, a worm can spread very rapidly and be very persistent. For example, the Conficker worm (which was originally released in 2008) quickly infected millions of computers and an estimated 1 million computers around the world are still infected today.

Trojan horses

A Trojan horse is a type of malware that masquerades as something else—usually an application program. When the seemingly legitimate program is down loaded or installed, the Trojan horse infects the device. Many recent Trojan horses masquerade as normal ongoing activities (such as the Windows Update service or a warning from a security program) to try to trick unsuspecting users into downloading a malware program or buying a useless program.

A growing type of Trojan horse is ransom ware, which either freezes up the infected device and displays a message that the device has been used for illegal activity or encrypts the victim's photos, documents, and other files located on the device and holds them hostage. In either case, the malware creator demands the user pay a fine or ransom in order to unlock the device or decrypt the files. Still other Trojan horses are spyware designed to find sensitive information about an individual or a company located on infected computers and then send that information to the malware creator. Unlike viruses and worms, Trojan horses cannot replicate themselves. Trojan horses are usually spread by being downloaded from the Internet, though they may also be sent as an e-mail attachment, either from the Trojan horse author or from individuals who forward it, not realizing the program is a Trojan horse.

Protecting Against Computer Sabotage

One of the most important protections against computer sabotage is using up-to-date security software. This and other precautions are discussed next. Security Software ANTISPYWARE SOFTWARE Security software protects devices against malware and other threats. It typically includes a variety of security features, such as a firewall; protection against viruses, spyware, and bots; and protection against some types of online fraud.

One of the most important components of security soft ware is antivirus software, which protects against computer viruses, computer worms, Trojan horses, and other types of malware. Like most security software components, antivirus soft ware typically runs continuously to monitor the device

as well as incoming messages, Web page content, and downloaded files, in order to prevent malicious software from executing. Many antivirus programs also automatically scan devices when they are connected to a USB port to ensure those devices are not infected. Antispyware software) can detect and remove spyware. Mobile security soft ware is used to protect smartphones and other mobile devices. To prevent personal devices from infecting a school or business network, schools and businesses should ensure that students and employees are using up-to-date security software. Some colleges now require new students to go through a quarantine process, in which students are not granted access to the college network until they complete a security process that checks their devices for security threats, updates their operating system, and installs security software.

HEALTH RISKS

Describe some possible physical and emotional health risks associated with the use of computers.

Since the entry of computers into the workplace and their increased use in our society, they have been blamed for a variety of physical ailments. Carpal tunnel syndrome (CTS), De Quervain's tendonitis, and other types of repetitive stress injuries (RSIs) are common physical ailments related to computer use; computer vision syndrome (CVS), eye strain, fatigue, backaches, and headaches are additional possible physical risks. ***Ergonomics*** is the science of how to make a computer workspace, hardware, and environment fit the individual using it. Using an ergonomically correct workspace and ergonomic hardware can help avoid or lessen the pain associated with some RSIs. In addition, all users should use good posture, take rest breaks, alternate tasks, and take other common-sense precautions. For portable computers, docking stations, notebook stands, and tablet stands can be used to create more ergonomically correct workspaces. The stress of keeping up with ever-changing technology, layoffs, always being in touch, fear of being out of touch, information overload, burnout, and Internet addiction are all possible emotional problems related to computer use.