Ethics

Crimes & Ethics | Personal Information | P2P File-Sharing | Computer Viruses & Malware | Computer Hacking | Computer Forensics

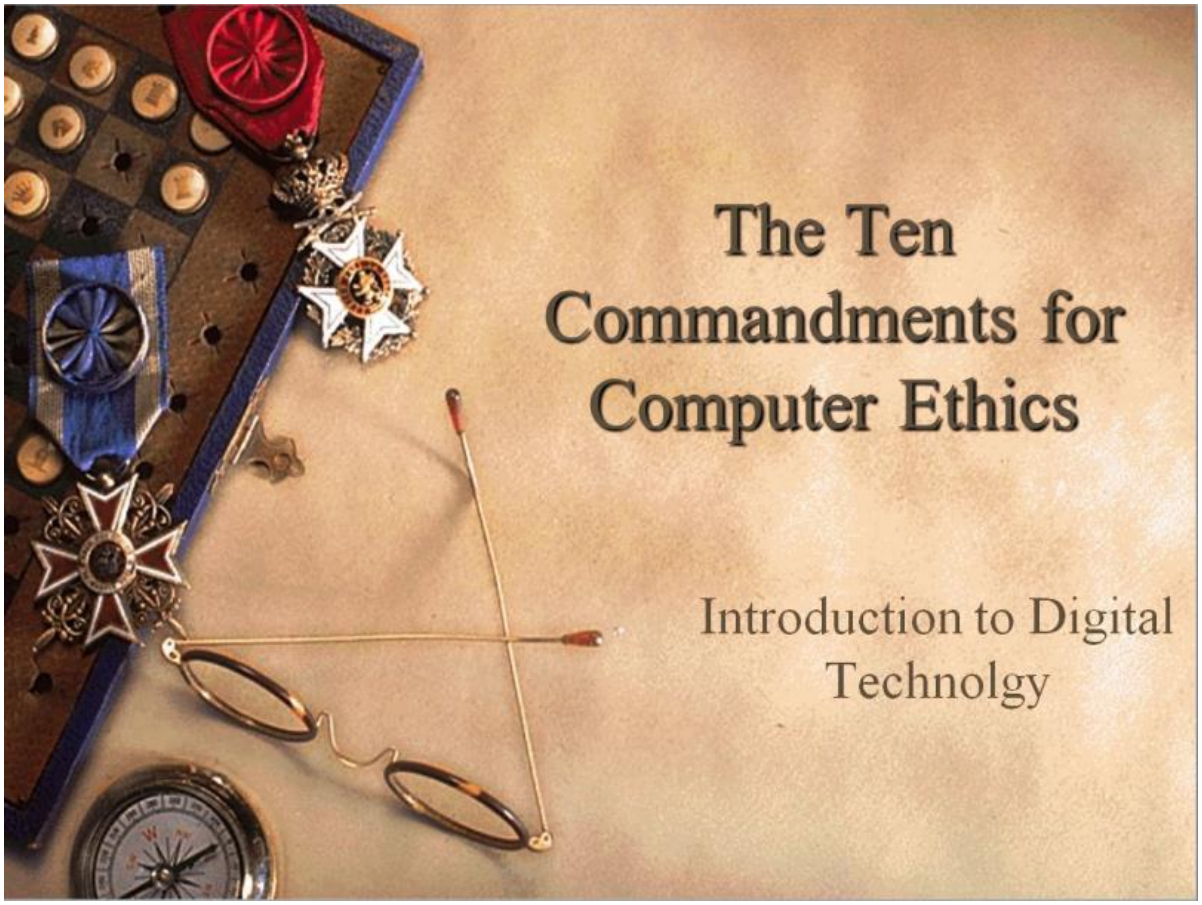
The computer, World Wide Web, and the Internet have opened up new doors to unethical and illegal activities. It has become increasingly easily to steal and victimize others via the computer. We all have an ethical responsibility to treat others with respect and to be aware and protect our own selves from unethical and illegal activities.

> "Our society is increasingly relying on new information technologies and the Internet to conduct business, manage industrial activities, engage in personal communications, and perform scientific research. While these technologies allow for enormous gains in efficiency, productivity, and communications, they also create new vulnerabilities to those who would do us harm. The same interconnectivity that allows us to transmit information around the globe at the click of a mouse or push of a button also creates unprecedented opportunities for criminals, terrorists, and hostile foreign nation-states who might seek to steal money or proprietary data, invade private records, conduct industrial espionage, cause a vital infrastructure to cease operations, or engage in Information Warfare."
>
> National Infrastructure Protection Center

Cybercrime is a bigger risk now than ever before due to the sheer number of connected people and devices. Cybercrime has surpassed illegal drug trafficking as a criminal moneymaker. Somebody's identity is stolen every 3 seconds as a result of cybercrime and without sophisticated security software; your unprotected PC can become infected within 4 seconds of connecting to the Internet. *Norton by Symantec*

In 2013, global cyber had an estimated cost of $300 billion to $1 trillion or 0.4% to 1.4% of the world's Gross Domestic Product (GDP). *McAfee*

Ellen Messmer, for Network World, wrote in her article Annual cost of cybercrime hits near $400 billion, that the losses are rising and the United States, China, and Germany are feeling the greatest lost from cyber-espionage theft of intellectual property, plus all types of personal and financial data stolen and dealing with the fallout.



Click on the picture to watch the presentation

Assignment: Computer Ethics in Real Life

Directions: Find a newspaper or magazine article or story, or a story from a reliable news site on the Internet, that shows an application (or lack of application) of at least one of these commandments. It can be of national interest, local interest, or personal interest. It must be fairly current (within the last five years.) Type a summary (one full page) explaining which commandment specifically applied to that situation and why. If more than one of them applied, explain which ones do and why. Download the full assignment from itsLearning.

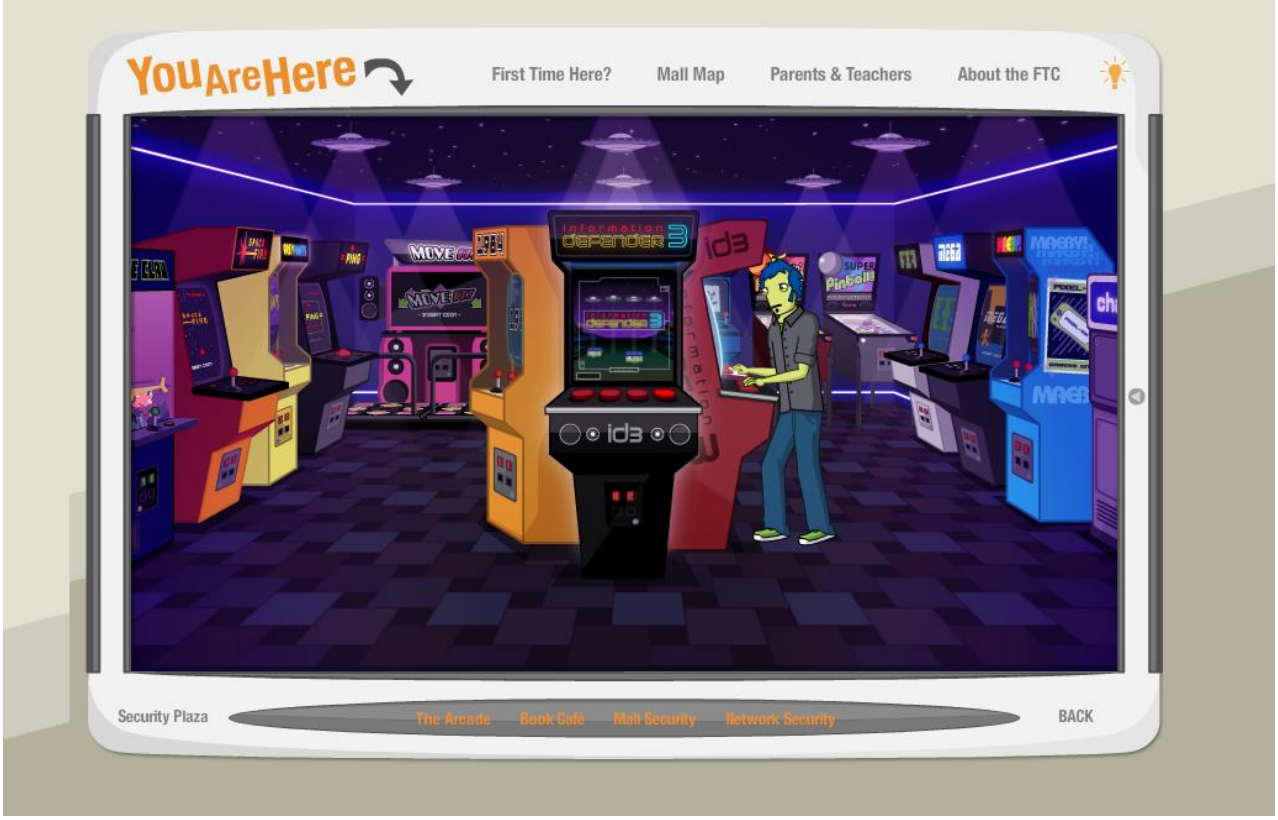
Personal Information

Online shopping, social networking, job hunting and the ability to carry out official functions such as renewing car tags or contacting local or contacting local councils and government departments online, are now an everyday part of life. Doing things online can offer convenience and widen opportunities, and in general people value it resulting in more and more people are conducting their personal affairs online.

Emily asks visitors for help designing her online profile. Find out the consequences of posting personal information online and get tips about when it's appropriate to share.

Click on the picture to enter the mall. Go to the Security Plaza and then enter Book Cafe'

At the arcade, visitors defend against Cyclorean space invaders who want to steal Earthlings' personal information. They also learn why their personal information is valuable and what's so important about a Social Security number.



Click on the picture to enter the mall. Go to the Security Plaza and then enter The Arcade

Identity Theft

Millions of Americans have fallen victim to identity theft. According to the Federal Trade Commission, it's the country's fastest-growing crime. Identity theft is a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity, usually as a method to gain access to resources or obtain credit and other benefits in that person's name. The victim of identity theft (here meaning the person whose identity has been assumed by the identity thief) can suffer adverse consequences if they are held responsible for the perpetrator's actions. Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.

Identity thieves get your personal information by:

- Stealing wallets, purses and your mail
- Stealing personal information you provide to an unsecured site on the Internet
- Stealing personal information on business or personnel records at home
- Stealing information from your home

- Gong through your trash or recycling at home, trash at business, or public trash dumps
- Posing by phone or email as someone who legitimately needs information about you, such as employers or credit card company representative
- Buying personal information from ‘inside’ sources

Consumers use their credit cards and debits cards on a daily basis. Those cards contain personal and financial information. Several big name companies like Target and Michaels have experienced data security breaches. Retail giant Target exposed credit card numbers and personal information of as many as 110 million people in November 2013. As a result, several people have had their credit stole or become victims of identity theft.

Will’s laptop has been stolen! At the security office, visitors learn who stole it, and find out what a stolen laptop has to do with identity theft. They also can ask questions about identity theft and learn how to avoid it.

Click on the picture to enter the mall. Go to the Security Plaza and then enter Mall Security

Assignment: Protecting Your Personal Information Infographic

Directions: Most teenagers don't think anything about sharing their personal information online. Create an infographic of the dos and don'ts of sharing personal information.

P2P File-Sharing

To share files, like games and music, through a peer-to-peer (P2P) network, you download software that connects your computer to other computers running the same software' sometimes giving access to millions of computers at a time. This has a number of risks. You could mistakenly

- download malware, pirated or copyrighted material, or pornography
- allow strangers to access and share your personal files

If you are considering P2P file-sharing, understand the inherent risks and take these steps to help minimize them.

- Install reputable security software
- Limit what you share and how often
- Talk to your family
- Understand file-sharing policies

Click on the picture to play the game

Is it okay to make a copy of software that you purchase and give it to a friend? Generally, the answer is going to be "no." When you purchase software, you are purchasing a single copy for your own use and to make copies for other people (even when you don't charge them) would be in violaton of the copyright agreement. However, you shoudl read the End User License Agreement (EULA) to find out the details of any restrictions.

While you are too young to remember *Napster*, here is where illegal free P2P files-haring gained the lime light. The digital music revolution started with Napster the file-sharing service dreamt up by two teenagers in 1999. Read Tom Lamont's article, Napster: the day the music was set free in *The Observer* to gain a greater perspective on illegal P2P file-sharing and copyright infringement.

Assignment: Napster Article Review

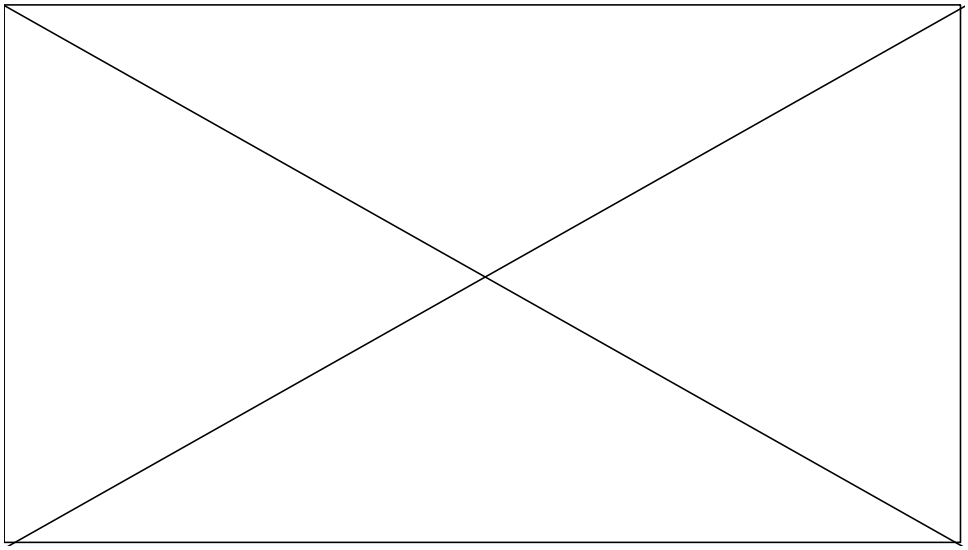
Directions: After reading the article Napster: The Day the Music was Set Free, answer the review questions in itsLearning.

Assignment: P2P PSA

Directions: Create a Public Service Announcement (PSA) of the risks of P2P file-sharing and how you can minimize the risk to yourself and others.

Computer Viruses & Malware

Malware is short for “malicious software." It includes viruses and spyware that get installed on your computer or mobile device without your consent. These programs can cause your device to crash and can be used to monitor and control your online activity. Learn more about how to avoid, detect, and get rid of malware.



People who write viruses do so mostly because they can! A virus is simply a computer program written with a dangerous or disastrous payload for the unsuspecting victim. Malware can be simply annoying such as pop up ad or it could wipe your entire hard drive or insert itself into your boot sector. A virus can send itself to everyone in your email address book posing as you. A keylogger virus can capture every keystroke you make on a keyboard thus capturing log in and password or credit card details all while you have no idea what is going on.

The most common way that viruses are spread is through email and downloading infected files from the Internet. You should never open email from people you do not know and be cautious of emails from people that you do know that just don't sound right. Always have virus protection installed on your system but utilize good common sense at the same time.

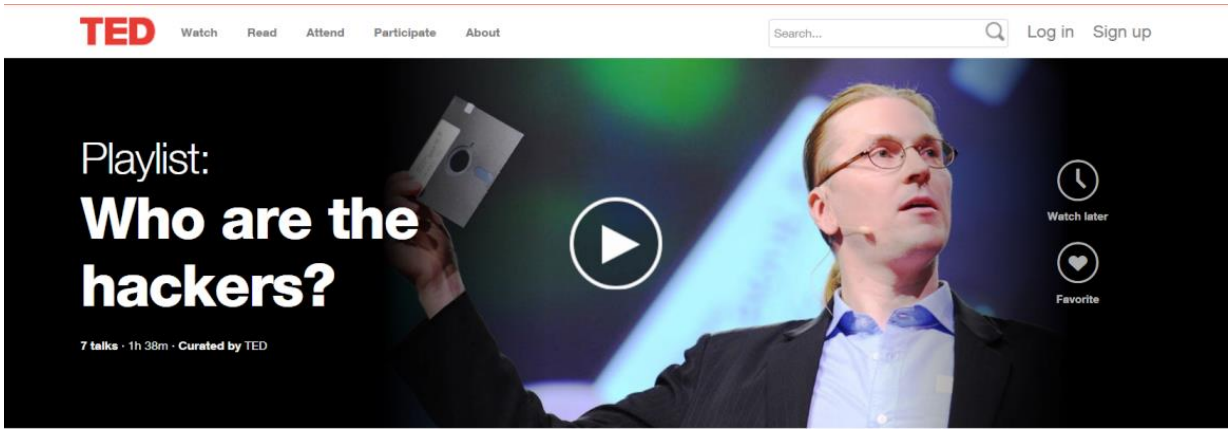
"Your computer files are being held for ransom. Pay up, or lose them. Your bank account is being emptied, click here to stop it. Your friend has died, click on this funeral home site for more information. Social engineering thugs have reach new lows" *Stacy Collett, CSO magazine*

Four despicable new attacks play on user's fear of privacy loss, theft, and even death:

- More potent ransomware: Ransomware caught the attention of businesses in 2013 when Cyptolocker (virus) held computer files hostage by encrypting them with strong RSA-2048 key encryption. The virus originators offer the encryption key in exchange for $500+.
- Robocalls for credit card information
- Phishing with healthcare records
- Phishing with funerals

It's been 25 years since the first PC virus (Brain A) hit the net, and what was once an annoyance has become a sophisticated tool for crime and espionage. Computer

security expert Mikko Hyppnen tells us how we can stop these new viruses from threatening the internet as we know it. The Internet connects us as never before, but there's a dark side to this web. Who are the hackers who wreak havoc online? And what is it they want? Sociologists, criminologists and hackers themselves shed light …



Click on the picture to watch the video: Fighting viruses, defending the net

Other dangers you should be aware of, include:

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies.

Phishing Facts

- 6.1 billion phishing emails sent world-wide each month.
- $1,200 is the average loss to each person successfully phished (FTC)
- 42,890 unique phishing attacks reported in December 2013 (Anti-Phishing Working Group)
- 42,890 phishing Web sites detected in December 2013 (Anti-Phishing Working Group)
- United States is the country hosting the most phishing sites (Anti-Phishing Working Group)

The most targeted industry sector for phishing attacks is payment services, making up 53.95% of phishing attacks. Trojan infections have reached record levels, accounting for almost 80 percent of all infections according to the Anti-Phishing Working Group. Be suspicious of any email with urgent requests for personal financial information Avoid

filling out forms in email messages that ask for personal financial information. Your Internet Service Provider, financial institution, or other websites with secure log in **will never** email you and request your login and password. If you receive an email with a link to access your account in any way. Close the email and login into the password secured website like you normally do. You have probably been phished and those emails look **very** legitimate!

Pharming is a cyber attack intended to redirect a website's traffic to another, bogus site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in domain name system (DNS) server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers are sometimes referred to as "poisoned". Pharming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server. Visit Norton by Symantec to read more about Online Fraud: Pharming.

Assignment: Virus Case Study

Directions: Read the article about CrypoLocker (full article in itsLearning), a particularly nasty Trojan horse that is currently circulating. After you have read about CryptoLocker, assume you work in the IT department of your company. Write a memo explaining to the staff what CryptoLocker is and how they should protect their data (this is not a copy and paste assignment. You must summarize in your own words.) Here is a short video on how to prepare a memo.

Computer Hacking

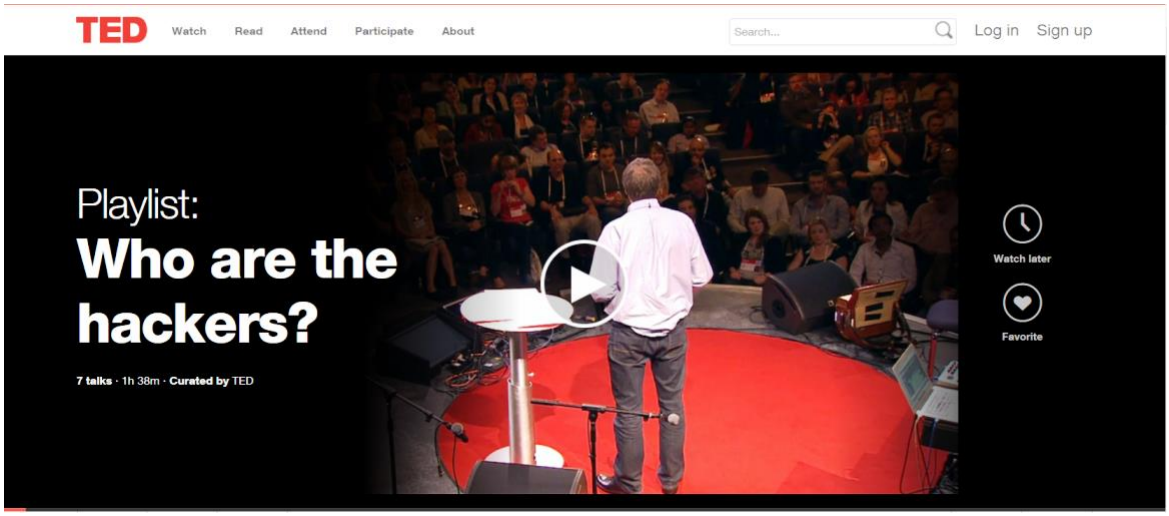
Hacking is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose. The person who is consistently engaging in hacking activities, and has accepted hacking as a lifestyle and philosophy of their choice, is called a hacker. Computer hacking is the most popular form of hacking in today's society, especially in the field of computer security. Computer security specialists learn hacking techniques so they can prevent breaches in computer security.

People who hack computers do so with a variety of motivation including fun, profit, espionage, psychological needs, extortion, revenge, exposing system weaknesses, technical reputation and proficiency, problem solving, and see games as life. Hackers

first appeared in the 1960's and it was mostly done for fun, just to see if they could hack a computer system. Today's hackers steal company information and personal information, deny services, deface websites, and shut down entire companies and governments to name just a few.

The 1983 movie *WarGames* demonstrated hacking by two teenagers. The film follows David Lightman, a young hacker who unwittingly accesses WOPR, a United States military supercomputer programmed to predict possible outcomes of nuclear war, through a backdoor. Lightman gets WOPR to run a nuclear war simulation, originally believing it to be a computer game. The simulation causes a national nuclear missile scare and nearly starts World War III.

Despite multibillion-dollar investments in cybersecurity, one of its root problems has been largely ignored: who are the people who write malicious code? Underworld investigator Misha Glenny profiles several convicted coders from around the world and reaches a startling conclusion.



Click on the picture to watch the video: Hire the Hackers!

While hacking itself can be considered a crime and certainly questions ethics, is all hacking bad? Is there an actual career opportunity for computer hacking for the good? There are black hat hackers such as those described in the paragraph above and then there are white hat hackers as you will see in the video *Hackers Outlaws and Angels*.

Assignment: Hackers Outlaws and Angels summary

Directions: Summarize the Hackers Outlaws and Angels video in a short (200-300 words) essay.

Computer Forensics

Computer forensics is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information. Although it is most often associated with the investigation of a wide variety of computer crime, computer

forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

Computer professionals can get certified in computer forensics. The top five certifications are:

- Digital Investigations
- Certified Computer examiner (CCE)
- Certified Hacking Forensic Investigator
- Certified Forensic Computer Examiner (CFCE)
- GIAC Certified Forensic Analyst and Forensics Examiner

You can read Ed Tittel and Mary Kyle's full article, Top 5 Computer Forensics Certifications.

Resources

If you are having problems viewing this page, opening videos, or accessing the URLs, the direct links are posted below. All assignments are submitted in itsLearning. If you have having problems, contact Mrs. Rush through the itsLearning email client.

Phishing Statics: http://docs.apwg.org/reports/apwg_trends_report_q4_2013.pdf

The Ten Commandments for Computer Ethics: http://www.mrsrush.net/idt/ethics/ten.pdf

Book Cafe: http://www.consumer.ftc.gov/sites/default/files/games/off-site/youarehere/site.html#/book-cafe

The Arcade: http://www.consumer.ftc.gov/sites/default/files/games/off-site/youarehere/site.html#/the-arcade

Mall Security: http://www.consumer.ftc.gov/sites/default/files/games/off-site/youarehere/site.html#/mall-security

P2P ThreePlay: http://www.onguardonline.gov/media/game-0010-p2p-threeplay

Napster, the Day the Music was Set Free: http://www.theguardian.com/music/2013/feb/24/napster-music-free-file-sharing

Protect Your Computer from Malware video: http://bcove.me/c8do6mdo

Fighting Viruses, Defending the Net video: http://www.ted.com/playlists/10/who_are_the_hackers

Sheldon Gets Hacked on World of Warcraft video: http://youtu.be/FmxEB-hZ_Ck

Hire the Hackers video: http://www.ted.com/playlists/10/who_are_the_hackers

Hackers Outlaws and Angels video: http://youtu.be/pLty-2U4BXs

Computer Forensics video: http://science.howstuffworks.com/34008-solved-computer-forensics-video.htm

Transcript: http://mrsrush.net/ethics/index.pdf

Credits

Collett, Stacy (2014, June). *Scammers Reach Cruel New Lows*, CSO Magazine.

Transcript of this lesson