What is a cybercrime?

Criminal.findlaw.com defines cybercrimes as criminal offenses committed via the Internet or otherwise aided by various forms of computer technology, such as the use of online social networks to bully others or sending sexually explicit digital photos with a smart phone.

With attacks online becoming more common, we are going to take a reading, and then answer a few questions about the topic. Reading Below:

Cyber Crime

Cyber-crime is one of the fastest growing crimes in the world. Frequent users of the internet buy things from online shopping platforms, perform online banking, and store their files on a ‘cloud’. These events provide endless opportunities for cyber criminals who take advantage of the weaknesses of others.

More than 70% of all Americans have experienced some form of cyber-crime in their lives. Most of these illegal online activities are hard to detect and solve. In many cases, victims of cyber-crime do not even realize that something illegal or illegitimate has taken place.

Basically, there are three types of cyber-crime:

- Harassment – Some people use the Internet anonymously and are engaged in illegal activities like stalking, harassment, and bullying.

- Hacking – Hackers break into online networks and try to corrupt or download all kinds of sensitive or valuable information.

- Phishing – Phishing is the activity of sending emails to people trying to trick them. The purpose of phishing is to obtain money from the recipients of these emails. Usually, the elderly, who are not very computer savvy are the most vulnerable groups for this kind of crime.

Anonymous

Anonymous is a group of hackers that is famous for their distributed denial-of-service (DDoS) attacks. They target organizations such as governments and large companies. A DDoS attack is a process in which many computer systems attack a single target, such as a website or a server. The enormous number of incoming messages (attacks) slow down the server so that it cannot be used anymore.
ASSIGNMENT 1:

Exercise 13: Are the statements below true or false?

1) Cyber-crime is the most common crime in the world. ( )
2) Online bullying is a cyber-crime. ( )
3) More than half of the American population has been affected by cyber-crime. ( )
4) Cyber-crimes are hard to detect and solve. ( )
5) Inexperienced Internet users are more vulnerable to cyber-crime. ( )
6) Hackers try to trick and harass people online. ( )
7) More than 70% of all Americans are bullied on the Internet. ( )
8) Phishing is the attempt of trying to acquire sensitive information. ( )

1) Why do you think it is so difficult to catch and prosecute cyber criminals?

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

5) What is Anonymous?

________________________________________________________________________
________________________________________________________________________

2) Have you ever been a victim of an online crime? If so, can you please describe the situation in detail?

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

6) What is a DDoS attack and how does it work?

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

3) Have you ever done something that is not allowed on the web? If yes, what was it and why did you do so?

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

4) Which cyber-crime do you think is the most dangerous? Give reasons to justify your answer.

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
DAY 3

Today we are going to talk about a particular type of cybercrime; scammers. Today’s assignment will bring light to a small portion of this. Remember, never give your info over the phone or via email, as real companies would never ask for these things.

Mr. Sabo rant: I recently had a friend nearly get scammed. Someone knew his email address and his phone number, probably via phishing or purchasing his information. What they did was went to Amazon.com, typed my friends email in then hit ‘forgot password.’ A button appeared on the screen that said ‘send code to this phone number ***-***-3653.’ What the scammer does next is calls my friend and pretends to be an employee of Amazon and told him that his account has been compromised, and he would be sending him a code to confirm it was him. As soon as he said he would send a code, he clicked the ‘send code to this phone number ***-***-3653’ button and my friend received the code, and told the guy over the phone what his code was. Just like that, the scammer had reset my friend’s password and locked him out of his account. Luckily at that point my friend smelled something and went to log in to his account to find it locked out and called Amazon right away, and things were cleared up. This is just to show how sneaky they can be, and to never give away even what may seem a harmless code.

ASSIGNMENT 2:

Complete the questions below. Many are designed for you to think about the topic, and may not have an exact answer, rather I want you opinion or what you think about things.

1. What would you do if you received the following email?

   From: Euro-International State Lottery
   Re: [Anti-spam]: Congratulations!

   We are delighted to inform you that your name has been selected by our computer and that you are a winner in our Lottery of the sum of €200,000. We shall forward the contact information of the bank which will enable you to claim the funds. Please be aware that there are some important documents that will be required by the bank to activate the transfer. Please contact us urgently to guarantee safe receipt of your winnings. Congratulations!

2. Which of the following terms do you know? If you know or have an educated guess, please do so.
   a. Spam
   b. Adware
   c. Spyware
   d. Scam
   e. Fraud
3. Read the article below, and count how many times the above words (and their derivatives, i.e. scammer, fraudsters) appear.

**Hi-tech fraud** Both the US and the UK are experiencing a rise in ‘phishing’, pronounced ‘fishing’. Fraudsters send an e-mail message that seems to come from a bank (Citibank, Lloyds) or a company like E-bay or Amazon. The message looks genuine, and may direct you to a website which includes a corporate logo. You are asked to send or confirm personal information, such as your bank account number or password. This information is then used for fraudulent activity, such as online gambling, or to siphon off money from your account. As many as 20% of recipients are fooled by this scam.

This is another example of spamming. The nature of spam is changing from being just a nuisance to more serious financial scams. Many mails sell fake pharmaceuticals on the black market. Financial and pharmaceutical spam now make up an incredible 70% of all spam.

IT managers estimate that over 90% of computers in organisations have been infected by some kind of spyware. Many employees unknowingly download spyware onto their machines. This software, which hides somewhere in your computer, collects information about you and what you do on the internet – it may even record your credit card details if you shop on the Internet. On average every PC has 28 so-called spyware programs installed on it, according to one recent audit by a software firm.

Adware is a form of spyware which installs secret advertising software on your computer, such as annoying pop-up ads. There are government moves in various countries to make spam illegal. As the Internet becomes more and more an integral part of our lives so we have to give more time to protecting ourselves against cyber-crime.

4. Tell me two things you did not know and/or found surprising.

5. Find the words in the text to fit the definitions below:
   a. to move money from one bank account to another illegally or dishonestly (paragraph 1)
   b. a symbol that represents an organization or company (paragraph 1)
   c. risking money, often in a game, hoping to win more if you are lucky (paragraph 1)
   d. made to look like something real in order to trick people (paragraph 2)
   e. an official examination of a situation within a company (paragraph 3)

6. Rank the following crimes in order of their seriousness. Decide on a suitable penalty for each.

   sending spam e-mails  
   manufacturing / selling fake drugs  
   placing spyware on a computer  
   sending adware across the Internet  
   creating / distributing a computer virus  
   stealing credit card details