HELLO EVERYONE

COMPUTER CRIME

Q.LIST THE TYPES OF CRIMES AND CYBERCRI

A.1.Phishing: using fake email messages to get personal information from internet users;

2.Misusing personal information (identity theft);

3.Hacking: shutting down or misusing websites or computer networks;

4.Spreading hate and inciting terrorism;

5.Distributing child pornography;

6. Theft and sale of corporate data.

Q.LIST TYPES OF COMPUTER CRIMINALS?

A.1.Hacking.

2. Virus dissemination

3.Logic bombs.

4. Denial-of-Service attack

5.Phishing.

6. Email bombing and spamming.

7.Web jacking.

8. Cyber stalking.

9. Data diddling.

Q.DESCRIBE HOW TO PROTECT YOUR COMPUTER AND YOURSELF?

A.1. Make sure that you have antivirus software installed on your computer.

2.Schedule weekly virus definition updates so that your software is able to catch the latest viruses.

3.Schedule weekly scans of your hard disks so that the software can find viruses before it infects your system.

4.Make sure that automatic protection is enabled so that the program is constantly looking for viruses as soon as you turn on your computer.

5.Make sure that the program is compatible with your email program so that it can immediately detect and block viruses in email attachments.

6. Run a full scan on your computer with your antivirus software. If a virus is detected your antivirus software will either clean, delete or quarantine the file.

7. If the virus can't be removed by your antivirus software you can find removal tools specific to the type of virus by going to the software manufacturer website (ie, McAfee, Symantec, etc).

Q.DEFINE ENCRYPTION?EXPLAIN HOW TO SECURE YOUR ONLINE INFORMATION?

A. Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as ciphertext, while unencrypted data is called plaintext.

There are 8 steps to secure your online information:

1.Avoid clicking on links or attachments:

Cybercriminals do a good job of tricking people into clicking on links supposedly from their bank, telecom operator, electric or gas company, tax service and other legitimate organisations. Think before you click – spelling errors, email addresses that don’t seem right,

2. Passwords are the keys to your digital kingdom:

Use unique, complex passwords with a combination of lower and upper-case letters, numbers and symbols and do not use the same password across your accounts.

3. Keep your identity safe:

Don't share passwords or choose one that can be easily guessed. Make sure to change them often. And where possible, use two-factor or strong authentication which combines something you know.

4.Back-up your data:

If your computer is infected by ransomware, malware or it crashes, the only way to definitely ensure that you will be able to retrieve your lost data is by backing it up and doing so on a regular basis.

5. Verify the web site you are on is safe:

before entering your payment details into any web site, check that the URL begins with https – the “s” stands for “secure.

Q. Describe the issues the government face when balancing the need for decrypting data and public rights to privacy?

A. Privacy and the Internet have a complex relationship. On the one hand, technology has enhanced privacy by offering more accessible means to communicate and access information. For example, activities that once required in-person visits to banks, post offices, libraries, shops and doctors' offices can now be carried out alone from the sanctity of home. Accompanying advances in encryption have made many online transactions and interactions increasingly secure .

Q.DISTINGUISH BETWEEN ELECTRONIC AND COMPUTER FORENSICS?

A.E-Discovery:

It is a term rooted in the American civil legal system and refers to the stage prior to a trial when a request is made by one party that the other hand over any and all archived electronic material that they hold in relation to the case. This will include emails, word processing documents, spreadsheets and other data. e-discovery involves the process of sifting through huge amounts of ‘raw’ data to remove duplicates (called ‘de-duping’) and useless information.

2.Computer Forensics:

Computer forensics, also known as digital forensics, on the other hand is a much more specific discipline, which involves the analysis of computers and other electronic devices in order to produce legal evidence of a crime or unauthorised action.

While e-discovery is essentially a process of organising data, computer forensics is a considerably more complex process which involves highly technical procedures such as ‘data carving’: the act of looking for flags in un-indexed, raw data which suggest the start and end of a block of data so that a single deleted file can be reassembled.

Q.UNDERSTAND THE COMPUTER SECURITY RISKS OF USING COMPUTER AND INTERNET?

A.1. Computer Viruses

Perhaps the most well-known computer security threat, a computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to your computer in the process. Carefully evaluating free software, downloads from peer-to-peer file sharing sites, and emails from unknown senders are crucial to avoiding viruses.

2. Spyware Threats

A serious computer security threat, spyware is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information. We've amassed a wealth of knowledge that will help you combat spyware threats and stay safe online

3. Hackers and Predators

People, not computers, create computer security threats and malware. Hackers and predators are programmers who victimize others for their own gain by breaking.into computer systems to steal, change, or destroy information as a form of cyber-terrorism. These online predators can compromise credit card information, lock you out of your data, and steal your identity.

4. Phishing

Masquerading as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Phishing attacks are some of the most successful methods for cybercriminals looking to pull off

A data breach.

Q.THE EFFECT OF TECHNOLOGY DEVELOPS ON PRIVACY AND ANONYMITY?

A. Technology thus does not only influence privacy by changing the accessibility of information, but also by changing the privacy norms themselves. For example, social networking sites invite users to share more information than they otherwise might. This “oversharing” becomes accepted practice within certain groups.

THANK YOU ……..

BY:RABI AHMED

REFERENCE BY:

WWW.researchgate.com

www.pandasecurity.com

www.kaspersky.com