PRIVACY CRIME AND SECURITY

TYPES OF COMPUTER CRIMINALS

Hackers, crackers, cybergangs, virus authors, swindlers, shills, cyberstalkers, cyberbullies and sexual predators

---

TYPES OF COMPUTER CRIMES AND CYBERCRIMES

identity theft; malware, including spyware and viruses; other rogue programs such as time bombs, logic bombs, worms, botnets, zombies, and Trojan horses; fraud and theft; password theft salami shaving and data diddling; forgery; black-mail; cyberstalking and cyberbullying; and Inter-net crimes like shilling, rip and tear, pump and dump, and bogus goods

HOW TECHNOLOGY DEVOLEPMENT AFFECT PRIVACY AND ANONYMITY

Cookies Generally downloaded into folders that hold temporary Internet files
banner ad targeted to match the topic or type of products you were browsing through
A globally unique identifier (GUID) is an identification number that is generated by a hardware component or a program
ubiquitous computing It refers to a trend in which individuals no longer interact with one computer at a time but instead with multiple devices connected through an omnipresent network
radio frequency identification: are often used, as an alternative to bar codes, for inventory control in the retail environment

SECURITY RISKS OF USING COMPUTER AND INTERNET

Wireless Networks

Corporate Espionage

Information Warfare

Security Loophole Detection Programs

Public Safety

DESCRIBE HOW TO PROTECT YOUR COMPUTER AND YOURSELF

Power-Related Problems

Controlling Access

Firewalls

Avoiding Scams

Preventing Cyberstalking

DEFINITION OF ENCRYPTION

Encryption is the process of converting data to an unrecognizable or "encrypted" form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet.

HOW IT MAKES ONLINE INFORMATIONS SECURE

Encryption is the process of taking plain text, like a text message or email, and scrambling it into an unreadable format — called “cipher text.” This helps protect the confidentiality of digital data either stored on computer systems or transmitted through a network like the internet.

When the intended recipient accesses the message, the information is translated back to its original form. This is called decryption.

To unlock the message, both the sender and the recipient have to use a “secret” encryption key — a collection of algorithms that scramble and unscramble data back to a readable format.

THE ISSUES THAT THE GOVERNMENT FACE WHEN BALANCING THE NEED FOR DECRYPTION DATA AND THE PUBLICE RIGHTS TO PRIVACY

The U.S. government continues to look for ways to balance the government's need to know with the public's right to privacy. The government recently released a new random-number standard, a critical component of encryption methods. However, a backdoor was discovered that could enable some-one to crack the code, compromising the security of this encryption and obtaining confidential information. The U.S. government understands the importance of encryption and the need to collect information, but within the limits of retaining the privacy of its citizens

DISTINGUISH BETWEEN E-DISCOVERY & COMPUTER FORENSICS

Electronic discovery is the exchange of electronic documents. Computer forensics, a branch of forensic science, examines hardware and software to detect cybercrime. Both facilitate the detection , apprehension, and conviction of cybercriminals.

THANK YOU