cybercrimes

EmtinanTobuli

COMPUTER CRIMES

- **computer crimes, computer-based activities that violate state, federal, or international laws. Cybercrime describes crimes carried out by means of the Internet.**

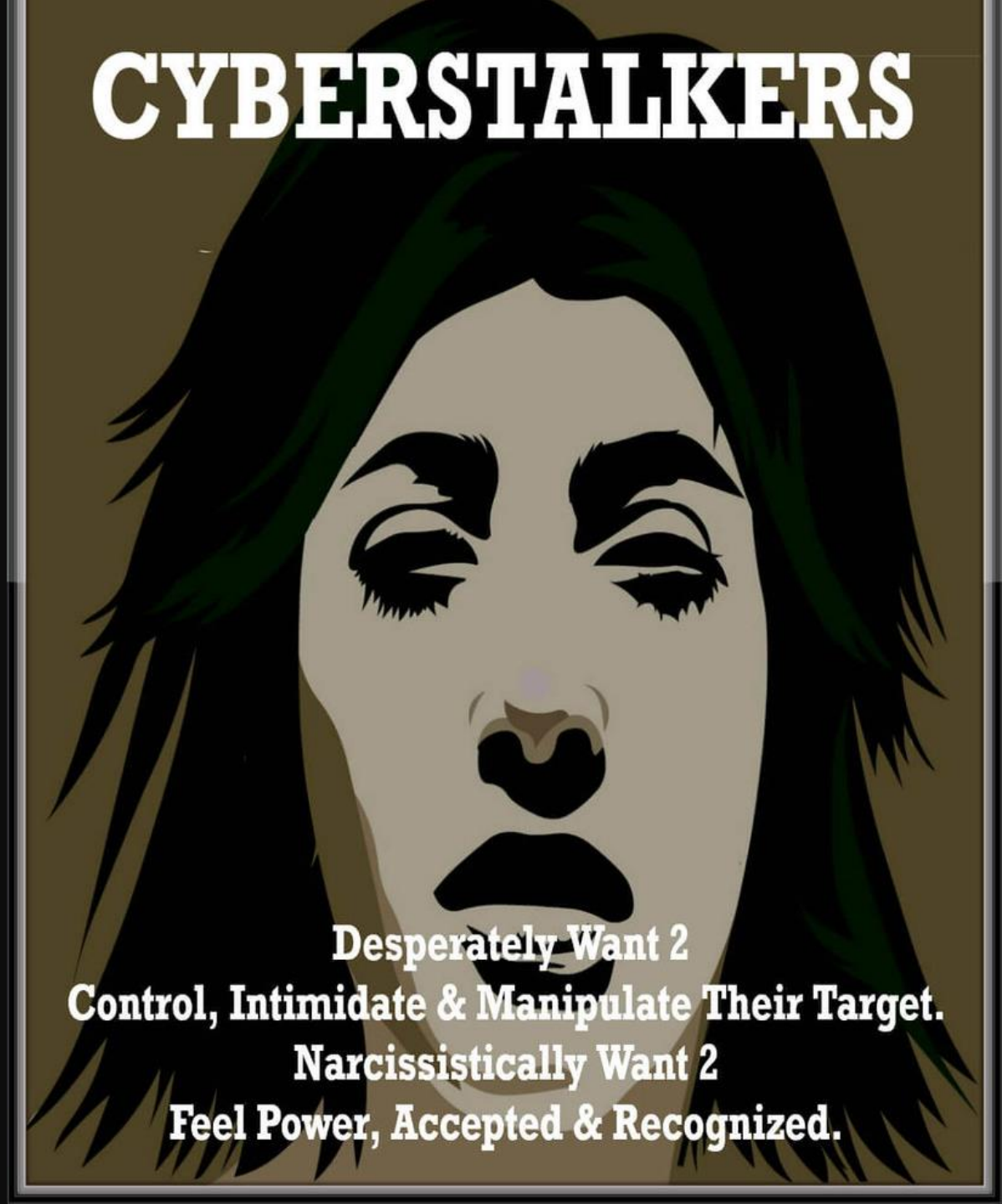
TYPES OF COMPUTER CRIMES

1. **Identity Theft :** a criminal obtains enough personal information to impersonate you. With key pieces of information, such as your address and Social Security number, credit card or bank account number
2. **Spear phishing:** uses fake e-mails to trick recipients into providing personal information to enable identity theft. But NOT sent randomly, spear phishing attempts are targeted to specific people, such as members of a particular organization.
3. **MALWARE:** short for malicious software designed to damage or infiltrate a computer system. used to commit fraud, send spam, and steal your personal data it includes spyware and computer viruses, another rogue programs like worms and Trojan horses .

- A computer virus is hidden code that attaches itself to a program, file, or e-mail message referred to as a host.
- Rogue Programs Spyware and viruses aren't the only types of rogue programs. Other destructive programs include time, logical bombs, worms, zombies, Trojan horses, and botnets.
- Fraud, Theft, and Piracy -Cybergaming Crime

TYPES
OF COMPUTER CRIMINALS

- **Hackers**
- **Crackers**
- **cybergangs**
- **Virus Authors**
- **Cyberstalkers**
- **Sexual Predators**
- **Cyberbulling**



HOW TECHNOLOGY DEVOLPMENT PUTS PRIVACY AND ANONYMETY AT RISK

- **technology makes it increasingly difficult for citizens to engage in anonymous speech. Anonymity refers to the ability to convey a message without disclosing your name or identity.**
- Examples of technologies that threaten online anonymity include cookies, global unique identifiers, ubiquitous computing, and radio frequency identification
- **Cookies:** Generally downloaded into folders that hold temporary Internet files, cookies are small text files that are written to your computer's hard disk by many of the Web sites you visit.
- **A globally unique identifier (GUID):**is an identification number that is generated by a hardware component or a program can be read by Web servers or embedded in various documents, identifying the computer and inadvertently making it more difficult to use the Internet anonymously
- **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:** The use of radio waves to track a chip or tag placed in or on an object is referred to as radio frequency identification (RFID)
- What troubles privacy advocates is the use of tracking cookies to gather data on Web users' browsing and shopping habits— without their consent. Several Internet ad networks, such as DoubleClick, use cookies to track users' browsing actions across thousands of the most popular Internet sites.

PROTECT YOUR COMPUTER SYSTEM

1-Power-Related Problems: caused by lightning storms or fluctuations in electrical currents, which can destroy sensitive electronic components and cause data loss using

uninterruptible power supply (UPS): a battery-powered device that provides power to your computer for a limited time when it detects an outage or critical voltage drop

2-Controlling Access: in addition of **password authentication**, using **know and-have authentication** requires using tokens, which are handheld electronic devices that generate a logon code The most secure authentication approach is **biometric authentication**

3-Firewall: is a computer program or device that permits an organization's internal computer users to access the external Internet but severely limits the ability of outsiders to access internal data it can be implemented through software, hardware, or a combination of both.

PROTECT YOURSELF

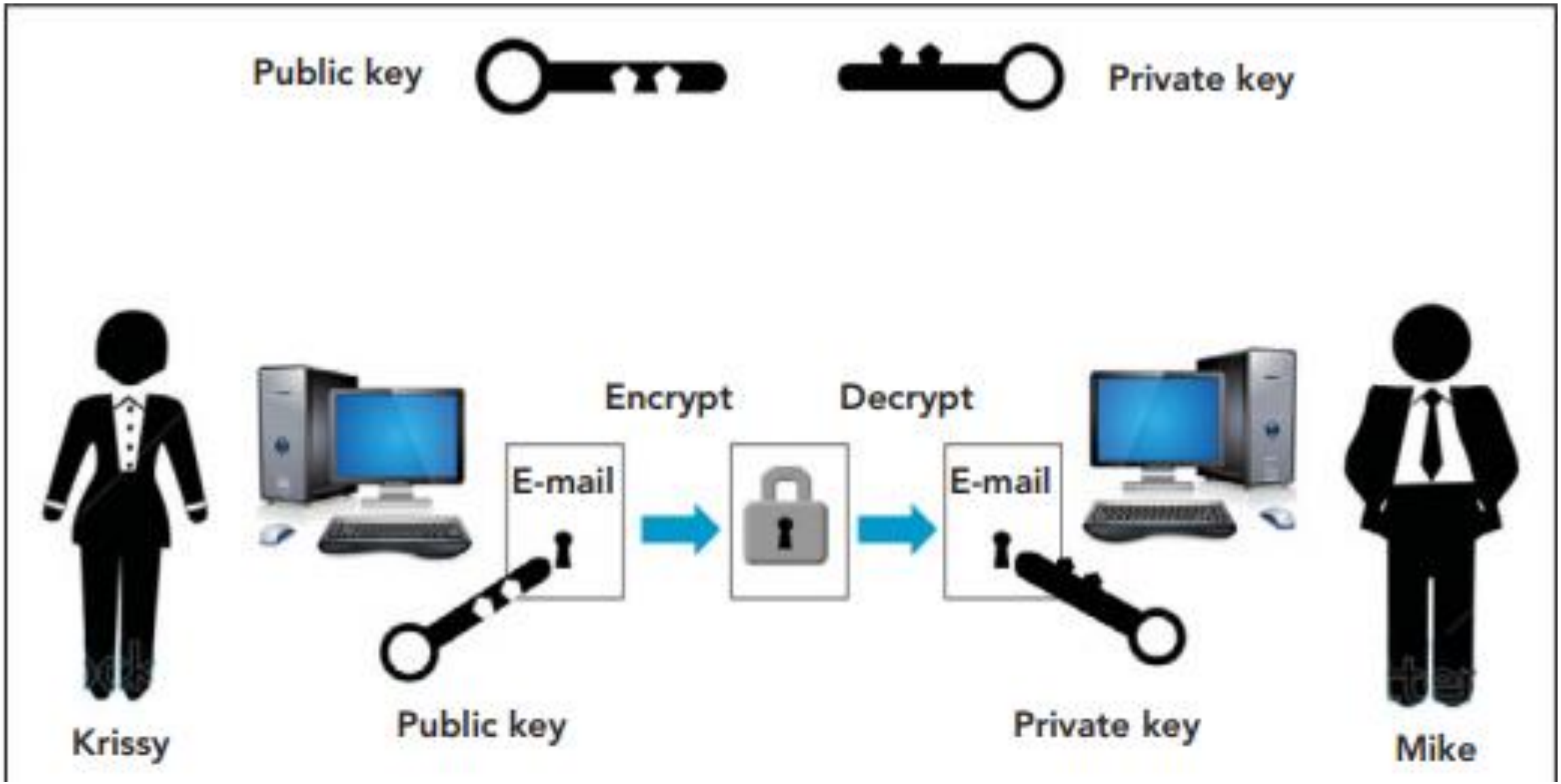
- **Avoiding Scams** To avoid being scammed on the Internet, follow these tips:
- Do business with established companies
- Read the fine print. If you're ordering something
- Don't provide financial or personal information or passwords
- Be skeptical when somebody in an Internet chat rooms.

- **Preventing Cyberstalking** To protect yourself against cyberstalking, follow these tips:
- Don't share any personal information.
- Be extremely cautious about meeting anyone you've contacted online.
- If a situation online makes you uncomfortable or afraid, contact the police immediately.

Encrypting and how it makes online information secure

- Cryptography is the study of transforming information into an encoded or scrambled format cryptographers. Encryption refers to a coding or scrambling process that renders a message unreadable by anyone except the intended recipient

- E-commerce for example requires strong, unbreakable encryption; otherwise, money could not be safely exchanged over the Internet. But now, powerful encryption software is available to the public which allows Criminals, including drug dealers and terrorists, can use encryption to hide their activities.


Public key
Private key
Encrypt
Decrypt
E-mail
E-mail
Public key
Private key
Krissy
Mike

The government issues in balancing the need of access and privacy:

- The government’s need to know often conflicts with the public’s right to privacy. Recently, the government released a new random-number standard, a critical component of encryption methods. It consisted of four random-number generators **A backdoo**r, a method of bypassing normal authentication to secure access to a computer. However, a backdoor was discovered that could enable someone to crack the code, compromising the security of this encryption and obtaining confidential information.

E-discovery and Computer forensics

- **E-discovery:** an abbreviated term for electronic discovery, is the obligation of parties to a lawsuit to exchange documents that exist only in electronic form, including e-mails, voicemails, instant messages, e-calendars, audio files, data on handheld devices, animation, metadata, graphics, photographs, spreadsheets, Web sites, drawings, and other types of digital data. e-discovery are more expensive, time-consuming, and burdensome than ever before.

- **Computer forensics:** a complex branch of forensic science, pertains to legal evidence found in computers and digital storage media. It is a field that requires careful preparation and procedural strictness. Because of the scope and technical requirements of this field, there are many subsections such as firewall forensics and mobile device forensics. However, all have the same purposes: to analyze computer systems related to court cases, evaluate a computer after a break in, recover lost data, gather evidence.