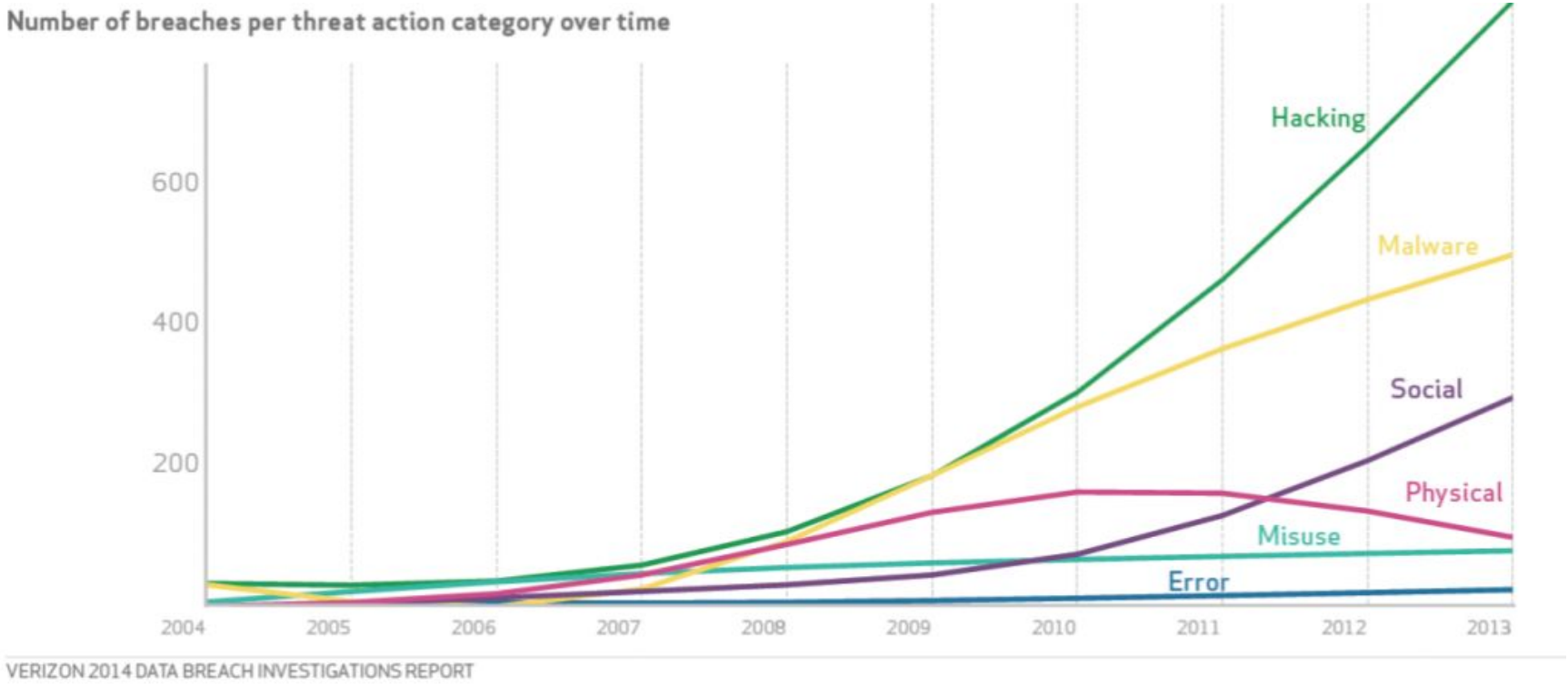
Cybercrime Timeline Evolution

Dr. Ala Berzinji

Computer Science Department

Cybercrime

Cybercrime is a fast-growing area of crime using Internet and computers.



Cybercrimes areas

- Attacks against computer hardware and software.
- Financial crimes and corruption.
- Crimes against children.

Against individuals (EFPCH)

- Email spoofing
- Fraud
- Phishing
- Cyber stalking
- Hacking computers

Against society

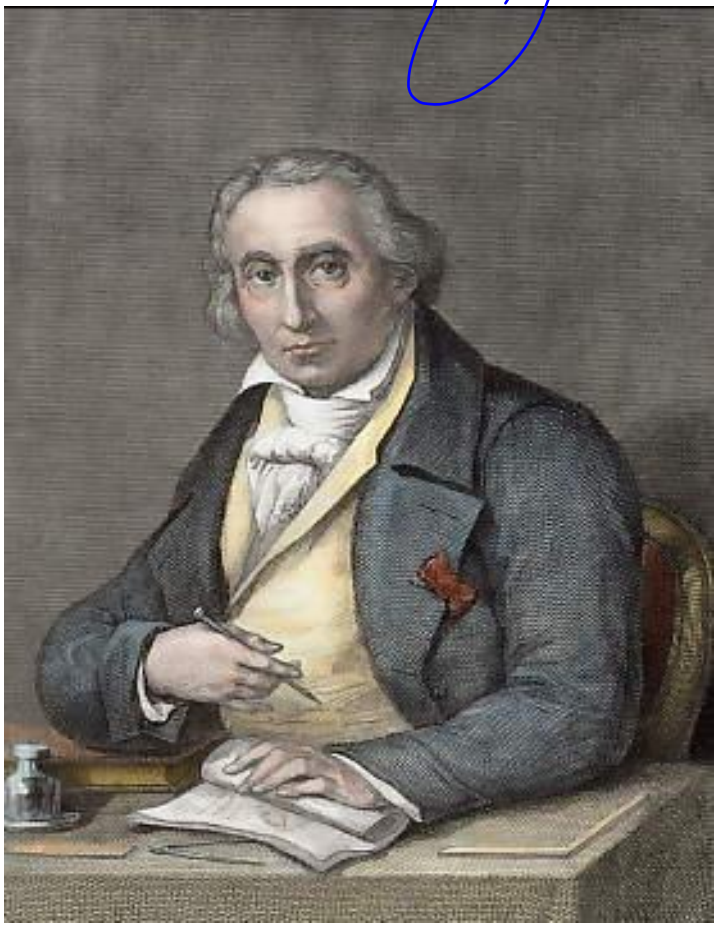
- Polluting the youth through indecent exposure.
- Trafficking financial crimes.
- Sale of illegal articles.
- Online gambling.

Against government & organizations

- Cyber terrorism.
- Distribution of pirated software.
- Unauthorized control/access. over computer system.
- Possession of unauthorized information.
- Forgery.

First recorded cybercrime

- The first recorded cyber crime took place in the year 1820! By Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics.



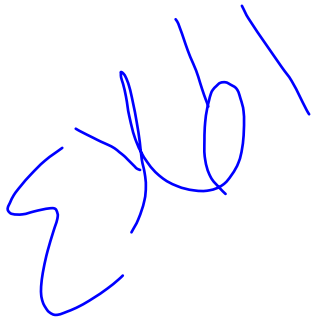
Cybercrime 1970-1990

- Free calls.
- Using computer to steal $2 million from New York bank.
- Changing the billing clock so that people receive discount.
- Movie WarGames introduces the phenomenon of hacking.
- Hacker magazine begins publication
- The oldest virus, infects IBM computers.
- break into government computers.
- secretly monitors the e-mail of American security officials.
- First large computer fraud case investigated in organizations.

Cybercrime 1991-2000

- Military secrets sold.
- 1st polymorphic virus released.
- Russian crackers steal $10 million from Citibank.
- Hackers deface federal web sites.
- Canadian hackers break into CBC.
- The US General Accounting Office reports hackers attempted to break into Defense Dept.
- America On-line (AOL) cuts direct access for its users in Russia due to the high level of fraud.
- Hacking Microsoft's Internet software and transfer money between accounts.

Cybercrime 2001-2005



- Break into Microsoft's corporate network and access source code for the latest versions of Windows and Office software.
- Microsoft falls victim of a new type of attack against domain name servers, a Denial of Service (DoS) attack.
- FBI agent Robert Hanssen is charged with using his computer skills and FBI access to spy for Russia (Mar)..
- Targeting MS SQL Server, fastest spreading worm in history.
- Disables critical safety systems at a nuclear power plant.
- U.S. Justice Department announces hacking.
- Steal costumer credit card information using wireless network.

Cybercrime 2001-2005

- Hacking into a T-Mobile computer system,
- Hacking websites.
- Paris Hilton’s T-Mobile phone hacked.
- Bank of America had 1.2 M names and Social Security numbers stolen.
- FBI's e-mail system hacked.
- Polo Ralph Lauren 108,000 accounts hacked
- CardSystems admits hackers planted virus and accessed 14M credit card numbers.
- In USA 978000 University accounts hacked.
- Hacking SKype

Cybercrime 2006- 2010

- Hackers break into Department of Homeland Security computers, install malware, and transfer files to a remote Chinese-language Web site;
- Ohio University alumni relations server compromised and 137000 SSN’s stolen .
- A flaw in Passport Canada's website
- A vulnerability in WordPress allows spammers to penetrate many websites.

Cybercrime 2010-2015

- The OpenSSL cryptographic software library used to encrypt Web traffic is affected.
- The U.S. Department of Defense is attacked .
- CurrentC Mobile payment attack.
- Over 83 million households and small businesses in U.S were affected.
- Unreleased films hit the Internet.
- Attack on the Belgian Internet company Belgacom's computer systems and email servers.

Cybercrime 2010-2015

- South Korea Over 27 million people and 220 million private records attacked.
- Images of the world's biggest female celebrities were posted online, as a result of a hack of Apple's ICloud services.
- Biting into mobile payments
- Open source, open target
- Attacks on infrastructure
- Satellite attacks in Belgian and France by ISIS

The changing nature of cybercrime

- In the past, cybercrime was committed mainly by individuals or small groups.

- Today, criminal organizations working with criminally minded technology professionals to commit cybercrime

Cyber Security

- Involves protection of sensitive personal and business information through prevention, detection and response to different online attacks.

Cyber Forensics

- Computer Forensics, is the application of scientifically proven methods to gather, process, interpret, and to use digital evidence to provide a conclusive description of cyber crime activities.

Cyber Law

- Any laws relating to protecting the internet and other online communication technologies

Needs for cyber law

- Integrity and security information
- Security of Government Data
- Intellectual property rights
- Privacy and confidentially of information
- Legal status of online Transactions

Conclusion

Cybercrime is new to Middle East counties, but it poses major threats on them compared to the developed countries, which have a more secured infrastructure, system and communication services.

So:

- Avoid using peer to peer programs.
- Avoid downloading unnecessary applications and freeware.
- Do not open suspicious files/emails.

Thank you for your Attention!