

THE HISTORY OF CYBERSECURITY AND ITS MODERN DEVELOPMENT

Muzychenko K.M. *kirilmuzychenkho@gmail.com*
National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute” ISZZI

Today a lot of people can't imagine their lives without internet. We communicate, get acquainted, entertain, study, get new information, watching videos and do other things there. But few people know history of this discovery.

In the 1960-s, the Advanced Research Projects Agency (ARPA) of the United States Department of Defense funded research into time-sharing of computers [1]. Survey in set exchanging, one of the significant Internet technologies, started in the deal of Paul Baran in the early 1960-s and, regardless, Donald Davies in 1965[2]. After the Symposium on Operating Systems Principles in 1967, packet switching from the suggested NPL web was included into the styling for the ARPANET and other resource sharing networks such as the Merit Network and CYCLADES, which were established in the late 1960-s and early 1970-s. Since 1995, the Internet has considerably? tremendously and even more marvelously influenced education and trafficking, involving the growth of close momentary communication by e-mail, messaging, reporting, voice-chatting telephony (Voice over Internet Protocol or VoIP), both side online video- calls, and the World Wide Web [3] with its debate panels, blogs, social networking services, and online shopping sites.

Fraudsters advanced as technology advanced. Cybercrime spread every year as a new kind of crime. Well, we have a big challenge nowadays. And cybersecurity will be solution of this problem. Cybersecurity is the defense of related systems such as equipment, programming support and information from virulent cyber damage. This deal used by persons and companies to defense versus strange availability to information resources, facilities and other machine frameworks. Realization virtuous cyber defense efforts is especially complicated nowadays as we have much more inventions that's why users, and fraudsters getting more contemporary.

A high-flyer cyber defense technique has numerous levels of defense proliferate through the machines, networks, programs, or information that one have purpose to be under protection. In an entity, the human, developments, security and technique must all supplement one another to discover a virtuous and fast security from different cyber raids.

People should know and work with basic information defense inventions for example selecting protectable passwords, existence of a lot applications in e-mail and mobile phone numbers, personal info. Also ability to know big amount of data relate to the main cybersecurity frameworks. Groups should have a basic knowledge for how they deal with both efforted and big-time cyber assaults. Technology is in need to giving businesses and persons the computer defense implements necessary to def themselves and other from cyber raids. Three main sections must be under protection: up to date devices such as machines, smart devices, and internet routers, networks, and the cloud. Simple technology used to defend these sections incorporated next generation partition wall, DNS filtering, malware defense, antivirus envelope, and different email defense decisions.

However why is cybersecurity vital? In nowadays linked networking earth, anybody looking for profit from cybersecurity advanced inventions. On the personal rate, a cyber

defense attack can have impact in all from determination fraudsters, to racketeering or shakedown efforts, to the loss of vital information such as documents or personal photos. Each who is based on crucial facilities like big factories, refineries, and financial or economical service teams. Defending these and other organizations is important to keeping our society functioning properly[4].

Everyone also have profit from the work of cyberthreat researchers, like the team of 250 danger fraudsters at Talos, who inquire into new and evolving threats and cyber raid plans. They disclose new innocent sides, enlighten the public on the significant of cyber defense, and length opensource instruments. Their issue makes the Internet much safer for everyone. And the main aim of cybers defense is to predict cyberterrorism that can take millions of life's.

Nowadays we have different kinds of cybers dangers. Phishing is like pattern of putting knavish e-mails that remind e-mails from authoritative resources and web sites. The goal is to steal major information such as credit card numbers and login information. It's the most provided kind of cyber raids. You can help to defend yourself with education or a technology decisions that will strain malicious e-mails.

Ransomware is a kind of ill-intentioned programming assistance. It is invented to squeeze funds by freezing available to files or the machine system until the buyout is paid. Paying the buyout does not ensure that the files will be recovered or the system re-established.

Malware is a kind of programming support that is dedicated to receive unsanctioned entry or to cause detriment to a computer.

Social engineering is a strategy that promotes to deceive you into expanding your own information. They can request a currency payment or gain entry to your secret information. Social engineering can compo with any of the dangers enumerated upper to offer you click on "interesting" references, upload virus, or trust a ill-intentioned programs.

All in all, cybersecurity is significant part of law and order nowadays. A lot of young people are at risk of internet die groups or other criminal organization and cyberpolice try to protect them. But everyone has to remember that he is main defender of his internet security and no one can save you completely from cyberterrorism except you. Henry Ford once said smart words: "Chop your own wood and it will warm you twice".

References

1. Hauben, Michael; Hauben, Ronda. "5 The Vision of Interactive Computing And the Future". Netizens: On the History and Impact of Usenet and the Internet. 1997.
2. "So, who really did invent the Internet?" Archived 3 September 2011 at the Wayback Machine, Ian Peter, The Internet History Project, 2004. Retrieved 27 June 2014.
3. How the web went world wide Archived 21 November 2011 at the Wayback Machine, Mark Ward, Technology Correspondent, BBC News. Retrieved 24 January 2011.
4. CISCO LIVE MELBOURNE December 7 - 10, 2021 URL: <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity>

Language adviser: *Sokyrska O.S., PhD in Philology, senior lecturer, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"*