1. It is true that millions and millions of bytes of personal data have been exposed on the internet but this is mostly because of the unawareness of people. Terms of use and privacy are usually mentioned properly on the site, after which the site asks for permission before proceeding, but people normally skip reading the terms of use and privacy and just check on the boxes and accept the terms without properly going through them. This may give sites access to private information without the knowledge of the user. (Manoush Zomorodi (2017) Do You Know How Much Private Information You Give Away Every Day? Ideas and technology https://time.com/4673602/terms-service-privacy-security/)

Why people still have faith in the internet:

This is because the internet provides a good platform that connects people irrespective of their location in the world. This serves to spread information faster and allows interaction of people. At the same time, the internet provides personalized services for example banking and deliveries, which is very convenient and easy to use and saves time and money. Keeping this in mind, despite the various disadvantages, people still have faith in the internet because the good outweighs the bad and thus people will overlook the bad and still use it.

2. The term hacking has changed meaning over the years. This is because hackers of nowadays not only steal the data and mess around with computers like the past conventional hackers used to but also steal money, keep track of our behavior and regular habits like our interest and sites we visit., and commit other cybercrimes that are harmful to the society. This enables them to get a feel of who we are, what we do on the regular in terms of jobs and leisure. This allows them to go beyond stealing data to stealing whole identities and breaking our security outside the internet as well. They actively keep monitoring the end-user without them knowing through the regular sites we visit. Thus, the term hacking has grown from the conventional “black hooded guy in a dark bedroom” to everyday people who access people’s information secretly and use them in the process of identity theft and fraud. (Tripwire guest authors (2016) The Evolution of Hacking, https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-evolution-of-hacking/)

3. The most dangerous hacker tools include Metasploit, Wireshark, and Nmap. These tools can be used to both break the security wall and get all the security-related information from the system giving access to sensitive data and passwords to the hacker.

Metasploit: Can be used to show security vulnerabilities and enumerate networks thus allowing the hacker to execute attacks and remain undetected.

Wireshark: Used in the packet sniffing of user data from a network connection. Data that is snatched can be usernames, passwords, and images

Nmap: This is a scanning tool that uses IP packets to identify devices connected to a network and provide information on operating systems and services.

(Gregg, M., & Santos, O. (2019). Certified Ethical Hacker (CEH) version 10 cert guide.)

4. The NSA hacker tools were leaked by a group called The Shadow Brokers using file-sharing sites such as BitTorrent and DropBox. This group is suspected to have had an insider who stole this hacker tool from the NSA. This leak followed by the repurposing of the exploits in the WannaCry and NotPetya led to the shutting down of computers worldwide. The leak of these tools meant that the security of government and corporate networks was undermined. (Lily Hay Newman (2010) The Leaked NSA Spy Tool That Hacked the World, https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/)

5. The attackers who attacked Target’s systems gained access to customer information, installing malware on the system thus capturing full names, email addresses, payment cards, credit card verification, and more sensitive data.

There were several factors that led to the data loss. These include:

a) Vendors were subject to and susceptible to phishing attacks by receiving emails from Vendor machines which were as a result of Malware being installed on the same machines.

b) There was a lack of network segregation.

c) The point-of-sale systems (POS) were susceptible to memory scraping malware that went undetected by the strategies employed by Target employees.

d) Failure to respond to FireEye alerts which could have alerted any vulnerability.

(Tracy Kitten (2013) Target Breach: What Happened? https://www.bankinfosecurity.com/target-breach-what-happened-a-6312)

6. Hacktivism is the act of misusing or misappropriating a network or any computer system for a social, economic, or politically motivated reason. It is done by hacktivists who act as hackers to leak information thus bringing something to public attention. I believe it is a form of protest that provides the public with hidden information that allows us to make an informed decision. Unless hacktivism is used for destructive purposes to individuals or corporations it is a positive form of protest. (Madelyn Bacon, Hacktivism https://searchsecurity.techtarget.com/definition/hacktivism#:~:text=Hacktivism%20is%20the%20act%20of,socially%20or%20politically%20motivated%20reason.&text=A%20hacktivist%20uses%20the%20same,a%20political%20or%20social%20cause.)

7. Stuxnet is one exceptionally complex computer worm that takes advantage of multiple previously unidentified Windows zero-day vulnerabilities to infect computers and spread. When it infects a device, it looks to see if it's related to one of Siemens' unique models of programmable logic controllers (PLCs). PLCs are the devices that enable computers to communicate with and control industrial machinery such as uranium centrifuges. The worm then changes the programming of the PLCs, causing the centrifuges to spin too fast and for too long. As a result, the fragile equipment is damaged or destroyed in the process. As this is going on, the PLCs are reporting that all is good to the controller machine, making it impossible to identify or diagnose what's wrong until it's too late.

(Zetter, K. (2014). Countdown to zero-day: Stuxnet and the launch of the world's first digital weapon. New York, N.Y: Broadway Books.)

8. ARPANET was the first wide-area packet-switching network with distributed control and one of the first networks to use the TCP/IP protocol suite. Both technologies became the Internet's technological base. The Advanced Research Projects Agency (ARPA) of the United States Department of Defense established the ARPANET. Its original intent was to use telephone lines to link computers at Pentagon-funded research institutions. (Kevin Featherly (2016), ARPANET https://www.britannica.com/topic/ARPANET)

9. DBS is safe and successful in patients who are appropriately selected. There are risks and possible side effects, but they are usually minor and reversible. They include:

i. Low risk of a brain hemorrhage (1%), including stroke

ii. Infection

iii. Device malfunction or error in the systems

iv. Lack of benefit for certain symptoms

v. Headache

vi. Deterioration of mental or emotional health

(Julie G Pilitsis, MD, PhD, FAANS Deep Brain Stimulation https://www.aans.org/en/Patients/Neurosurgical-Conditions-and-Treatments/Deep-Brain-Stimulation)

10. The red team is a group in an organization that plays the role of the enemy or threat in order to identify and assess vulnerabilities or loopholes in an organization. They help in determining how an organization can be under threat by portraying the enemies and try and infiltrate the systems in order to find the Achille’s heel. They have been authorized to attack the system in order for the organization to cover this threat before real attackers with malicious intentions are able to take advantage of it. ( Zenko, M., & Overdrive Inc. (2015). Red Team. Place of publication not identified: Basic Books.)