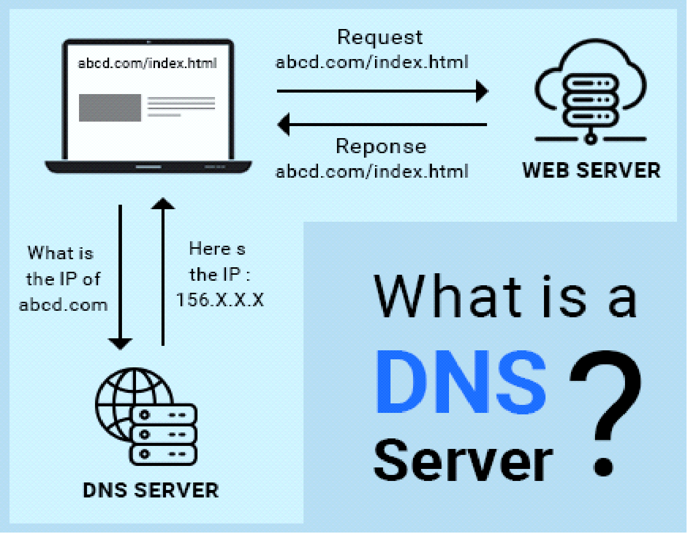
Cyber Society of India

Responses to Participants' questions in the Kaninar Series 6 conducted by CySI Virtually on 05.06.2021

Q1) DNS (Domain Name Server) Protection:

The Domain Name System, otherwise known as DNS, is a key component of the Internet. DNS is the resolution of a domain name to an IP address. The Domain Name System (DNS) is the protocol that makes the Internet usable by allowing the use of domain names.



DNS Key Security Best Practices:

DNS servers are a frequent target of cyber-attacks. Securing DNS infrastructure is a crucial step in preventing breaches into your organization. To avoid a major impact on your DNS setup, make sure **to employ the security measures outlined below.**

Enable DNS Logging

DNS logging is the most efficient way to monitor DNS activity. The logs let you know if someone is meddling with your DNS servers. Besides client activity, debug logs tell you when there are issues with DNS queries or updates.

Lock DNS Cache

Whenever there is a query from a client, DNS finds the information and stores it in the cache for future use. This process allows the server to respond faster to the same queries. Attackers can exploit this feature by altering the stored information.

Filter DNS Requests to Block Malicious Domains

DNS filtering is an effective way to prevent users from accessing a website or a domain. The main reason to block name resolution for a domain is if that domain is known to be malicious. When a client sends a query for a blocked website, a DNS server stops any communication between them.

Validate DNS Data Integrity with DNSSEC

Domain Name System Security Extensions (DNSSEC) ensure clients receive valid responses to their queries. Data integrity is achieved by DNSSEC digitally signing DNS data provided to nameservers.

Configure Access Control Lists

Access Control Lists (ACL) are another way of **protecting DNS servers against unauthorized access and spoofing attacks**. Only IT administrators and system admins should have access to your primary DNS. Configuring ACLs to allow inbound connections to a nameserver from specific hosts ensures that only the intended staff can communicate with your servers.

Q2) Are Apple (Mac) Systems safe when compared to Windows systems?

Each system has got own pros & cons, both macOS and Windows have their flaws and strengths which may influence your decision. With each user having very different levels of technical skill, you may find yourself choosing a platform that feels more comfortable and familiar.

Regardless of choice, you will find the most secure platform to be the one you know the best. Learning how to properly use your software will keep you more secure than any definitive security statistics can.

Having said that, here are some key takeaways to help you see the big picture:

Mac OS

- Pros: Smaller attack rates, moderate browser security, ease of use
- Cons: larger threat growth, slower OS update cycles
- Tip: Less technical users may find this platform easier to navigate and keep safe.

Windows OS

- Pros: constant OS update cycles, fairly reliable out-of-the-box threat protections
- Cons: Largest cyberthreat attack rate of any OS, requires more attention to security upkeep
- Tip: Ideal for more hands-on users or those already familiar with Windows PCs.

In a nutshell, Apple's macOS has a relatively lower rate of attacks as noted with its much smaller market share. However, the growth and increased relevance of Apple devices may leave it open to a shift in attack rates. Microsoft's Windows OS has a substantially higher rate of attacks, largely due to its dominant market share. Immediately, this platform demands a bit more attention for users to stay safe. A decrease in rates of attack is unlikely due to the massive hold on the OS market.

Q3) How far Public Cloud based storages are safe?

Cloud computing has grown in recent years to become one of the dominant forces within the world of business IT and cloud adoption by individuals & Organizations have grown significantly in the recent times.

Cloud storage allows you to store your data on someone else's hard drive, in datacenters around the world. You do not have to worry about losing your data, and you can access it from anywhere.

Understandably, the security of these platforms has become a key concern.

Securing Your Data

When you upload your data to cloud storage, they encrypt your data-at-reset. Some providers allow you to password protect, require an encryption key or apply Multi-factor authentication requiring an additional verification step to gain access.

There are a variety of cloud storage providers, and the majority of them have a free-tier ranging into multiple gigabytes. By using various cloud providers, you could have terabytes of free storage.

In a nutshell, it's a widely accepted fact that no cloud storage system will ever be 100% secure, especially given that upholding the integrity of every account is reliant on the user following best practices.

The decision you have to make as a customer is deciding which storage platform does the most to avoid potential security incidents. The factors that influence this decision will vary depending on the nature of your requirements, be it personal or business and whether you have specialist requirements, such as businesses in a heavily regulated industry.

However, for most consumers and small businesses, each of the platforms listed here are generally good enough for protecting data, as each provides some form of data encryption at rest and in transit, Strong authentication (MFA), access Controls - which are perhaps the most important thing here. Data protection is also improving all the time, and each of these platforms are being updated with better safeguards each year, meaning you can typically rely on the company to do most of the legwork.

Q4) What is meant by Sandbox?

A sandbox is an isolated testing environment that enables users to run programs or execute files without affecting the application, system or platform on which they run. Software developers use sandboxes to test new programming code. Cybersecurity professionals use sandboxes to test potentially malicious software or malware analysis.

Q5) Is Internet banking safe?

Yes, Internet banking is safe but depends up on our handling. Internet Banking is a very safe channel to carry out your transactions until you share you credentials to a third party. It is advised that you do not do an Internet Banking transaction at a public browsing centre. Always use a strong password and keep changing them frequently, never save your login information, ensure you browse the correct website of your respective Bank and type the URL yourself. Last but not the least, never share your login id or password to anyone. As a customer, we need to be more Vigilant and responsible.

Q6) Why Banks are not using Block chain technology for safety?

Presently banks use **Block chain** technology for KYC on experimental basis. Since blockchain technology cost are high. BC technology is for multiple stakeholders who wants to have secure and persistence transactions. Banks have already started testing the block chain technology for financial transactions so sooner or later this would be adopted by the banks in India.

Q7) Legal Steps to follow an incident is found with regard to social engineering impacts.

Immediately copy the URL of the fake account and take screenshots of the same. You can either report it to the nearby police station or via online www.tnpolice.gov.in .Alert your close connects regarding the fake account & Virtual Begging either through a post in your original Facebook account or through Whatsapp.

Q8) Courts are requesting email id and mobile no. Is it not a challenge for a common man to provide these and push legal cases?

This would be the new norm for the judicial systems in India here after as it was already proved to be convenient and successful method in various other countries. However, the old system was not completely scrapped in India and still the courts follow the both systems. As per the convenience of the party he may choose either choose online or physical filing/ appearance. Providing email id & mobile no is not a challenge and it is the order of the day. We must be careful while responding email & Phone call.