Cyber Security Fundamentals

Assignment-4

N Ravinder Reddy

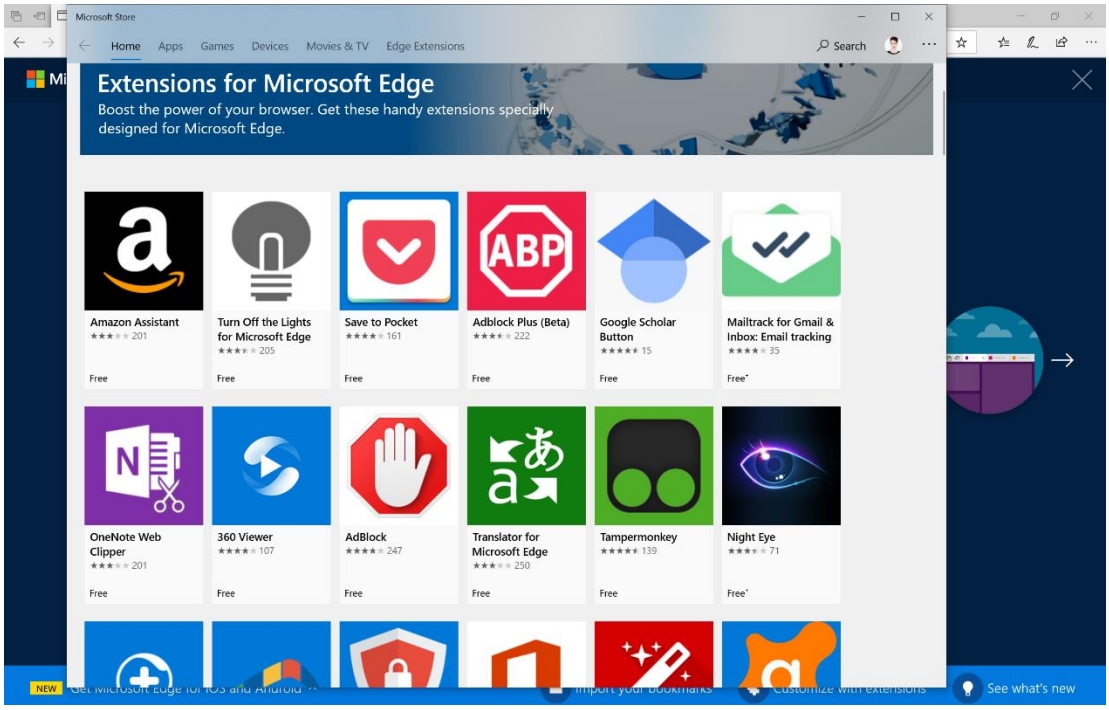
Roll No: 2406CYS106

Q. 1. Web Browser Extensions: How risky are extensions & how can you choose safe ones?

Ans: Extensions are small software programs that customize the browsing experience. They enable users to tailor Chrome functionality and behavior to individual needs or preferences. They are built on web technologies such as HTML, JavaScript, and CSS.

When Installing an Extension:

1. Be picky. The more extensions installed, the bigger the attack surface you open up to attackers. ...
2. Only install through trusted sources. While not guaranteed safe, security technicians review extensions for malicious content.
3. Review permissions. ...
4. Use antivirus protection.



6 Ways to Make Sure Your Chrome Extensions Are Safe

1. Use the Chrome Web Store. ...
2. Research the Developer. ...
3. Make Sure the Extension Is Updated Regularly. ...
4. Check Reviews. ...
5. Regularly Perform Antivirus Scans. ...
6. Use Chrome Enhanced Safe Browsing and Surf the Web Safely.

   Verify the developer's legitimacy: To determine the safety of an extension, look for a professional developer with a public profile or website. If the website doesn't have an HTTPS connection or you notice other suspicious elements like a vague privacy policy, it's best to avoid installing that extension.

Here are some privacy and security concerns that browser extensions can pose:

- They can work as potential keyloggers to capture your passwords and login details. A keylogger can track everything you type, making it a huge threat to your sensitive data such as credit card details and financial information.
- Malicious browser extensions can redirect your search traffic elsewhere.
- A dangerous web extension could potentially download malware, adware, and Trojan horse viruses.
- Some browser extensions can gather bits of information from your browsing history and pass it on to third parties or sell it to advertisers.
- Most extensions can be updated automatically which means that even a legit extension could be hijacked and updated on your device without you ever finding out.

There is no guarantee that the safest browsers can protect your privacy when it comes to their browser extension offerings. In 2020, Google had to remove a total of 106 Chrome browser extensions from its Chrome Web Store in response to a report that they were being used to funnel sensitive user data.

Avoid Using Too Many Extensions

When it comes to browser extensions, less is always more so keep your list of extensions to a bare minimum.

Most web browsers come with customizable features and do not need additional extensions that were once popular, such as managing to-do lists or saving news articles for reading later.

Since most good extensions eventually become a part of the browser itself, there is no need to add additional ones boasting the same features and expose yourself to the dangers of malicious extensions.

It is extremely important to only install extensions coming from popular sources such as the Chrome Web Store or Mozilla.

Avoid installing quick and seemingly easy extensions as there is no way to predict what type of data exploitation they might be conducting. Also, an extension created by a random stranger to customize popular services like Gmail or YouTube is a red flag and should be avoided as it can open doors for malware.

However, if an extension is coming directly from a reputable source like Google or Microsoft then it's worth a shot: these are generally safe and not sold to third-party companies for malicious purposes.

To keep users safe, Google uses machine learning to detect and block malicious extensions whereas Mozilla conducts automated validation checks on its extensions. But again, always err on the side of caution, even with the popular browser providers.

If an extension has been sitting idle in your browser, then simply uninstall it.

Go through all of your browser extensions regularly and delete the ones that are no longer needed. This reduces the risk of security flaws that can be introduced through extensions especially the ones offered by third-party providers.

By deleting unnecessary extensions, you also help your browser work better routine cleaning of your browser is a great performance booster for your system.

Deleting browser extensions varies by browser.

For instance, in Chrome, you can click on the extension icon in the upper right corner of the window and then select **Remove**. Alternatively, you can click the **More** button (the dotted vertical line on the top right) and select **More Tools**. Then click on **Extensions** to see a list of all your installed extensions and remove the ones that are not needed.

Q. 2. Securing Your Browser: Best methods & their trade-offs for a safer browsing experience.

Ans: Secure web browsing involves the use of tools and techniques to protect users from cyberattacks, malware, or other cybersecurity vulnerabilities. Web browsers allow users to view sites on the internet by displaying images and text, executing code, rendering animations, and saving information.

Safe Browsing Tips

1. Updated Browsers and Plugins Go a Long Way.
2. Be Mindful of the HTTPS.
3. Clear Cookies and the Web Browser Cache.

4. Not Everything You Download is Safe.
5. Install Antivirus and Firewall Protection.
6. Use a VPN.
7. Make Use of the “Do Not Track” Feature.

How can I improve my safety while browsing the internet?

1. Get the latest anti-virus and firewall software.
2. Update your internet browser.
3. Create a strong and easy-to-remember password.
4. Use a different password to the one you use for other services.
5. Change your password on a regular basis.
6. Never share your password.
7. Don't let your browser remember your log on details.

6 Best Practices for Secure Web Browsers

- Keep Browsers Up-to-Date.
- Use HTTPS.
- Use Unique Passwords.
- Disable Auto-Complete for Forms.
- Block Pop-ups and Ads.
- Limit the Use of Cookies.

Security trade-offs are the inevitable compromises that security architects have to make when designing and implementing security solutions. They involve balancing the costs, benefits, risks, and opportunities of different security measures, such as performance, usability, scalability, compliance, and innovation.

Here are some of the key trade-offs to consider in cyber security:

- Security vs Cost: Implementing strong security measures can be expensive and time-consuming. ...
- Security vs Complexity: Some security measures, such as encryption and two-factor authentication, can be complex and difficult for users to understand.

  What is the meaning of tradeoffs? Tradeoffs in network design refer to the balancing of various factors and decisions that impact the overall performance, cost, manageability, security, and scalability of a network.

Some common tradeoffs in network design include:

1. Cost vs. Performance: Higher-performance network components and devices typically come with higher costs. Designers must balance the need for performance with budget constraints, choosing the right combination of devices and technologies to achieve the desired performance without breaking the budget.

2. Scalability vs. Complexity: As networks grow and scale, their complexity increases. A highly scalable network may require more advanced protocols, technologies, and management tools, increasing complexity and making the network more challenging to maintain and troubleshoot. Designers must find a balance between scalability and complexity, ensuring the network can grow as needed without becoming unmanageable.

3. Security vs. Usability: Implementing strong security measures can sometimes impact network usability and performance. For example, deploying firewalls, VPNs, and encryption can add processing overhead, potentially affecting network speed and responsiveness. Designers must balance security needs with usability and performance, ensuring that the network remains secure without sacrificing user experience.

4. Redundancy vs. Cost: Building redundancy into a network design improves reliability and fault tolerance but also increases costs due to additional hardware, software, and maintenance requirements. Designers must balance the need for redundancy with cost constraints, determining the appropriate level of redundancy for the specific network requirements.

5. Centralized vs. Decentralized Control: Centralized network control can simplify management and administration but may introduce a single point of failure and potential performance bottlenecks. On the other hand, decentralized control can improve fault tolerance and performance but may increase management complexity. Designers must find the right balance between centralized and decentralized control to meet the network's requirements.

6. Proprietary vs. Open Standards: Using proprietary technologies or protocols may offer unique features and performance benefits but can lead to vendor lock-in and compatibility issues. Open standards generally provide

more flexibility and interoperability, but they may not always offer the latest features or best performance. Designers must weigh the advantages and disadvantages of proprietary and open standards technologies when making decisions.

7. Real-time vs. Delay-tolerant Traffic: Networks often need to support a mix of real-time (e.g., VoIP, video conferencing) and delay-tolerant (e.g., email, file transfer) traffic. Designers must balance the need for low latency and high bandwidth for real-time applications with the efficient handling of delay-tolerant traffic.

8. Short-term vs. Long-term Planning: Network designers must balance immediate needs and requirements with future growth and technological advancements. Focusing too much on short-term goals might result in a network design that becomes outdated or requires significant rework in the future, while overemphasis on long-term planning might lead to unnecessary complexity and costs.

9. Local vs. Cloud-based Services: Network designers must decide whether to use local or cloud-based services for various functions. Local services can offer better control, security, and performance, but they require more in-house resources for management and maintenance. Cloud-based services can simplify management and reduce costs but may introduce latency, security concerns, or reliance on third-party providers.

10. Proactive vs. Reactive Network Management: Proactive network management aims to prevent issues before they occur by investing in monitoring, maintenance, and capacity planning. Reactive network management focuses on fixing problems as they arise. Balancing these approaches is essential to ensure a network remains reliable without incurring unnecessary costs or resource allocation.

11. Wired vs. Wireless Connectivity: Wired networks generally provide more stable, secure, and high-speed connections but may require more infrastructure investment and maintenance. Wireless networks offer flexibility and ease of deployment but can be prone to interference, security vulnerabilities, and performance fluctuations. Network designers must balance the benefits and drawbacks of wired and wireless connectivity based on the specific requirements and constraints.

12. Ease of Deployment vs. Customization: Standardized, off-the-shelf solutions can simplify deployment and reduce initial costs but may lack the customization and features needed for specific network requirements. Customized solutions can provide tailored functionality but may increase deployment complexity, costs, and ongoing maintenance requirements.

13. Energy Efficiency vs. Performance: Energy-efficient network components and devices can reduce operating costs and environmental impact but might compromise performance or introduce additional constraints. Network

designers must balance the need for energy efficiency with the performance and functional requirements of the network.

14. Ease of Use vs. Feature Richness: Simple, easy-to-use network solutions may lack advanced features and capabilities that could benefit the organization. Conversely, feature-rich solutions might be more difficult to learn, configure, and maintain. Designers must balance ease of use with the desired feature set to ensure the network meets the organization's needs without becoming overly complex.

15. Quality of Service (QoS) vs. Resource Utilization: Implementing QoS mechanisms to prioritize specific types of traffic may improve the user experience for critical applications, but it can also consume additional network resources and increase management complexity. Network designers must balance the benefits of QoS with the potential impact on resource utilization and overall network performance.

16. Manual vs. Automated Management: Manual network management can provide granular control and customization but may be time-consuming and error-prone. Automated management solutions can improve efficiency and reduce human error but may be less flexible or customizable. Network designers must balance the benefits of automation with the need for manual control and customization.

17. Physical vs. Virtual Infrastructure: Physical network infrastructure provides dedicated resources and performance but can be expensive and inflexible. Virtual infrastructure can offer cost savings, flexibility, and resource efficiency but may introduce additional complexity and potential performance issues. Designers must balance the benefits of physical and virtual infrastructure to meet the organization's specific requirements and constraints.

18. Network Monitoring vs. Privacy: Implementing network monitoring tools can help detect performance issues, security threats, and other problems. However, excessive monitoring may raise privacy concerns and lead to potential compliance issues. Network designers must balance the need for network monitoring with the privacy expectations of users and regulatory requirements.

19. Latency vs. Throughput: Networks need to handle various traffic types, some of which are more sensitive to latency (e.g., voice and video), while others require high throughput (e.g., large file transfers). Designers must balance the network's ability to handle latency-sensitive traffic while still maintaining high throughput for other traffic types.

20. Modularity vs. Monolithic Design: A modular network design allows for easier updates, replacements, and expansion of individual components, making it more adaptable and easier to maintain. In contrast, a monolithic design may have fewer points of failure and be more cost-effective, but it can

be more difficult to update or replace components. Designers must balance modularity and monolithic approaches according to the organization's needs and future growth plans.

21. Converged vs. Dedicated Networks: Converged networks combine multiple services (data, voice, video) on a single infrastructure, potentially simplifying management and reducing costs. However, converged networks can introduce performance and security challenges due to the shared resources. Dedicated networks separate services onto different infrastructures, improving performance and security but increasing costs and management complexity. Designers must balance the benefits and drawbacks of converged and dedicated networks.

22. Propagation Delay vs. Network Diameter: Network designers must consider the propagation delay (the time it takes for a signal to travel across the network) when designing large-scale networks. A larger network diameter (the longest path between two nodes) may increase propagation delay, which can impact real-time applications. Designers must balance the network diameter and propagation delay to ensure optimal performance for time-sensitive applications.

23. Multicast vs. Unicast Traffic: Multicast traffic allows a single source to send data to multiple destinations simultaneously, which can be more efficient for certain types of applications (e.g., video streaming). However, multicast can introduce additional complexity in routing and management. Unicast traffic, where each data transmission is between a single sender and a single receiver, may be simpler to manage but less efficient for some applications. Designers must balance the use of multicast and unicast traffic based on the network's specific needs.

24. Centralized vs. Distributed Storage: Centralized storage concentrates data in a single location, simplifying management and backup processes. However, it can create a single point of failure and increase latency for users accessing data from remote locations. Distributed storage spreads data across multiple locations, improving fault tolerance and potentially reducing latency but increasing management complexity. Designers must balance the advantages and disadvantages of centralized and distributed storage based on the organization's requirements.

25. Static vs. Dynamic Routing: Static routing relies on manually configured routes, which can provide predictable and stable paths but requires manual updates when network changes occur. Dynamic routing uses routing protocols to automatically discover and update routes based on network conditions, providing better adaptability to changes but potentially increasing complexity and resource usage. Designers must balance the advantages and disadvantages of static and dynamic routing based on the network's specific requirements.

26. Bandwidth vs. Latency: Network designers must balance the allocation of bandwidth and the minimization of latency to ensure optimal performance for various applications. High bandwidth is necessary for data-intensive applications, while low latency is crucial for real-time applications. Balancing these factors can be challenging, as increasing bandwidth may also increase latency in some cases.

27. Network Visibility vs. Control Plane Overhead: Network visibility is essential for managing and troubleshooting a network, but it often comes at the cost of increased control plane overhead. For example, routing protocols, management protocols, and monitoring tools all generate additional control plane traffic. Designers must balance the need for network visibility with the potential impact on control plane resources.

28. Public vs. Private Networking: Public networks, such as the internet, offer global reach and easy access, but they may expose organizations to various security threats and performance issues. Private networks provide better security, control, and performance but often come with higher costs and limited accessibility. Network designers must balance the use of public and private networking based on the organization's specific needs and constraints.

29. Hardware vs. Software Solutions: Hardware-based solutions can offer high performance, reliability, and dedicated functionality but may be more expensive and less flexible than software-based alternatives. Software solutions can provide greater flexibility, easier updates, and lower costs but may not offer the same level of performance or reliability as hardware-based options. Designers must balance the advantages and disadvantages of hardware and software solutions based on the network's specific requirements.

30. Greenfield vs. Brownfield Deployments: Greenfield deployments involve designing and building a network from scratch, offering the opportunity to create an optimized and efficient network without legacy constraints. Brownfield deployments involve upgrading or modifying an existing network, which may be more cost-effective but can introduce challenges due to existing infrastructure, configurations, and constraints. Designers must balance the tradeoffs between greenfield and brownfield deployments based on the organization's goals, resources, and existing infrastructure.

31. Vendor Lock-in vs. Multi-Vendor Strategy: Relying on a single vendor for networking equipment and solutions can simplify management, support, and compatibility, but may lead to vendor lock-in, potentially limiting innovation and increasing costs. A multi-vendor strategy allows for greater flexibility and access to best-of-breed solutions but can introduce complexity in terms of integration, support, and management. Designers must balance the tradeoffs between vendor lock-in and a multi-vendor approach based on the organization's specific needs and goals.

32. Network Redundancy vs. Cost: Implementing network redundancy can improve reliability, fault tolerance, and availability, but it can also increase costs and complexity. Designers must balance the benefits of redundancy with the associated costs and resource requirements, ensuring that the network meets the organization's availability goals without overspending on unnecessary redundancy.

33. Edge Computing vs. Centralized Computing: Edge computing brings processing and storage closer to the data source, potentially reducing latency and bandwidth usage. However, it can introduce management complexity and increased costs for distributed resources. Centralized computing consolidates resources in a centralized location, simplifying management but potentially increasing latency and bandwidth requirements. Designers must balance the benefits and drawbacks of edge and centralized computing based on the network's specific requirements.

34. In-house Management vs. Outsourced Management: In-house network management provides direct control and oversight of the network, but it requires dedicated staff and resources. Outsourced network management, through managed service providers or other external partners, can reduce the burden on internal resources but may result in less direct control and potential reliance on third parties. Designers must balance the advantages and disadvantages of in-house and outsourced management based on the organization's resources and objectives.

35. Scalability vs. Initial Cost: Designing a network with scalability in mind can accommodate future growth and changing requirements, but it may require a higher initial investment. On the other hand, focusing on minimizing initial costs may lead to a less scalable design, potentially resulting in increased costs and complexity when the network needs to be expanded or modified in the future. Designers must balance scalability and initial costs to ensure that the network can adapt to future needs without excessive upfront investment.

36. Security vs. Usability: Implementing strong security measures is critical to protecting network resources and data, but overly restrictive security policies can negatively impact usability and hinder productivity. Designers must balance the need for robust security with the need to maintain a user-friendly and efficient network environment.

37. Automation vs. Manual Control: Automation can simplify network management, reduce human errors, and increase efficiency. However, it may require significant investment in tools and skills, and may not be suitable for every aspect of network management. Designers must balance the benefits of automation with the need for manual control and human intervention in certain situations.

38. Quality of Service (QoS) vs. Complexity: Implementing QoS can prioritize critical applications and ensure optimal performance, but it introduces

additional complexity in terms of configuration, monitoring, and management. Designers must balance the benefits of QoS with the added complexity and the potential impact on network resources.

39. Cloud-based vs. On-premises Infrastructure: Cloud-based infrastructure offers scalability, flexibility, and potentially reduced costs, but may introduce concerns about data security, privacy, and compliance. On-premises infrastructure provides greater control and security but may require higher upfront costs and ongoing maintenance. Designers must balance the tradeoffs between cloud-based and on-premises infrastructure based on the organization's specific needs, resources, and regulatory requirements.

40. Physical vs. Virtual Network Functions: Physical network functions (PNFs) provide dedicated hardware for specific tasks, which can offer high performance and reliability. However, PNFs may be less flexible and more difficult to scale compared to virtual network functions (VNFs), which run on general-purpose hardware and can be more easily scaled and updated. Designers must balance the advantages and disadvantages of PNFs and VNFs based on the network's specific requirements and constraints.

41. Monolithic vs. Modular Architecture: A monolithic network architecture combines multiple functions and components into a single, tightly-coupled system, which can simplify management and reduce compatibility issues. However, it may also limit flexibility, scalability, and adaptability. A modular architecture uses separate, loosely-coupled components that can be easily added, removed, or updated, offering greater flexibility and scalability but potentially increasing management complexity. Designers must balance the tradeoffs between monolithic and modular architectures based on the organization's specific needs and goals.

42. Anycast vs. Unicast: Anycast routing allows multiple devices to share the same IP address, improving load balancing, reliability, and reducing latency. However, it can also introduce complexity in terms of routing, management, and troubleshooting. Unicast routing uses a unique IP address for each device, simplifying routing and management but potentially limiting performance and reliability improvements. Designers must balance the benefits of anycast and unicast routing based on the network's specific requirements.

43. Centralized vs. Distributed Control: Centralized control offers a single point of management, simplifying configuration and monitoring but potentially creating a single point of failure and increasing latency for remote devices. Distributed control spreads management across multiple devices, reducing the risk of a single point of failure and potentially lowering latency but increasing management complexity. Designers must balance the tradeoffs between centralized and distributed control based on the organization's specific needs and network topology.

44. Proactive vs. Reactive Network Monitoring: Proactive network monitoring involves continuously checking for potential issues and addressing them before they cause problems, providing increased reliability and stability. However, it can consume significant resources and may require advanced monitoring tools. Reactive network monitoring focuses on addressing issues as they arise, potentially conserving resources but potentially leading to longer downtimes and decreased reliability. Designers must balance the tradeoffs between proactive and reactive network monitoring based on the organization's specific needs and resources.

45. User Authentication Methods: Designers must balance the tradeoffs between various user authentication methods, such as passwords, tokens, biometrics, and single sign-on (SSO). Each method has its advantages and disadvantages in terms of security, usability, and cost. Designers must choose the most appropriate authentication method(s) based on the organization's specific security requirements, user needs, and budget constraints.

46. Wired vs. Wireless Connectivity: Wired connections typically offer higher performance, reliability, and security compared to wireless connections but may require more extensive cabling and infrastructure. Wireless connections provide greater flexibility and mobility but may face challenges in terms of performance, reliability, and security. Designers must balance the tradeoffs between wired and wireless connectivity based on the organization's specific requirements, network environment, and user needs.

47. Static vs. Dynamic Routing: Static routing involves manually configuring routes, which can provide greater control and predictability but requires ongoing manual maintenance and may not adapt well to changing network conditions. Dynamic routing uses routing protocols to automatically learn and adapt routes, providing greater flexibility and scalability but potentially introducing additional complexity and resource consumption. Designers must balance the tradeoffs between static and dynamic routing based on the organization's specific needs and network size.

48. Traditional vs. Intent-Based Networking: Traditional networking involves manually configuring and managing network devices, which can provide direct control but may be time-consuming and prone to human error. Intent-based networking (IBN) uses automation, analytics, and artificial intelligence to translate high-level business intent into network configurations, simplifying management and reducing errors but potentially requiring additional investment in tools and skills. Designers must balance the tradeoffs between traditional and intent-based networking based on the organization's specific requirements and resources.

49. In-band vs. Out-of-band Management: In-band management uses the same network channels for management traffic and production traffic, potentially simplifying setup but potentially introducing security risks and performance impacts. Out-of-band management uses separate network channels for management traffic, providing greater security and isolation but

requiring additional infrastructure and setup. Designers must balance the tradeoffs between in-band and out-of-band management based on the organization's specific needs and risk tolerance.

50. Hardware vs. Software-based Networking Solutions: Hardware-based solutions, such as dedicated appliances, can offer high performance and reliability but may be less flexible and more expensive compared to software-based solutions. Software-based solutions, running on general-purpose hardware, can provide greater flexibility, scalability, and potentially lower costs but may have performance and reliability limitations. Designers must balance the tradeoffs between hardware and software-based networking solutions based on the organization's specific needs and resources.

51. Network Segmentation vs. Unified Network: Network segmentation can improve security, manageability, and performance by dividing a network into separate subnets or virtual networks. However, it can also introduce additional complexity and management overhead. A unified network simplifies management and may reduce costs but may have security, performance, and manageability challenges. Designers must balance the tradeoffs between network segmentation and unified network based on the organization's specific requirements and risk tolerance.

52. Stateful vs. Stateless Firewalls: Stateful firewalls track the state of each network connection and can provide more granular security controls, but they can be more resource-intensive and complex to manage. Stateless firewalls are less resource-intensive and simpler to manage but may not offer the same level of security granularity. Designers must balance the tradeoffs between stateful and stateless firewalls based on the organization's specific security needs and available resources.

53. End-to-End vs. Hop-by-Hop Encryption: End-to-end encryption secures data from the source to the destination, providing greater privacy and security but potentially limiting visibility and control for network administrators. Hop-by-hop encryption secures data between individual network hops, allowing network administrators to inspect and manage traffic but potentially introducing additional complexity and reducing end-to-end privacy. Designers must balance the tradeoffs between end-to-end and hop-by-hop encryption based on the organization's specific security requirements and network management needs.

54. Hot Standby vs. Cold Standby Redundancy: Hot standby redundancy involves having backup network components that are always powered on and ready to take over in case of a primary component failure, providing fast failover and high availability. However, it can be more expensive and consume more power. Cold standby redundancy involves having backup components that are powered off and only activated when needed, reducing costs and power consumption but potentially increasing failover times. Designers must balance the tradeoffs between hot and cold standby redundancy based on the organization's specific availability requirements and budget constraints.

55. On-Premises vs. Cloud-based Networking Solutions: On-premises solutions provide greater control over infrastructure and data, potentially offering better performance and security for specific use cases. However, they may require significant upfront investment, ongoing maintenance, and in-house expertise. Cloud-based solutions offer scalability, flexibility, and potentially lower costs, but may introduce latency and require reliance on a third-party provider. Designers must balance the tradeoffs between on-premises and cloud-based networking solutions based on the organization's specific needs, resources, and risk tolerance.

56. Quality of Service (QoS) vs. Over-provisioning: QoS techniques prioritize and manage network traffic to ensure optimal performance for critical applications and services. However, implementing QoS can introduce complexity, configuration overhead, and may require advanced hardware or software. Over-provisioning involves adding extra bandwidth and resources to accommodate peak usage and reduce the need for QoS. This approach can simplify network management but may lead to higher costs and underutilized resources. Designers must balance the tradeoffs between QoS and over-provisioning based on the organization's specific performance requirements and budget constraints.

57. Single vs. Multi-Vendor Environments: Single-vendor environments can offer greater compatibility, streamlined management, and potentially better support. However, they may limit flexibility, innovation, and potentially increase costs due to vendor lock-in. Multi-vendor environments provide the ability to choose best-of-breed solutions from multiple vendors, potentially driving innovation and cost savings. However, they can introduce compatibility challenges, management complexity, and may require additional expertise. Designers must balance the tradeoffs between single and multi-vendor environments based on the organization's specific needs, resources, and risk tolerance.

58. Dedicated vs. Shared Infrastructure: Dedicated infrastructure provides exclusive resources for a specific application, service, or tenant, potentially offering better performance, security, and predictability. However, dedicated infrastructure can be more expensive and less efficient than shared infrastructure. Shared infrastructure involves multiple applications, services, or tenants sharing the same resources, potentially reducing costs and improving resource utilization. However, shared infrastructure may introduce performance, security, and management challenges. Designers must balance the tradeoffs between dedicated and shared infrastructure based on the organization's specific requirements and risk tolerance.

59. Centralized vs. Distributed Data Storage: Centralized data storage consolidates data in a single location, simplifying management and backup processes but potentially increasing latency for remote users and creating a single point of failure. Distributed data storage spreads data across multiple locations, potentially reducing latency and providing greater resilience against failure but increasing management complexity and potentially introducing

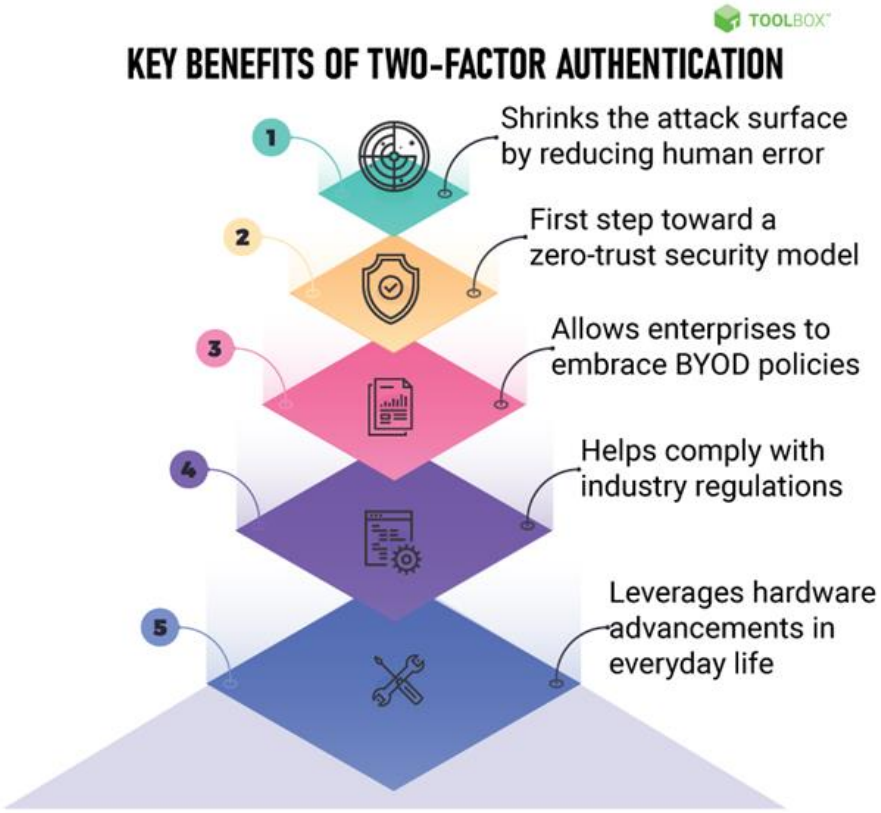
consistency challenges. Designers must balance the tradeoffs between centralized and distributed data storage based on the organization's specific needs and network topology.

60. Physical vs. Virtual Network Functions: Physical network functions (PNFs) rely on dedicated hardware appliances to perform specific tasks, potentially offering high performance and reliability but at a higher cost and with reduced flexibility. Virtual network functions (VNFs) run on general-purpose hardware or in the cloud, providing greater flexibility, scalability, and potentially lower costs but may have performance and reliability limitations compared to PNFs. Designers must balance the tradeoffs between physical and virtual network functions based on the organization's specific needs and resources.

Q. 3. Two-Step Authentication: Compare methods, strengths, and weaknesses & choose the right one.

Ans: Two-factor authentication (2FA) is a security system that requires two separate, distinct forms of identification in order to access something.

The first factor is a password and the second commonly includes a text with a code sent to your smartphone, or biometrics using your fingerprint, face, or retina.



What is two-factor authentication and why is it used?

Two-factor authentication (2FA), sometimes referred to as *two-step verification* or *dual-factor authentication*, is a security process in which users provide two different authentication factors to verify themselves.

2FA is implemented to protect better both a user's credentials and the resources the user can access. Two-factor authentication provides a higher level of security than authentication methods that depend on single-factor authentication (SFA), in which the user provides only one factor -- typically, a password or passcode. Two-factor authentication methods rely on a user providing a password as the first factor and a second, different factor -- usually either a security token or a biometric factor, such as a fingerprint or facial scan.

Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts because, even if the victim's password is hacked, a password alone is not enough to pass the authentication check.

Two-factor authentication has long been used to control access to sensitive systems and data. Online service providers are increasingly using 2FA to protect their users' credentials from being used by hackers who stole a password database or used phishing campaigns to obtain user passwords.

There are several ways in which someone can be authenticated using more than one authentication method. Currently, most authentication methods rely on knowledge factors, such as a traditional password, while two-factor authentication methods add either a possession factor or an inherence factor.

Authentication factors, listed in approximate order of adoption for computing, include the following:

- A **knowledge factor** is something the user knows, such as a password, a personal identification number (PIN) or some other type of shared secret.
- A **possession factor** is something the user has, such as an ID card, a security token, a cellphone, a mobile device or a smartphone app, to approve authentication requests.
- A **biometric factor**, also known as an **inherence factor**, is something inherent in the user's physical self. These may be personal attributes mapped from physical characteristics, such as fingerprints authenticated through a fingerprint reader. Other commonly used inherence factors include facial and voice recognition or behavioral biometrics, such as keystroke dynamics, gait or speech patterns.
- A **location factor** is usually denoted by the location from which an authentication attempt is being made. This can be enforced by limiting authentication attempts to specific devices in a particular location or by tracking the geographic source of an authentication attempt based on the source Internet Protocol address or some other geolocation information, such as Global Positioning System (GPS) data, derived from the user's mobile phone or other device.
- A **time factor** restricts user authentication to a specific time window in which logging on is permitted and restricts access to the system outside of that window.

The vast majority of two-factor authentication methods rely on the first three authentication factors, though systems requiring greater security may use them to implement multifactor authentication (MFA), which can rely on two or more independent credentials for more secure authentication.

How does two-factor authentication work?

Enabling two-factor authentication varies depending on the specific application or vendor. However, two-factor authentication processes involve the same general, multistep process:

1. The user is prompted to log in by the application or the website.
2. The user enters what they know -- usually, username and password. Then, the site's server finds a match and recognizes the user.
3. For processes that don't require passwords, the website generates a unique security key for the user. The authentication tool processes the key, and the site's server validates it.

4. The site then prompts the user to initiate the second login step. Although this step can take a number of forms, the user has to prove that they have something only they would have, such as biometrics, a security token, an ID card, a smartphone or other mobile device. This is the inherence or possession factor.
5. Then, the user may have to enter a one-time code that was generated during step four.
6. After providing both factors, the user is authenticated and granted access to the application or website.

Two-factor authentication vs multi-factor authentication: Which method adds more security?

Even though both 2FA and MFA add enhanced security measures beyond username and password credentials, **they each provide different levels of assurance** that the person accessing the account is legitimate. So, is MFA more secure than 2FA? The short bittersweet answer is, it depends.

In general, any 2FA or MFA is more secure than single-factor authentication. However, **the security added by any MFA strategy is as strong as the authentication methods chosen by risk professionals**.

MFA is only as secure as the authentication methods chosen

The layered approach adds security, but the inherent low security of a few authentication methods could still maintain low security even with MFA. As an example, an authentication relying on a password (knowledge), one-time password (OTP) (possession), and FaceID (Inherence) are more secure than only using a password, but both passwords and OTP methods are weak in security.

2FA could be more secure than authentication relying on even three authentication factors

On the other hand, a 2FA used by an account supporting Recognition Signals, such as location behavior (Inherence) and Mobile Push (possession), both methods that are among the most difficult to crack, could be deemed more secure than the MFA with three different factors. That is why any MFA strategy is only as strong as the methods used.

The use of mobile recognition signals offers the possibility of stronger authentication methods for MFA.

Added security could also mean more friction, but not always

The more layers added to MFA, the better for security. Higher security can prevent many bad actors from presenting a threat, but if users have to face high friction as well, most likely they will use other services. Users hate friction, particularly in their mobile user experience. In 2018, less than 10%

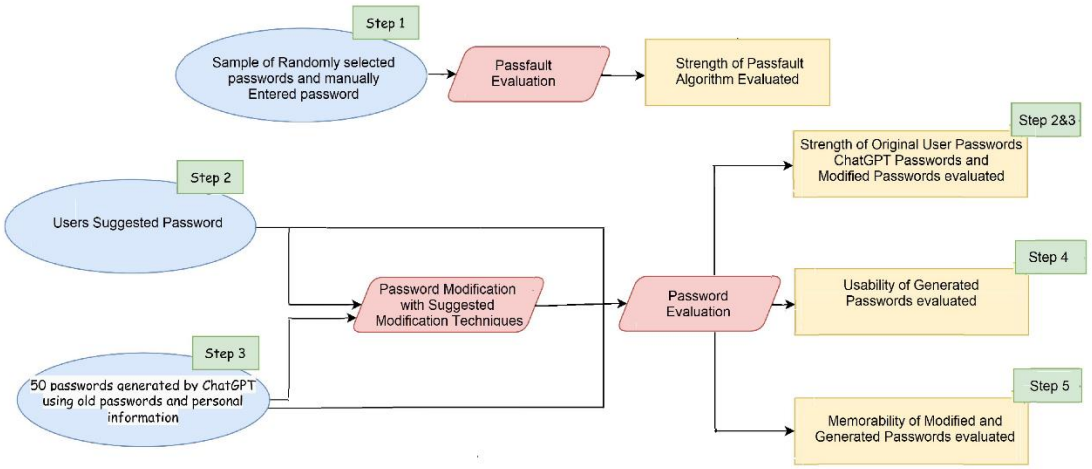
of Google's users had activated optional two-factor authentication (2FA), so, it is clear that users choose a frictionless experience over security when given the chance. Even so, it is a necessity to keep users safe. So, how to give them the choice to have a frictionless experience and still provide an opportunity to choose enhanced security?

Recognition signals on mobile are one of the types of authentication that offer higher security with the lowest possible friction. By using sensors from mobile devices, it is possible to recognize anomalies in user and device behavior, such as location behavior that is not typical for the user. Location is proven to be the strongest trust signal for mobile. Data from Incognia's network shows that 90% of the logins and 95% of the sensitive transactions at financial services Apps happen from a trusted location (a location that is often frequented by the user). That is why Incognia provides zero-factor authentication, an approach that could invoke MFA only when needed, depending on the identification of anomalies in behavior. If the user behavior is identified as trusted, there is no reason why they should face more friction to gain access to their accounts.

Any MFA strategy should rely on the highest security and lowest friction methods possible. 2FA is enough if the authentication methods are used to follow these same guidelines.

Q. 4. Strong Passwords: What makes them weak, how attackers exploit them & how to create secure, memorable one.

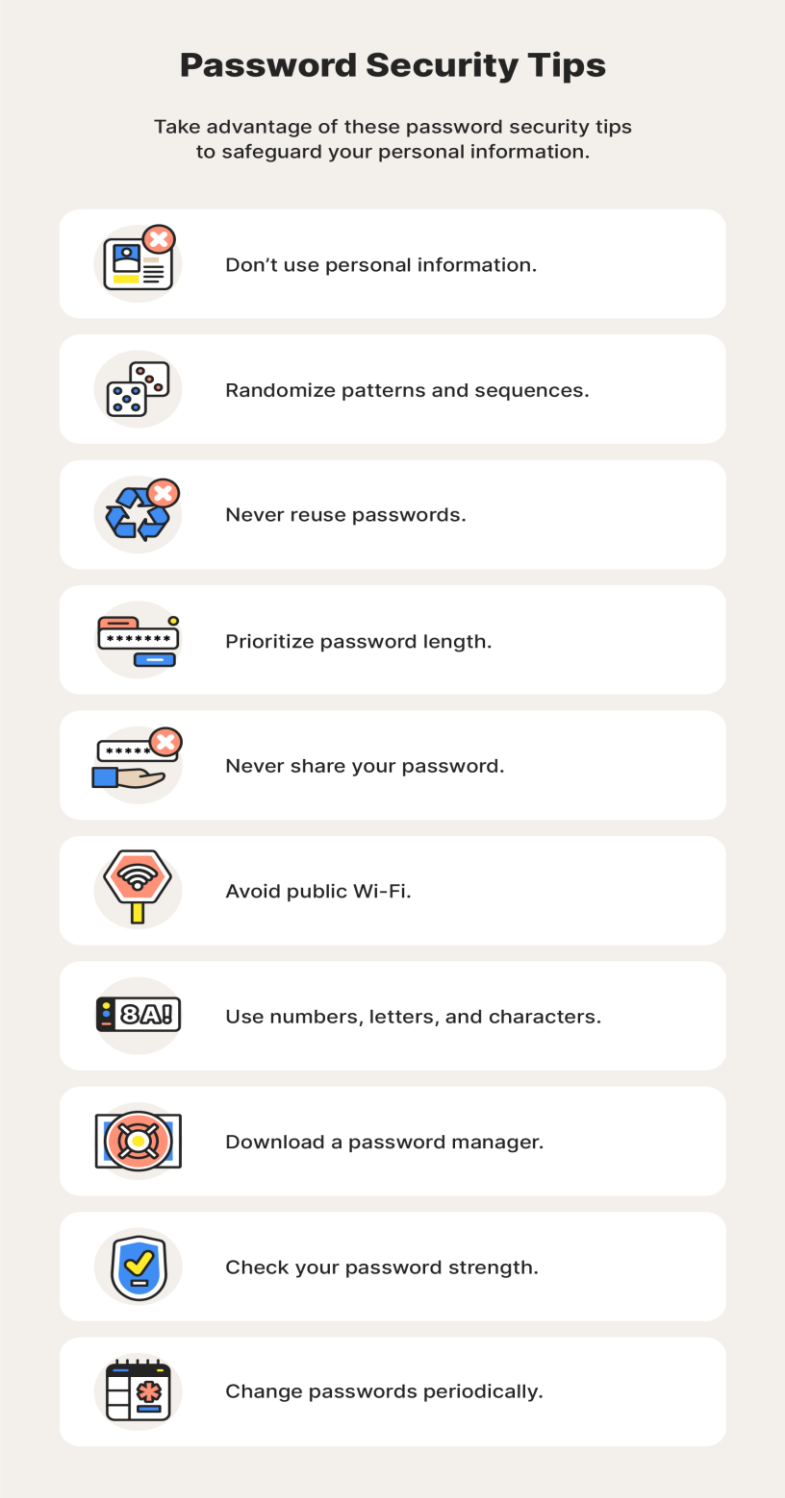
Ans: A strong password is one you **can't guess or crack using a** brute force attack. Progress in the technological sphere leads to improvements in malicious hacker's arsenals, too. Therefore, strong passwords consist of a combination of uppercase and lowercase letters, numbers, and special symbols, such as punctuation. They should be **at least 12 characters** long or even lengthier.



Here are the **main characteristics of a secure and strong password:**

- At least 12 characters long or more
- Combination of uppercase and lowercase letters, numbers, and symbols
- Not a familiar name, person, character, or product
- Is not based on your personal information
- Passwords are unique for each account you have
- Significantly different from your previously used passwords

When you're setting up an online account, there'll often be prompts reminding you to include numbers or a certain number of characters. Some may even prevent you from setting a *weak password,* which is usually one word or number combination that's easy to guess.



But even if you aren't reminded to set a strong password, it's imperative to do so whenever you're setting up a new online account or changing passwords for any existing account.

Phrase	Password
I first went to Disneyland when I was 4 years old and it made me happy	I1stw2DLwIw8yrs&immJ
My friend Matt ate six doughnuts at the bakery café and it cost him £10	MfMa6d@tbc&ich£10
For the first time ever, Manchester United lost 5:0 to Manchester City	4da1sttymevaMU5:02MC

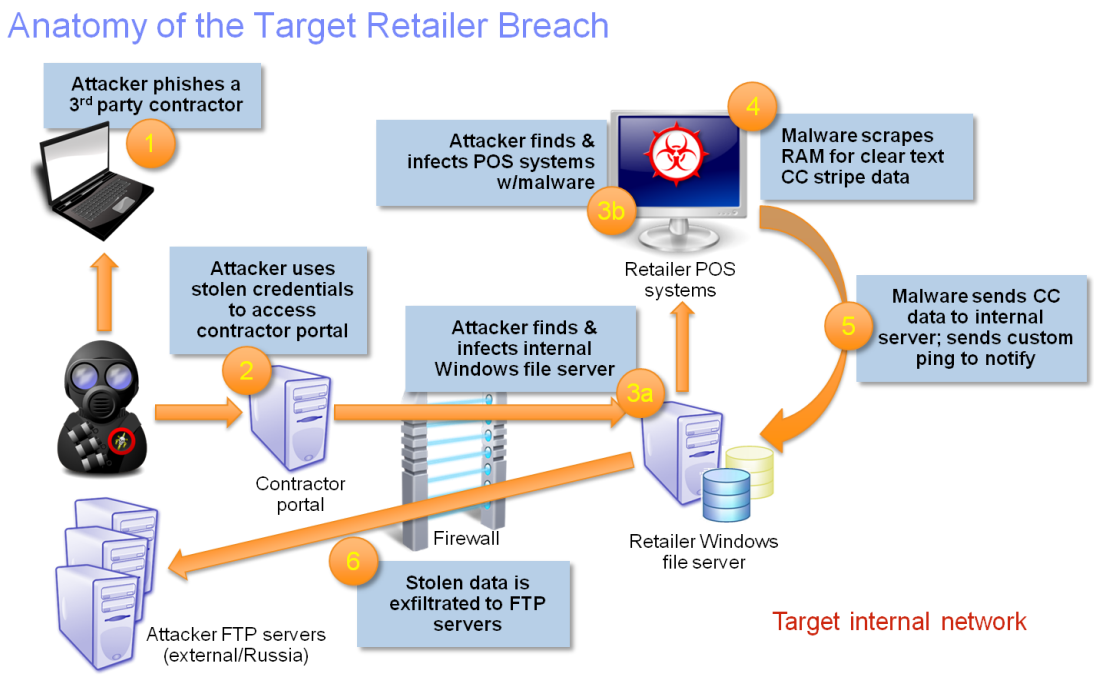
How to keep your strong passwords secure

Now that you've set up a strong password for each of your online accounts, the next step is to keep them safe and secure from hackers or other cyber threats. Here are some of our top **tips for password safety**:

- **Choose a secure password manager**. Use a reputable password manager to generate and store complex passwords securely. Password managers encrypt your passwords and provide easy access.
- **Enable two-factor authentication**. Implement two-factor authentication (2FA) whenever possible. This adds an extra layer of security by requiring a second form of verification.
- **Don't save your passwords locally.** Avoid saving passwords in browsers or locally on your devices. If your device is lost or compromised, locally saved passwords can be easily accessed by unauthorized individuals.
- **Check if your email has been leaked**. Regularly check if your email address has been involved in any data breaches. If your email is compromised, change your password immediately and update it across other accounts.
- **Do not reuse passwords**. Avoid using the same password across multiple accounts. If one account is compromised, using unique passwords ensures that other accounts remain secure.
- **Avoid personal information**. Refrain from using easily accessible personal information such as your name, birthdate, or common words related to you. Hackers often use information readily available online to guess passwords.
-

Q. 5. POS Security Threats: Identify vulnerabilities & suggest solutions for malware, breaches & theft.

Ans: A POS system is still a computer and **susceptible to cyber attacks**. A POS malware attack enters through weak or damaged systems and memory scraping malware goes through the random-access memory (RAM) to locate credit card numbers, gift cards, and other types of data.



1. Unauthorized access to point-of-sale application

Fraudsters exploit mobile point-of-sale apps to steal personal and sensitive information such as credit or debit card information. They then use these to make fraudulent purchases, which results in both financial losses and damaged credit standings for unsuspecting customers.

It's a fact that customers are more likely to buy from retailers that they believe protect their information. Compromised retailers suffer far-reaching consequences from point-of-sale hacks, as their customers may switch to other retailers. That's not to mention enduring a burden of a potential lawsuit, which could leave the company substantially out of pocket.

Combating this fraud is therefore of crucial importance to point-of-sale vendors because it can threaten the very existence of the business itself, and has a devastating impact on retailers, the core customer of point-of-sale vendors.

It is vital for point of sale vendors to improve the security of point of sale applications and to make it easier to identify suspicious and fraudulent POS transactions and act on them to protect shoppers' sensitive data.

2. Malware targeting point-of-sale application

Mobile malware is quickly becoming one of the main ways that cybercriminals steal payment card details. Malware is used to obtain sensitive information, and in some cases to even steal money directly from bank accounts. Retailers are vulnerable to point-of-sale malware attacks and remain so until they implement the right security technology to strengthen their point-of-sale applications.

An effective application security technology should be able to detect malware, tampering, rooted/jailbroken point of sale devices, and more, so that point-of-sales providers can act before it's too late. The right application security technology needs to include a feature that alert retailers and POS providers when it is not safe to use mobile POS devices for making payments or performing other electronic transactions.

3. Cyberattacks against the point-of-sale application backend system

A point-of-sale application running on a smartphone, a tablet or a mobile device is only a single component in a full, intricate point-of-sale system. The majority of business transactions are processed on the server's side. That means most cyberattackers use the entry point from the point-of-sale application to the server to begin their attack on internal business systems.

Once the cyberattackers get inside the data center of POS vendors or retailers, not only can they access the compromised POS application, but also all other POS applications used by the retailer in other locations. Attacking the entry point at the backend is a common attacking method, and countless large-scale security breaches have been caused by this method.

Therefore, it is essential that this entry point is kept secure and protected. Point-of-sale application backend systems and other business systems hosted in the data center need to be shielded from direct internet exposure. Otherwise, hackers could easily exploit a single weakness to access numerous POS retail apps.

For retailers to trust a mobile point of sale application, they need to feel comfortable operating mobile POS apps without the risk of having their internal business systems hacked and risk being sued by affected customers.

4. Business disruption due to poor unavailability of point-of-sale applications

Retailers not only want their business and customer data to be kept safe, but also expect that there will be no disruption to their business caused by cyberattacks or technical downtime with their point of sale applications. Retailers want to operate point of sale applications in a secure, reliable way, and prevent attacks before they even happen. For this to happen, the ideal point of sale application needs to not only boast strong POS security technology but also feature a reliable security monitoring and incident

response service. This service should alert IT personnel- either in-house or outsourced to a third-party outsource- when there is a breach, and also monitor POS application-related activities, detect and flag up threats, and provide real-time responses to any problems.

Having a reliable POS security monitoring and incident response service in place help POS providers to assure their retailer customers, and give them a peace of mind as they process countless of data transactions via point-of-sale applications.

If you are a provider and operator of POS application, you want to pay attention to these four common security issues affecting point-of-sale applications. If you make sure that each of them is covered, then you can rest assured that your POS application is secure, and you putting yourself at unnecessary risk of cyberattacks