

DESKTOP SECURITY



Best Practices

- Use genuine Operating System and Software.
- Keep your Operating System updated.
- Install anti-virus and anti-malware solutions and keep them updated.
- Use strong login password and change them periodically.
- Regularly take backups of your important files and data.
- In-case of incidents such as hardware failure, or cyberattacks, having backups can help you restore important information.
- Maintain multiple copies of critical data in different locations to prevent loss in case of disasters.
- Periodically test and verify your backups to ensure they can be used for restoration when needed.



BROWSER SECURITY



Best Practices

- Update your web browser with the latest patches.
- Disable pop-up windows in your browser.
- Delete browser cookies and cache regularly.
- Have "Safe Search" ON in Search Engines.
- Enable private browsing or incognito mode.
- Be careful with the websites you visit.
- Check the URL of a website to make sure that it has the "https://" or a padlock icon.



E-MAIL SECURITY

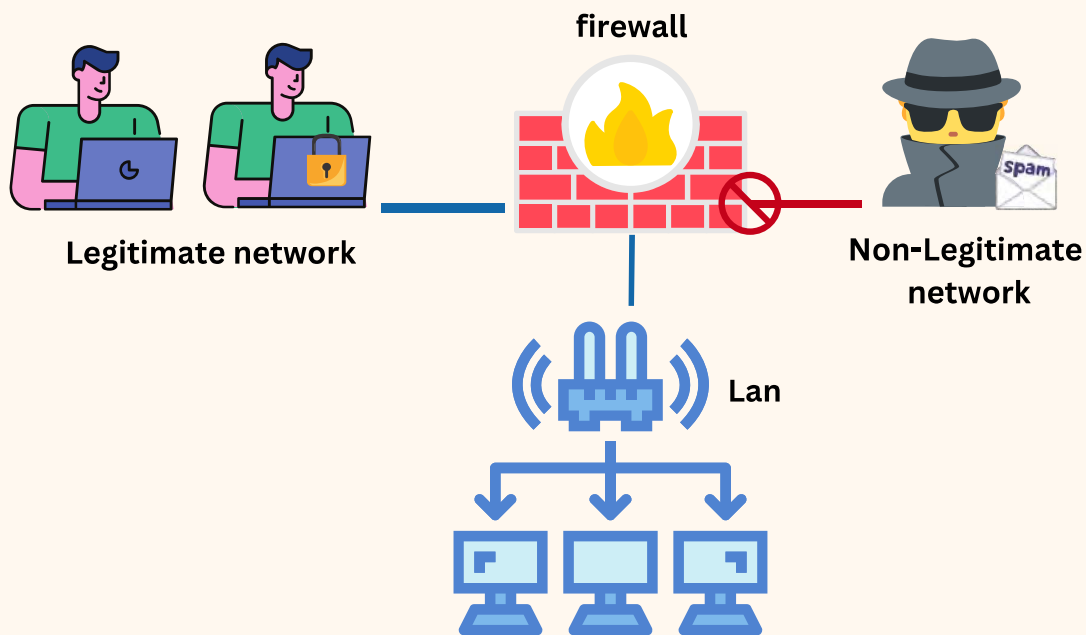


Best Practices

- Verify the sender before clicking on any link/ attachment.
- Check the domain name in the email address of the sender. Look for misspelled or typo errors.
- Don't click any link/attachment from suspicious emails received from strangers.
- Do not use official email accounts for online shopping or ticket booking.
- Do not click on shortened URLs received in emails/ chats/ messages without verifying them by expanding the URL.
- Use strong passwords.
- Enable Multi-Factor Authentication (MFA).
- Do not store Username and passwords in public systems.



FIREWALL SECURITY



Best Practices

- Always make sure the firewall is hardened and configured properly.
- Keep the software updated with the latest updates.
- Regularly update firewall protocols.
- Review and update access controls on a regular basis.
- Implement a comprehensive logging and alert mechanism.
- Set up procedures for backup and restoration.
- Perform regular audits of firewalls.



BROADBAND SECURITY



Best Practices

- Always download broadband drivers from the legitimate websites recommended by the manufacturer.
- Change the default administrator or admin password of broadband router modem given by manufacturer .
- Install broadband Internet bandwidth usage monitoring tool.
- Enable SSH (secure channel) for remote administration.
- Power-off the modem router after completing the Internet access.
- Do not enable auto-connect to open Wi-Fi networks.
- Don't use USB broadband modem with insecure computers / Laptops.
- Use effective end point security solution (with anti virus, anti spyware, desktop firewall etc) to protect PC / Laptop from broadband Internet threats.



DATA SECURITY



Best Practices

- Encrypt sensitive data to protect it from unauthorized access.
- Enable Multi Factor Authentication (MFA) to add an extra layer of security to your accounts.
- Be cautious when working with sensitive information in public places or on shared devices.
- Avoid using easily guessed or common passwords.
- Use different passwords for different accounts.
- Avoid using public Wi-Fi to do secured transactions.
- Use strong passwords to lock your devices.



VPN SECURITY



Best Practices

A Virtual Private Network (VPN) is a service used for establishing a secure connection over the Internet.

- Keep your VPN software up to date with the latest security patches.
- Monitor and enable logs of VPN activity to identify and address suspicious activity.
- Select VPNs that follow standard security protocols.
- Configure VPN with all web application security settings enabled.
- Use strong passwords for VPN accounts.



BENEFITS OF USING ANTI-VIRUS SOFTWARE

1



An essential step in preventing and identifying malware infection is installing antivirus software from a trustworthy vendor

2



Realtime protection by system scanning and blocks malicious pop-ups and ads

3



Alerts malicious files present in internal and external devices

4



Alerts when visiting infected or malicious websites

5



Keeping them updated helps to improve protection against latest threats



PASSWORD MANAGEMENT BEST PRACTICES

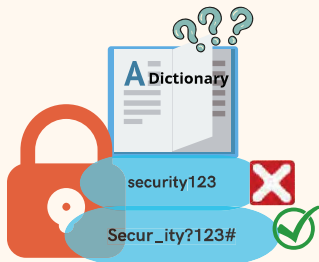
1



Use Strong and long passwords


Always prefer to create lengthy passwords.
Short length passwords are easy to crack.

2



Don't use dictionary words as passwords

Such passwords are too easy to crack.

 Dictionary words are vulnerable to brute-force attack by hackers.

3



Create passwords using special characters

Passwords mixed with uppercase, lowercase, numerals and special characters are difficult to crack

4



Change passwords periodically

Avoid using guessable patterns of password.

5



Enable Multi Factor Authentication

MFA adds another layer of security to your accounts.



BACKUP-BEST PRACTICES



Best Practices

- Backups of the system, application and data should be performed on a regular basis.
- Ensure that a valid, virus-free backup exists and is available for use at any time
- Up-to-date backups of all critical items should be maintained to ensure the continued provision of the minimum essential level of service.
- Back-up procedures should be documented, scheduled and monitored.
- The backups must be kept in an area physically separate from the server.
- Offline backups with encryption for critical systems should be maintained.
- Online backup systems should be properly hardened and access to its network should be strictly restricted.

