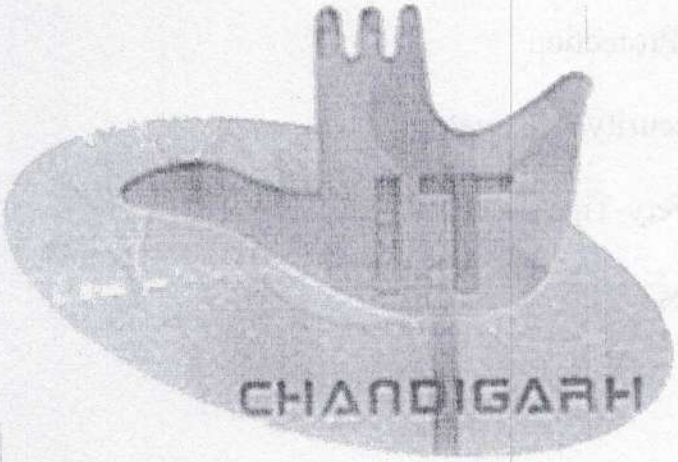
Cyber Hygiene
for
Cyberspace
Do's & Don't s



Department Of Information Technology
UT, Chandigarh

Contents

Computer Safety Tips

Computer Security

Computer security is the protection of computer systems and information from theft and unauthorized access. It is the process of prevention and detection on of unauthorized use of the computer systems.

Computer security Threats

Computer security threats are possible dangers that can cause impediment to the normal functioning of the computer. Some of the common and harmful computer threats are depicted below:-

- Computer Viruses
- Computer Trojans
- Phishing Mail/URL
- Botnet Keylogger
- Keylogger

Dos

Computer Safety Trips

- Always download application/ software from trusted sources
- Regularly update Operating System, Applications and Anti-Virus software of the system
- Ensure backup of important data/files/ documents at regular intervals
- Lock the computer screen when not in use
- Always keep the computer firewall "ON"
- Use account with limited privileges on systems
- Always insist on using genuine/ licensed so ware applica ons
- Scan all the files/contents downloaded from websites, e-mails or USBs
- Uninstall unnecessary programs or so}ware
- Use "Task Manager" to iden fy any unwanted programs running on the computer system
- Access to servers should be allowed via Mul -Factor Authentication on (MFA)
- Disable Remote Desktop Connec}on and network file sharing , when not in use Set Opera ng System update se ngs to "Auto-Download" op on for regular updates

Don'ts

- Do not install or use pirated copies of so ware/ applica ons under any circumstances. These may contain malware
- Do not use guessable/weak passwords like "password@123", etc.
- Do not click on untrusted/unexpected Pop-Up adver sements/ programs
- Do not dispose computer or hard drive without dele on and wiping of data

USB device Security

USB devices are very convenient to transfer data between different computers. One can plug it into a USB port, transfer important data, remove and use it appropriately as desired. However, this portability, convenience and popularity also bring different threats to the information system.

THREATS

Unsecured use of USB drive can lead to data the□s, data leakages and malware infection. USB security can be ensured with care, awareness and by using appropriate scanning tools to secure the information.

TYPES OF DEVICES WHICH SUPPORT USB

- Flash Drive/ Pen drive
- Portable Hard Drive/ SSD
- Mobile Phone
- Digital Camera
- Card Reader
- USB Keyboard/ Mouse

USB DEVICE SECURITY

- Scan USB device with Antivirus /Endpoint Protection before its Use.
- Autorun/ Autoplay feature shall be disabled in all the computers, while using USB

Password Security Management

Password helps in protection of information accessible via computers. It allows access to information only to authorised users. Strong multi character passwords must be enforced in all the systems.

Password attack

Cyber criminals use many methods to access accounts, including dictionary brute-force attack (attacks made to guess passwords), as well as comparing various word combinations against a dictionary file. Cyber criminals may also use password capturing tools like "Keyloggers" on victim's computer.

Do's

- Always use different passwords for different accounts. Ensure password is strong.
- Strong passwords should contain combination of upper case, lower case, numbers," Special" characters (e.g., @#$%^&*()_+|~--= etc.
- Immediately, change any password which might have been shared or revealed by mistake.
- Passwords must be changed at regular intervals.

A password should not contain

- Birth dates, names, ID proofs and other personal information such as addresses and phone numbers.
- Commonly used words such as names of family members, pets, friends, colleagues, movie/novel/comics characters, etc.
- thirteen characters Password recovery answers should not be guessable
- Password should not be less than eight characters.

Don't

- Do not use public systems to access banking/ sensitive sites.
- Do not share password, OTP through e-mail, chat or any other electronic communication.
- Do not reveal password on questionnaires or security forms.
- Do not choose/ select "remember my password" option for banking/ sensitive sites.
- Never write down your password anywhere, especially as a 'note stick' to the computer.
- Don't use your biometrics (fingerprint, etc.) at untrusted terminals/places.

General Internet safety Precautions

Invention of internet has revolutionized the way of communication and information sharing. However, unsecured usage of internet may pose risks to an organization. Internet security includes browser security, website security, network security, software applications, etc. Its objective is to enforce rules and measures against attacks over the Unsafe internet practices may lead to risks from phishing, online viruses, trojans, worms, ransom ware, business email compromise, financial loss etc.

Do's

- clicking/downloading from suspicious links/URLs
- clearing browser history after confidential activities/transactions
- Cloud storage to be used with appropriate security/ privacy settings.
- Verify the Authenticity and Identity of social media profiles before getting involved in any correspondence.
- Be vigilant and verify the advertisements/ sponsored contents on search results or websites

Don't

- Do not use any public computer or Wi-Fi for carrying out financial transactions like online shopping, internet banking, UPI transaction, etc.
- address, phone number and details of payment cards on untrusted and unsecured.
- Do not trust and share unverified content on social media and messaging apps.

Financial Transaction - Safe Practices

Digital modes of payments like internet banking, UPI, cards, mobile banking have made day-to-day payments very convenient. Any security lag in online transactions may result in financial loss to an individual or an organization.

Do's

- Keep your UPI PIN safe and do not share with anyone.
- UPI PIN is not needed while receiving payments.
- Protect device and payment app with strong passcode.
- Verify the name of "Payee" or QR code before proceeding with the payment.
- Card Number, Expiry & CVV number are confidential. Never share with anyone.
- Use cards only after verifying authenticity of PoS/terminals/ATMs and websites.
- Sharing OTP may result in unauthorized debits.
- Use genuine/licensed Operating System for internet banking transactions.
- Verify Internet Banking URLs received in SMS/Email before entering your credentials Public computers and insecure internet connections must be avoided Use a strong internet banking password which is different from other accounts likee-mail, e-commerce,etc. Example-https://retail.onlinesbi.com ,http://xyz.com/SBIBank.
- Public computers and insecure internet connections must be avoided.
- Use a strong internet banking password which is different from other accounts like e-mail, e-commerce,etc.
- Privacy settings must be carefully chosen before sharing any content over internet.
- Be vigilant before revealing your location information over the internet.
- Friend requests must be accepted after verification with proper caution.
- Content posted on social media must be verified for authenticity before forwarding /sharing.

Don't

- Do not use social media account without Multi-Factor Authentication (MFA).
- Never log into social media accounts from untrusted systems.

Mobile phone safety

Mobile phones are integral part of any organization. Secure usage of phone is essential for personal and organizational data protection. Data theft, financial loss, unauthorized access, malware infection, etc. may be a result of mobile phone compromise.

Do's

- Be cautious with public Wi-Fi
- Information shared over public network may be misused.
- Review the default privacy settings of the smartphone, mobile applications and social media accounts media accounts.
- Personal photos posted on social media with public visibility may be misused.
- Before downloading any App, same should be checked for its reputation/ authenticity.
- Read vendor privacy policies and verify app permission before downloading apps mobile phone safety.
- Prefer downloading mobile apps from genuine source.
- Turn off / remove unnecessary apps.
- Register for Do Not Disturb (DND) service with Telecom Operators
- Use Parental control mode, while handing over mobile phones to kids or minors.
- Use device / SD card encryption to safeguard confidential data.
- Protect your device with a strong PIN/Password or Biometrics and enable auto lock setting in Mobile phones.
- Always take back-up of data (contacts, personal photos, etc.)

Don't

- Do not reply or click on link sent through SMS, e-mails or chat messenger by strangers.
- Do not store any classified/ sensitive data (text /video /photograph) in the device.
- Do not log into accounts, especially the financial accounts, when using public wireless networks.

Malware protection wireless networks

The Term Malware is a combination of words, 'Malicious' and 'Software'. Malware is intentionally developed to perform various unauthorized and destructive tasks on the victim's system without one's knowledge. Malware performs various tasks that include locking of important files, stealing sensitive information from the system, gaining unauthorized remote access, spy on the user activity, consuming computer memory, internet bandwidth, corrupting important files, etc. The various types of malwares are spyware, viruses, worms and trojans, ransomware, Botnet, etc.

How to protect against malware?

Keep all software up to date, including the Operating System and applications.

- Do not click on untrusted URL links.
- Use an-malware solutions.
- Patch Management to be ensured to overcome vulnerabilities.

Do's

- Scan USBs, Files on your computer regularly or before use. Disable USB devices if not needed.
- Use Licensed Version of Operating Systems and Application Software.
- Keep your system and Anti-virus up-to-date with regular patches.

E-MAIL SECURITY PRACTICES

Don't open/reply to e-mail links (hyperlinks/ web-links/ URLs mentioned in the body of such mails) giving any luring offer. It may result in compromising your personal and financial details. Do not access to any spam e-mails, until the sender is properly verified.

Do's:

1. **Keep Software Updated**: Regularly update your operating system, browsers, and applications to patch security vulnerabilities.
2. **Use Strong, Unique Passwords**: Create complex passwords using a mix of letters, numbers, and symbols. Consider using a password manager.
3. **Enable Two-Factor Authentication (2FA)**: Add an extra layer of security to your accounts by enabling 2FA wherever possible.
4. **Be Skeptical of Emails and Links**: Verify the source before clicking on links or downloading attachments. Phishing scams often disguise themselves as legitimate communications.
5. **Secure Your Network**: Use a strong password for your Wi-Fi network and consider using a VPN when accessing public networks.
6. **Monitor Your Accounts Regularly**: Frequently check your bank and credit card statements for any unusual activity.
7. **Backup Important Data**: Regularly backup your data to an external hard drive or cloud service.
8. **Use Security Software**: Install reputable antivirus and anti-malware software and keep it updated.
9. **Educate Yourself**: Stay informed about the latest cyber threats and scams.
10. **Verify Website Security**: Ensure that websites are secure (look for "https://" and a padlock icon) before entering sensitive information.

Don'ts:

1. Don't Click on Suspicious Links: Avoid clicking on links in unsolicited emails or messages.
2. Don't Share Personal Information Unnecessarily: Be cautious about what personal information you share online and with whom.
3. Don't Use the Same Password for Multiple Accounts: If one account is compromised, others could be at risk.
4. Don't Download Unverified Apps or Software: Only download software from trusted sources.
5. Don't Use Public Wi-Fi for Sensitive Transactions: Avoid accessing your bank accounts or other sensitive services over public Wi-Fi.
6. Don't Fall for Scare Tactics: Scammers often use fear to trick you into revealing personal information or transferring money.
7. Cyber frauds happen in no time. Do not share your personal details like card info, bank account, Aadhar, PAN anytime.
8. Cyber scams will take you by surprise, Don't click on unknown links Be wise.

9. You might be next victim of cybercrime, never respond to ' Request Money' option from unknown sources.
10. Cyber scamsters carefully set their trap, Don't install app and software from unknown resources.
11. Cyber scams are on the rise, don't share your PIN, card details and pay a heavy price.
12. Don't Ignore Updates: Failing to update your software can leave you vulnerable to security threats.
13. Don't Give Out Personal Information Over the Phone or Email: Be skeptical of unsolicited requests for your information.
14. Don't Leave Devices Unattended: Ensure your devices are secure, especially in public places.
15. Don't Use Weak Security Questions: Choose security questions and answers that are difficult to guess.
16. Staying vigilant and following these guidelines can significantly reduce your risk of falling victim to cyber fraud. Stay safe!

Cyber Safety Tips for Government Employees

Do's:

1. Use Strong Passwords:
   - Create complex passwords with a mix of uppercase, lowercase, numbers, and special characters.
   - Use a password manager for securely storing passwords.
2. Enable Multi-Factor Authentication (MFA):
   - Always use MFA for email accounts, official portals, and sensitive systems.
3. Keep Software Updated:
   - Regularly update operating system, applications, and antivirus software.
4. Verify Emails and Links:
   - Be cautious with unexpected emails, especially if they contain links or attachments.
   - Hover over links to check their destination before clicking.
5. Secure Devices:
   - Lock devices with strong PINs or biometric authentication.
   - Use encryption for sensitive data on laptops and USB drives.
6. Report Suspicious Activity:
   - Immediately inform the IT Head/Technical Person of any phishing attempts, data breaches, or suspicious emails.
7. Use Secure Networks:
   - Use only secure and trusted Wi-Fi networks; avoid public Wi-Fi or use a Virtual Private Network (VPN) when connecting.
8. Back-Up Data Regularly:
   - Store backups securely, and ensure they are tested and up-to-date.
9. Follow Government Policies:
   - Adhere to the cybersecurity guidelines and policies issued.

Don'ts:

1. Don't Share Passwords:
   - Never share your login credentials with colleagues or external parties.
2. Avoid Unsecured Devices:
   - Do not use personal or unauthorized devices for official work.
3. Don't Open Suspicious Attachments:
   - Refrain from opening attachments from unknown sources or unverified senders.
4. Don't Use Guessable Passwords:
   - Avoid using easily guessable passwords like "123456" or "password."
5. Avoid Untrusted Websites:
   - Refrain from visiting non-secure websites (look for "https" and a padlock symbol).
6. Don't Install Unauthorized Software:
   - Avoid downloading or installing software without proper authorization.
7. Don't Leave Devices Unattended:
   - Lock computers and devices when leaving them unattended, even for a short period.
8. Don't Click on Unknown Links:
   - Be cautious of links in emails, SMS, or social media, especially those promising rewards or urgent actions.
9. Don't Ignore Security Alerts:
   - Take immediate action on security alerts or warnings.
10. Don't Use USB Drives from Unknown Sources:
    - Avoid connecting external storage devices unless they are scanned and approved by IT.

References

1. Ministry of Home Affairs:
https://www.mha.gov.in/en/divisionofmha/cyberandinformation-security-cis-division

********** End of Document **********