SECURITY MEASURES TO PROTECT DATA

SECURITY MEASURES FOR INDIVIDUALS:

- Regular Backups: One of the easiest yet most effective ways to avoid data loss or to lose important and crucial files is by taking a backup of data regularly. There are many ways to take backup and it is up to each individual how many copies of your data they wish to keep. While external hard disks are a common way to take backup, these days cloud computing too proves to be a cheap and easy way to maintain a backup of all files at a safe location. It won’t prevent data loss but would at least ensure that no important information is lost.

- Establish strong passwords: The first step that every business must most take is to establish strong passwords for all your accounts, bank details and other kinds of accounts. Also, one must try to keep very strong passwords that may not be easily guessed by anyone. The passwords must be a combination of characters and numbers. The password must be easy to remember for you but should not be your birthday, your name, or any other personal detail that anyone else could guess. The password must be between 8-12 characters long, at least.

- Secure Mobile Phones: Smartphones too hold a lot of important and confidential data such as messages, bank account details, and emails, etc. thus it is important to secure mobile phones as well. There are many ways to secure mobile phones and some of them include, establishing strong passwords, to have encryption software, to have remote wiping enabled and to opt for phone finding apps so that phone can be located if it is lost or stolen.

- Surf Safely: Individuals must be careful when surfing the internet. It is a common practice to click on certain links or attachments thinking that they are harmless, but they could lead to data hacking or planting of malicious files. This may infect the system and may squeeze out information. Thus, it is important to surf safely, use internet security software and never give out personal information and bank details to sites that are not trustworthy. Individuals should beware of the vulnerabilities and avoid being casual when using the internet.

- Encrypting data: Modern tools make it possible for anyone to encrypt emails and other information. GPG for Mail, for example, is an open source plug-in for the Apple Mail program that makes it easy to encrypt, decrypt, sign and verify emails using the OpenPGP standard. And for protecting files, newer versions of Apple's OS X operating system come with FileVault, a program that encrypts the hard drive of a computer. Those running Microsoft Windows have a similar program.

- Anti-malware protection: Malware is a serious issue and it's known for cropping up in inconspicuous places, not known to users. Anti-malware protection is essential for laying a foundation of security for all electronic devices. Malware includes computer viruses, worms, trojan horses, spyware, and more. It can be present on websites and in emails, or hidden in downloadable files, photos, videos, freeware or shareware. The best way to avoid getting infected is to run a good anti-virus protection program, do periodic scans for spyware, avoid clicking on suspicious email links or websites.

- Keep operating system up to date: Operating system updates are a necessary evil, as these updates contain critical security patches that protect computers from recently discovered threats. Failing to install these updates puts the computer at risk. Hence, it's important that you update it regularly.

- Use an encrypted cloud service: Cloud storage makes for an ideal backup solution, but it can also be prone to hackers if users are not careful about the cloud services they choose. To use cloud services safely, it is important to encrypt the data stored in cloud or use cloud services that encrypt data themselves. Some cloud services provide local encryption and decryption of stored data. This ensures that stored data is safe from unauthorised access. Even service providers and administrators can not access this data without the necessary privileges. This is known as zero knowledge policy.

- Securing bluetooth connection: Bluetooth technology has offered incredible conveniences to the mobile world, but it also opens the door for vulnerabilities. Most threats exploiting Bluetooth connectivity are dependent on the active Bluetooth connection, and while they aren't typically devastating or dangerous, they're certainly inconvenient and can be serious. Bluetooth attacks depend on exploiting the permission request/grant process that is the backbone of Bluetooth connectivity. The only way to completely prevent attackers from exploiting permission request/grant process is to power off the device’s Bluetooth function when it is not being used and not putting it into an invisible or undetectable mode, but completely turning it off.

- Sharing personal information: When sharing personal information, individuals must take into account the following: Who is asking for personal information? Why do they need it? How will they use it? What security measures do they have in place to ensure that your private information remains private? When in doubt, information should be withheld.

- Sharing passwords: Passwords should not be shared without concern; rather, it is important to determine when another person legitimately requires access to an individual’s personal information or account and grant access on a case-by-case basis. If another person needs access for a single, isolated purpose, password should be changed after the task is completed and they no longer need the access.

- Shredding old documents: One of the most common methods used by hackers to steal personal information is dumpster diving, which entails rummaging through trash looking for old bills or other documents that contain personal information. So it is important to shred old documents to ensure adequate data protection.

- Dealing with spam emails: If an email is received from an unknown source or individual, best practice is not to open it, and definitely avoid clicking any links or file attachments. Delete email from unknown sources. Watch out for files attached to e-mails, particularly those with an 'exe' extension. Some files transport and distribute viruses and other programs that can permanently destroy files and damage computers and websites. Forwarding an e-mail should be avoided when sender of the e-mail or the attachments are suspicious.

- Different addresses for different contexts: A good strategy is to use a different email address for different contexts, such as one for personal accounts, one for business-related accounts, one for online retail accounts, and so on. This minimises the impact if an email account is hacked.

- Saving passwords: The common practice of 'remembering passwords' in browsers is a dangerous practice. Indeed, should someone gain access to an individual’s computer or mobile device, they'd be able to easily access any accounts for which login credentials are saved in the browser. While it may make logging in more convenient, it's a risky habit in terms of data protection.

Security measures to protect government:

- Anti-Virus protection: The government should invest in effective antivirus programs. Free anti-viruses will only provide the basic level of protection. The government should buy the premium version of reliable solution provider that will offer the fool-proof security to their systems. It acts as the first line of defence against security attacks and prevents them from causing damage to your sensitive data. It takes care of a variety of security threats such as malware, viruses, spyware and adware. Some even offer email protection and prevent harmful downloads.

- Firewall protection: One of the best ways to protect the network is to install a firewall. Although, it is an old technique to secure the network but it is very effective even today. It keeps the network secure by managing internet traffic coming in and going out of the network.

- Setting password guidelines: The passwords used should never contain any personal data, common words spelled backward and sequence of character and numbers. As suggested by security experts the password generated should be hard to guess and contains combination of numbers, upper and lower case letters and symbols to make it hack-proof. The ideal length of passwords should be anywhere around 10-12 characters. If the above guidelines are followed the password can be prevented from getting in wrong hands.

- Protect wireless networks: Wireless networks are at a greater risk of cyber-attacks as compared to a wired network because of its open nature and comparatively weaker control. Therefore, it is important to pay extra attention towards securing the wireless networks. Use WPA2 (Wi-Fi Protected Access Version 2) technology to secure the wireless network. If government institutes are still using old technology such as WEP (Wired Equivalent Privacy), they should switch immediately to latest wireless security because they are much more secure than their older counterparts. The network can be made stronger by adding a layer of security by using complex PSK (Pre-Shared Key).

- Software updates: It is quite unfortunate to see many government institutions still using old software and operating system. The problem with that approach is that it makes systems more vulnerable to security attacks. The government should always ensure that they use good software but more importantly, they should keep them updated to the latest versions. The advantage of using updated software is that it fixes many bugs and loopholes that a hacker can exploit and protect them from cyber-attacks.

- Regular reviews of user access control: On a semi-annual or annual basis, government's IT team should sit down with employees who access data from data lakes and repositories, and review data access permissions for all authorised personnel. Access permissions can be adjusted upward or downward based upon employee/contractor work responsibilities. When employees/contractors are no longer employed with the company, they should be immediately removed from access.

- Data masking: In some cases, masking can be used to redact sensitive data elements (e.g., social security numbers, names). While giving access to employees of the database this technique can be employed as per the requirement. So this data isn't shared with all employees and they cannot make use of it.

- Automatic Screen Savers: Most systems allow for screensavers to activate after a period of inactivity on a computer, requiring a password to re-establish access. This automatic lock activation is useful as the alternative manual locking of a workstation requires positive action by the user every time he/she leaves the computer unattended.

- Use of Smart card / tokens: These are devices that provide authentication either by generating a code to be entered or containing a chip that authenticates with the system being accessed. The token generates a PIN number that is valid for a very short period of time. This is used in conjunction with a username and password to authenticate the user.

- Monitoring Remote Access: When a government staff member/contractor is allowed to access the network from a remote location (e.g. from home or from an off-site visit) such access creates a potential weakness in the system, not least when accessed from a wireless network. For this reason the need for such access should be properly assessed and security measures reassessed before remote access is granted. If feasible, the access should be limited to specific IP addresses. Security should be the first consideration in granting access to partner organisations.

- Logs and Audit Trials: Access control systems and security policies are undermined if the system cannot identify abuses. Consequently, a system should be able to identify the user name that accessed a file and the time of the access. A log of alterations made, along with author/editor, should also be created. Logs and audit trails can help in the effective administration of the security system and can deter staff members tempted to abuse the system. Staff should be informed that logging is in place and that user logs are regularly reviewed. Monitoring processes should focus not only on networks, operating systems, intruder detection systems and firewalls, but should include remote access services, web applications and databases.

- Physical Security: Physical security safeguards should include the following considerations: Perimeter security (monitoring of access, office locked and alarmed when not in use), Restrictions on access to sensitive areas within the building (such as server rooms), Computer location (so that the screen may not be viewed by members of the public), Storage of files (files not stored in public areas with access restricted to staff with a need to access particular files) and Secure disposal of records (effective "wiping" of data stored electronically; secure disposal of paper records).

- Portable Devices: Laptops, USB keys, smart phones and other forms of portable device are especially vulnerable to theft and accidental loss. Where a data controller considers it essential to store personal data on a portable device, these devices should be encrypted. Whole disk encryption should be used to mitigate against storage of files outside of an encrypted segment of the disk. In the case of smart phones, a strong password should be required at start up and also after several minutes of inactivity. When such a device is lost steps should be taken immediately to ensure that the remote memory wipe facility is activated. Staff allocated such devices should be familiar with the relevant procedures.

- Educating Employees: Despite establishing a secured infrastructure, government may end up losing the data. This happens because the employees do not have adequate knowledge. Government should inform them about the latest technology trends and security threats. By educating the employees, government can eliminate the risks of malware and ransomware. Malware can enter the system through multiple channels but one of the most common among them is malicious links, which the employees click. Cyber attackers use social engineering to conduct ransomware attacks. Government can easily prevent these common ransomware attacks from harming their systems by creating awareness among your employees.

References:

https://blog.taskque.com/data-security-measures/

https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe