Protecting Yourself from Data Breaches

What is a Data Breach?

A data breach, in relation to personal data, refers to any unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data. It also includes the loss of any storage medium or device, on which personal data is stored, in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

For individuals, the data breached may include Personally Identifiable Information (PII) such as an individual's name, NRIC number, mobile number, address, email address, bank account number or credit card details. Threat actors may use such information to carry out targeted phishing attacks or compromise other accounts, such as resetting passwords or requesting for One-Time Passwords.

As the number of data breaches reported has increased globally, there is a need for individuals to be vigilant and take steps to prevent them. Practising good cyber hygiene measures can help to mitigate the impact of having their data exposed, in the event of a data breach.

This advisory provides information on the common causes of data breach, preventive measures that individuals can take, and how to respond to a data breach. It comprises the following sections:

Common Causes of Data Breach

Weak/Stolen Passwords

Weak password management facilitates threat actors' unauthorised access into a system. This includes the use of weak passwords, such as those that comprise personal information or easy-to-guess passwords. Passwords are the keys to a lock and should be safeguarded in both the physical and cyber realms.

Unpatched Vulnerabilities

Vulnerabilities which are left unpatched could be exploited by threat actors to gain unauthorised access into networks or systems to perform various malicious actions. These include modification of files, data exfiltration, and installation of malware, including ransomware.

Social Engineering

Social engineering is the use of psychological manipulation to obtain sensitive credentials from victims. Phishing, the most common type of social engineering, is a technique used to obtain sensitive information such as login credentials or credit card details. A phishing email is an email disguised as being sent from a legitimate entity, with the motive of tricking victims into clicking on a phishing link. Clicking the link will lead to a phishing page which would request for the victims' confidential details or cause the victim's computer to be infected with malware. Phishing may also be conducted via SMS or social media.

Insider Threats

Insider threats may take the form of deliberate actions by disgruntled/rogue employees who knowingly leak data to competitors or sell them for financial gain. They may also take the form of unintended actions by careless employees who lose data-storage devices or send confidential emails to the wrong recipients.

Cybersecurity Measures for Individuals to Manage Devices and Online Presence

To reduce the risk and mitigate the impact of having data exposed, individuals are advised to adopt the following cyber hygiene measures:

- Change your passwords regularly.
- Avoid using personal information in passwords. Use a strong password or passphrase of at least 12 characters which includes upper case, lower case, numbers and/or special characters. To make it easier for you to remember, you can use passphrases by putting together a sentence or combination of words based on a memory unique to you. As passphrases are longer than traditional passwords and tend to be unique, they are more secure than short passwords as it often requires significantly more time for cyber criminals to crack. Avoid using the same password for different accounts.
- Enable two-factor authentication (2FA), where available.
- Ensure that an antivirus software is installed on your device and update it regularly.
- Perform antivirus scans regularly to remove any known malware on your device.
- Enable password protection on data storage devices and lock them up when not in use.
- Limit access to social media accounts. Also, limit sharing of personal information online as threat actors commonly look for and use such personal information to carry out targeted phishing. Review your account privacy settings and permissions and adjust your privacy settings as appropriate.
- Turn on login alerts, if available. The platform should send you an alert when someone logs into your account from an unrecognised device or browser. For email accounts, review any unrecognised login sessions immediately for unusual account activities such as setting of email forwarding rules to unknown accounts.
- Always be wary of suspicious emails and verify before clicking on any links or downloading any attachments, especially if the email came from an unfamiliar sender.
- Verify a link in an email/SMS by checking the domain name of the site, as it is an indicator of whether the site is legitimate. Users can hover their mouse over the link to ensure that they are being directed to the URL stated.

When Performing Online Transactions

- Avoid using public Wi-Fi when accessing bank accounts and logging in to websites that require sensitive personal information such as banking details and login details, as others may spy on the public network and intercept such transactions.
- Consider designating a single credit card for all online purchases and closely monitor transaction alerts via SMS or email. Individuals may also customise a daily transaction limit to prevent large transactions from occurring if your accounts were to be compromised.

- Ensure that the website supports secure payment service. You can verify that the website is legitimate and trustworthy by checking the Secure Sockets Layer (SSL) certificate through the lock icon on your browser's URL bar. This SSL certificate also enables encryption on the website through Hypertext Transfer Protocol Secure (HTTPS). Users should avoid websites that do not support HTTPS.

Individuals may also check if their email account details have been leaked in past data breaches by visiting the 'Have I Been Pwned' (HIBP) webpage. Email addresses flagged by HIBP webpage are those that were exposed during a prior online platform data breach, where the email addresses were used as a login credential. Although it may not mean that the email account has been compromised, individuals should consider changing to a strong password and enabling 2FA on the account.

Securing your Identity after a Data Breach

- Confirm that the breach has happened by visiting the organisation's website or searching the web. If the breach is real, there should be news alerts online and a data breach notification displayed on the website or your account page.
- Understand what sensitive data was stolen. This will help you understand the types of identity theft you are at risk of and how you can mitigate the potential damage.
- Change your passwords immediately. Use a strong password or passphrase of at least 12 characters which includes upper case, lower case, numbers and/or special characters.
- Avoid using the same password for different accounts.
- Enable two-factor authentication (2FA), where available.
- Check for updates from the company of which the data was leaked from. The company will likely post ongoing updates and disclosures concerning affected customers and steps that people could take to protect themselves.
- Monitor your accounts for unusual activities and suspicious transactions.
- Consider identity theft protection services if necessary.

References:

https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/tech-omnibus/how-to-guard-against-common-types-of-data-breaches-handbook.ashx
https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-on-Managing-and-Notifying-Data-Breaches-under-the-PDPA-15-Mar-2021.ashx?la=en