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 making unauthorised transactions.

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

This advisory provides guidance to individuals on the following

- Common Causes of Data Breach
- Cybersecurity Measures for Individuals to Manage Devices and Online Presence
- Securing your Identity after a Data Breach

Common Causes of Data Breach

Weak/Stolen Passwords

Weak password management facilitates threat actors' access into a system. This includes the use of weak passwords 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 or ransomware.

Social Engineering

Social engineering is the use of psychological manipulation to get victims to perform certain actions or reveal sensitive credentials. Phishing, the most common type of social engineering, is a technique used to obtain sensitive information such as login credentials or credit card details. Phishing can be conducted via email, messaging platforms such as WhatsApp and SMS or social media, with the message being disguised as being sent from a legitimate entity. The motive is to trick victims into clicking on a phishing link which could either lead to a phishing page requesting for the victims' confidential details or cause the victim's computer to be infected with malware.

Insider Threats

Insider threats may originate from deliberate actions by disgruntled/rogue employees of an organisation who knowingly leak data to competitors or sell them for financial gain. It may also arise from 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

We urge users to adopt the following measures:

- Avoid using personal information in passwords. Use a strong password or passphrase of at least 12 characters which includes uppercase, lowercase, 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 as it often requires significantly more time for cybercriminals to crack than short passwords.
- Limit sharing of personal information on social media accounts 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.
- Avoid using the same password for different accounts.
- 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.
- 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.
- Always be wary of suspicious emails and messages and verify before clicking on any links or downloading any attachments, especially if the email came from an unfamiliar sender.
- Verify the link 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.

<u>When Performing Online Transactions</u>

- 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 it.
- 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 account were to be compromised.
- Ensure that the website supports secure payment service. You can verify that the website is secure by checking the Transport Layer Security (TLS) certificate through the lock icon on your browser's URL bar. This TLS certificate also enables encryption on the website through Hypertext Transfer Protocol Secure (HTTPS). Users should only assess websites with a URL that starts with HTTPS.

Users can check if your email account details have been leaked in past data breaches by visiting the 'Have I Been Pwned'(HIBP) website. Email addresses flagged by the HIBP website are those that were exposed during a prior online platform data breach, where the email address was used as a login credential. Although it may not mean that your email account has been compromised, you should change your password to a strong one and enable 2FA on the account.

Securing your Identity after a Data Breach

- Confirm the breach 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 on the website or your account page.
- Understand what sensitive data was stolen. This will help you understand what 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 uppercase, lowercase, numbers and/or special characters.
- Avoid using the same password for different accounts.
- Enable 2FA where available.
- Check for updates from the organisation from which the data was leaked. The organisation will likely post ongoing updates and disclose who were affected and steps to protect your account.
- 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