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 personal data 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 protect one's data. 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 Breaches
- Cybersecurity Measures for Individuals to Manage Devices and Online Presence
- Securing your Identity after a Data Breach

Common Causes of Data Breaches

<u>Weak/Stolen Passwords</u>

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 offer a layer of security to your personal information and should be safeguarded in both the physical and cyber realms. Reusing passwords across multiple accounts may also increase the risk of account compromise, particularly when login credentials have been exposed in previous data breaches.

<u>Unpatched Vulnerabilities</u>

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 trick victims into performing 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 and messaging platforms such as WhatsApp, 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.

Threat actors may also use fraudulent websites or messages containing urgent or threatening language to trick victims into disclosing sensitive information or downloading malicious applications. Personal information obtained from previous data breaches may also be used to make phishing and impersonation attempts appear more convincing. Threat actors may also use AI-generated deepfakes, which refer to digitally manipulated multimedia content , to impersonate trusted individuals or organisations and deceive victims into revealing sensitive information.

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.

Cloud Misconfiguration and Inadequate Access Controls

Improperly configured cloud storage services, databases, accounts or applications may inadvertently expose personal information to unauthorised parties. Weak access controls, excessive user privileges and compromised access credentials may also allow threat actors to access or download sensitive information.

Cybersecurity Measures for Individuals to Manage Devices and Online Presence

We urge users to adopt the following measures:

- Avoid using personal information such as NRIC in passwords. Use a strong password or passphrase of at least 12 characters which includes a mixture of uppercase, lowercase, numbers and/or special characters. To make it easier for you to remember your password, you can put together a sentence or combination of words based on a memory unique to you. This is known as a passphrase. 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 campaigns.
- Review your account privacy settings and permissions and adjust your privacy settings as appropriate.
- Review application permissions regularly and restrict unnecessary access to personal information.
- Avoid using the same password for different accounts. Consider using a reputable password manager to generate and securely store unique passwords.
- 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 Multi-Factor Authentication (MFA), particularly for important accounts, such as email, banking and other services containing sensitive personal information. Where available, consider using passkeys, as they provide stronger protection against phishing attacks by reducing the risk of credential theft.
- Ensure that an antivirus software is installed on your device, update it regularly and perform regular antivirus scans to remove any known malware on your device.
- Keep your devices, operating systems and applications updated with the latest security patches to protect them against known vulnerabilities.
- 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. Exercise caution when scanning QR codes from unknown or unverified sources.
- 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 a legitimate URL

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 it. Where possible, use a trusted network or mobile data connection when performing financial 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, protecting your account in the event of a compromise.
- Ensure that the website supports secure payment service. You can verify that the website uses an encrypted connection by checking for Hypertext Transfer Protocol Secure (HTTPS) in the browser's address bar.
- Always verify the website address and the authenticity of the service before providing personal or financial information.

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 are urged to change your password and enable MFA on the account. Users should also review the information exposed and change any passwords that were reused across other accounts.

Securing your Identity after a Data Breach

- Confirm the breach happened by visiting the organisation's official website or contacting the organisation through its official channels. Avoid clicking on links in unexpected data breach notification messages, as threat actors may impersonate affected organisations to conduct phishing attacks.
- Understand what sensitive data was stolen. This will help you understand the types of identity theft you may be at risk of and how you can mitigate potential damages.
- 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. If the compromised password was reused for other accounts, change those passwords as well. Enable MFA where available.
- Review your account activities and security settings for unfamiliar login sessions, unauthorised changes or suspicious activities. Log out of unrecognised sessions and contact the relevant service provider if you suspect that your account has been compromised.
- Check for updates from the organisation from which the data was leaked. The organisation will likely post ongoing updates and inform those who were affected by the breach along with steps to protect your account.
- Monitor your accounts for unusual activities and suspicious transactions. Notify your financial institution immediately if unauthorised transactions are detected.
- Report suspected misuse of personal information. If you suspect that your personal information has been used for fraudulent activities, contact the

relevant organisation or financial institution immediately. For suspected scams, contact the ScamShield Helpline at 1799. Lodge a police report if you have fallen victim to a scam or other criminal activity.

- Consider engaging identity theft protection services if necessary.

References

1. Personal Data Protection Commission (PDPC) – Guide on Managing and Notifying Data Breaches under the PDPA: 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.pdf
2. Personal Data Protection Commission (PDPC) – Good Practices to Secure Personal Data in the Cloud Platform: https://www.pdpc.gov.sg/assets/37d76636-a8ad-4903-af1d-d4503bda7d0d
3. Have I Been Pwned (HIBP) – Check for Data Breaches: https://haveibeenpwned.com/
4. ScamShield – Official Scam Prevention Resources: https://www.scamshield.gov.sg/resources/