

Best Practices To Improve Data Security



With digitalisation dominating the business landscape, threat actors are quickly adapting to take advantage of it through methods such as phishing emails, malware and ransomware.

Singapore has strong privacy legislation - the Personal Data Protection Act (2012), and specific to the financial industry, notices to [Cyber Hygiene](#) and [Technology Risk Management Guidelines](#).

At Chubb, we strive to uphold strict privacy and security guidelines within the organisation, so as to protect our most vital assets – our people, as well as our property, reputation and brand. This will enable us to ensure security and business continuity, and we expect the same of our intermediaries.

We have prepared some best practices on managing data security which might be useful for you to incorporate into your workflow and processes.

How Can You Improve Data Security?



1. Patch Operating Systems

Ensure up-to-date operating systems on servers and local devices, by **installing patches regularly** – This can help maintain the integrity of the operating systems.



2. Encryption Practices

When sending emails

- **Do not document** sensitive and/or personal data in the email body
- **Fully encrypt or password protect** attachments that contains sensitive and/or personal data
- Send all **passwords separately**
- **Turn off auto-fill feature** when inserting email addresses; always double-check recipient list before sending out the email

When using devices

- **Change password regularly** on your devices
 - Remember to **lock your devices** whenever you must step away (even for a moment)
 - **Do not record/write down passwords** and place them with your devices
-



3. Awareness of Common Malicious Activities

Phishing

- Always check for **spelling or grammatical errors, deviation in email addresses** from the usual sender and for any **unverified sources requesting for your urgent response**.

Malware/Ransomware

- **Do not click into links** in emails that look suspicious or from unverified sources.
- **Do not provide information or details** in data fields through such links.
- **Do not download files** from unverified sources or links.



4. Incidents Notification

Report any incident immediately to Chubb's Data Protection Officer at DPO.SG@Chubb.com

Additional Resources

For more insights/resources on the importance of upholding data security best practices, please visit Chubb's Cyber Insights webpage at <https://www.chubb.com/sg-en/articles/cyber-insights.html>

For more information about the above data security best practices, kindly reach out to your IDP Manager or contact us at DPO.SG@chubb.com.

Regards,

Chubb Risk & Compliance