UOBKayHian

UOB Kay Hian Cyber Security Advisory

Recently, there has been a new cybercrime group, LAPSUS$, that specializes in stealing data from companies and extorting money from these companies by threatening to publish the stolen information. The group is currently operating via Telegram and email.

LAPSUS$ may pretend to be a trusted person such as government officials, bank officials or IT Support staff to trick you into providing your usernames and passwords voluntarily.

They may also trick you into changing your account's mobile phone number to their own phone numbers. They would be able to intercept any one-time password (OTP) used for multi-factor authentication (MFA) and can even reset password of online accounts that allows password reset via link sent via SMS.

To protect yourself from being a victim, you should:

Protection against Impersonation:

- Always check that you are speaking with the correct person. If you are unsure of the person's identity, hang up and call the numbers listed on the company's official website again
- **NEVER** give out your username and passwords to anyone. Legitimate companies will never ask you for your passwords.

Account Protection:

- Enable 2-factor authentication on your accounts when possible and **NEVER** give out the OTP to anyone
- When receiving a suspicious SMS, never click on any links or attachments provided.
- Be cautious when receiving password reset links via SMS. If you did not request for the password reset, you should delete the message and change your password immediately

Password Protection:

- Ensure that your password does not use any common words and numbers (E.g. password1, Passw0rd, P@ssw0rd etc)
- Ensure that your password contains a combination of alphanumeric characters and special symbols
- Change your account passwords periodically
- Ensure that you do not reuse the same passwords for multiple accounts

Updated on 25 March 2022