CANADIAN CENTRE FOR CYBER SECURITY

INSTANT MESSAGING

Social media and instant messaging (IM) applications are integrated into our daily lives, both in the personal and business contexts, as a convenient form of communication. Although these applications help you communicate quickly and easily, be aware that you are vulnerable to different security threats when using them. Additionally, different application developers have different security standards.

IS INSTANT MESSAGING SECURE?

IM applications are used in the workplace as quick and easy ways to communicate with coworkers, whether working in the office or remotely. However, IM applications are not entirely safe or private. Threat actors can gain access to the information you are transmitting; always be cautious of the sensitivity level of the data that you are sending through these applications.

Some IM applications are linked to your social media accounts. If you use your social media account credentials to log in to an IM application, you are connecting the applications. Many social media and IM applications are owned by the same company, which allows the company to collect and share your data between your associated accounts. Threat actors who successfully hack into one of your accounts can also access your data that is associated with other connected applications.

IS END-TO-END ENCRYPTION SECURE?

End-to-end encryption is a confidentiality service that encrypts the sender's data (e.g. converts information to hide its contents and prevent unauthorized access) and only allows the receiver to decrypt it. Many IM applications use end-to-end encryption to secure your information and messages. Although this seems like a high level of security when sending and receiving information, you should not rely entirely on end-to-end encryption to protect your data. Threat actors can compromise your devices to retrieve the encrypted data either in the hopes of decrypting at a later time, or by compromising your unencrypted data. It is important to take these points into consideration before sending a message with a higher level of sensitivity.

WHAT ARE THE RISKS INVOLVED IN USING IM?

There are many risks that should be considered when using IM as a form of communication. Threat actors can obtain your information through some of the following methods:

- Gaining access to your log-in credentials (e.g. unprotected passwords).
- Obtaining credentials for other accounts that are connected to the IM application.
- Exposing sensitive information that you have sent to them by sharing it with others (e.g. through a screenshot).
- Collecting personal information from shared accounts (e.g. exposing your personal information online [birthdate, address] can lead to potential password hacks).
- Stealing information through an infected device (e.g. open applications being exposed to spyware).
  - Encrypted messages are unreadable until attackers gain the credentials to decrypt them.

Even if you are using a legitimate and safe IM application, threat actors can take advantage of unknown loopholes and vulnerabilities in the applications. These vulnerabilities put your sensitive information at risk of being placed in the wrong hands.

AWARENESS SERIES

Canada

WHAT SHOULD I BE LOOKING FOR IN AN APPLICATION?

There are a few things you need to look out for when choosing an application to use for either personal or business use. Your organization's supply chain (i.e. the link between your organization and other organizations that helps you serve your customers) should be considered. For more details on supply chain integrity, refer to *ITSAP.00.070 Supply Chain Security for Small and Medium-sized Organizations,* which is available on the CCCS website.

We recommend that you consider the following questions when choosing an application:

- Where does the messaging application store or process your data?
  - Use applications from vendors who store your data in Canada to ensure your information is protected under Canada's privacy laws.

- How does the architecture of the application support the security measures that the vendor implements?
  - Know the features offered by the vendor (e.g. message lifespan, contact lists, communication logs).
  - Know how long your information is stored and how it is destroyed.

- Does the vendor have security policies in place?
  - Go with a vendor who uses strong authentication mechanisms (e.g. two-factor authentication).
  - Have plans and procedures in place in case your account is compromised.

- What protocols does the vendor use to encrypt messages?
  - End-to-end encryption does not guarantee that your information is secure.
  - Ensure the vendor uses supported encryption methods to protect your data (e.g. messages in transit and at rest need to be accounted for).

- Are there any connected applications or third-parties involved?
  - Identify which applications are connected and linked to your information.
  - Know which applications and companies are involved to ensure you can rely on the vendor's services.
  - Ensure the vendor provides the services that they claim to provide and nothing more (e.g. sharing your data).

HOW CAN I USE SECURE MESSAGING SAFELY?

Although many IM applications claim to be fully secure through end-to-end encryption, there are still ways attackers can obtain the information sent and received through the application. To ensure your information is kept as secure as possible, we recommend that you follow some guidelines:

- Keep your IM applications and device's operating system up to date (e.g. latest versions will include security patches).

- Use a different password for each IM application.
  - For more details on passwords, refer to *ITSAP.30.032 Best Practices for Passphrases and Passwords,* which is available on the CCCS website.

- Use two-factor authentication for your accounts (if available on the application).

- Limit the use of personal identification details (e.g. name, phone number) in your account profiles.

- Do not use "remember me" features and log out when you are no longer using the application.

- Do not share sensitive information (e.g. banking information, social security numbers).

- Ensure the vendor or application is legitimate (e.g. fake messaging applications can infect your devices with malware).

- Use messaging applications over secure networks (e.g. do not use public Wi-Fi).

- Limit connecting your IM accounts to your other devices (e.g. cloud, Internet of Things).

- Ensure you trust the recipient you are communicating with (e.g. receivers can screenshot messages to share).
  - Ensure blocked connections are disconnected on all applications (e.g. attached applications may not block communication through all accounts).
  - Validate the identity of the person you are communicating with (e.g. verification through a specific question or an encrypted key).

- Check reviews on the long-term use of specific vendors and applications when you are verifying their dependability and trustworthiness.