Communications Security Establishment | Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

Instant messaging

February 2024 ITSAP.00.266

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.

How do threat actors leverage instant messaging applications?

There are many risks that should be considered when using IM as a form of communication. For example, your information may not be secure within IM and could be compromised, stolen, or exposed by threat actors.

Threat actors can obtain your information through some of the following methods:

- Gaining access to your environment and encrypted messages through compromised log in credentials
- Conducting social engineering attacks and password guessing via personal information gathered from your employees' social media accounts and other platforms in which information is shared
- Infecting a device with malware or spyware to compromise and steal information

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.

Is end-to-end encryption secure?

End-to-end encryption is a confidentiality service that encrypts the sender's data and converts the information to hide its contents. It prevents 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. In some IM applications, end-to-end encryption only applies to messages in transit and does not apply to messages at rest, such as messages that have been stored or backed up. It is important to consider these points before sending a message with a higher level of sensitivity.

AWARENESS SERIES

Cat. No. D97-1/00-266-2024E-PDF
ISBN 978-0-660-68304-1

What should I be looking for in an application?

When considering an IM application you should ensure the vendor has a robust security framework in place. Your organization's supply chain is only as strong as the weakest link. Your supply chain is the link between your organization and other organizations that helps you serve your customers. For more details on supply chain integrity, refer to *Supply Chain Security for Small and Medium-sized Organizations (ITSAP.00.070)*.

To ensure the integrity of your supply chain, 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, such as message lifespan, contact lists, and 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 like multi-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 (for example, 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 (like 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 these guidelines:

- Keep your IM applications and device's operating system up to date (the latest versions will include security patches)
- Use a different password for each IM application
- Use multi-factor authentication for your accounts, when available
- Limit the use of personal identification details (like name, phone number) in your account profiles
- Do not use "remember me" features and log out when you are no longer using the application.
- Consider using a password manager
- Do not share sensitive information (such as banking information, social security numbers)
- Ensure the vendor or application is legitimate (fake messaging applications can infect your devices with malware)
- Use messaging applications over secure networks (for example, do not use public Wi-Fi)
- Limit connecting your IM accounts to your other devices (like cloud and Internet of things)
- Ensure you trust the recipient you are communicating with as receivers can screenshot messages to share them
  - Ensure blocked connections are disconnected on all applications (attached applications may not block communication through all accounts)
  - Validate the identity of the person you are communicating with (such as verification through a specific question or an encrypted key)
  - Scan attachments with anti-malware software before opening
- Check reviews on the long-term use of specific vendors and applications when you are verifying their dependability and trustworthiness

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at the Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**