USING ENCRYPTION TO KEEP YOUR SENSITIVE DATA SECURE

MAY 2021 **ITSAP.40.016**

Encryption technologies are used to secure many applications and websites that you use daily. For example, online banking or shopping, email applications, and secure instant messaging use encryption. Encryption technologies secure information while it is in transit (e.g. connecting to a website) and while it is at rest (e.g. stored in encrypted databases). Many up-to-date operating systems, mobile devices, and cloud services offer built-in encryption, but what is encryption? How is it used? And what should you and your organization consider when using it?

WHAT IS ENCRYPTION?

Encryption encodes (or scrambles) information. Encryption protects the confidentiality of information by preventing unauthorized individuals from accessing it.

For example, Alice wants to send Bob a message, and she wants to ensure only he can read it. To keep the information confidential and private, she encrypts the message using a secret key. Once encrypted, this message can only be read by someone who has the secret key to decode it. In this case, Bob has the secret key.

Eve is intentionally trying to intercept the message and read it. However, the message is encrypted, and even if Eve gets a copy of it, she can't read it without acquiring the secret key.

If an individual accidentally receives a message that includes encrypted information, they will be unable to read the encrypted contents without the key to decrypt the message.

HOW IS ENCRYPTION USED?

Encryption is an important part of cyber security. It is used in a variety of ways to keep data confidential and private, such as in HTTPS websites, secure messaging applications, email services, and virtual private networks. Encryption is used to protect information while it is actively moving from one location to another (i.e. in transit) from sender to receiver. For example, when you connect to your bank's website using a laptop or a smartphone, the data that is transmitted between your device and the bank's website is encrypted. Encryption is also used to protect information while it is at rest. For example, when information is stored in an encrypted database, it is stored in an unreadable format. Even if someone gains access to that database, there's an additional layer of security for the stored information. Encryption is also used to protect personal information that you share with organizations. For example, when you share your personal information (e.g. birthdate, banking or credit card information) with an online retailer, you should make sure they are protecting your information with encryption by using secure browsing.

Many cloud service providers offer encryption to protect your data while you are using cloud-based services. These services offer the ability to keep data encrypted when uploading or downloading files, as well as storing the encrypted data to keep it protected while at rest.

When properly implemented, encryption is a mechanism that you and your organization can use to keep data private. Encryption is seamlessly integrated into many applications to provide a secure user experience.

AWARENESS SERIES

Cat. No. D97-1/40-016-2021E-PDF
ISBN 978-0-660-38618-8

HOW CAN I USE ENCRYPTION?

Your organization likely already uses encryption for many applications, such as secure browsing and encrypted messaging applications.

SECURE BROWSING

If you access a website with padlock icon and HTTPS in front of the web address, the communication (i.e. the data exchanged between your device and the website's servers) with the website is encrypted.

To protect your organization's information and systems, we recommend that you use HTTPS wherever possible. To ensure that users are accessing only HTTPS-supported websites, your organization should implement the web security policy tool HTTP Strict Transport Security (HSTS). HSTS offers additional security by forcing users' browsers to load HTTPS supported websites and ignore unsecured websites (e.g. HTTP).

ENCRYPTED MESSAGING APPLICATIONS

Most instant messaging applications offer a level of encryption to protect the confidentiality of your information. In some cases, messages are encrypted between your device and the cloud storage used by the messaging service provider. In other cases, the messages are encrypted from your device to the recipient's device (i.e. end-to-end encryption). When using end-to-end encryption services, not even the messaging service provider can read your encrypted messages.

In deciding which tools to use, you need to consider both the functionality of the service and the security and privacy requirements of your information and activities. For further information, refer to *protect how you connect*.

Encryption is just one of many security controls necessary to protect the confidentiality of data.

WHAT ELSE SHOULD I CONSIDER?

Encryption is integrated into many products that are commonly used by individuals and organizations to run daily operations. When choosing a product that uses encryption, we recommend that you choose a product that is certified through the Common Criteria (CC) and the Cryptographic Module Validation Program (CMVP). The CC and the CMVP list cryptographic modules that conform to Federal Information Processing Standards. Although the CC and the CMVP are used to vet products for federal government use, we recommend that everyone uses these certified products.

THE CCCS RECOMMENDS

When choosing a suitable encryption product for your organization, consider the following:

- Evaluate the sensitivity of your information (e.g. personal and proprietary data) to determine where it may be at risk and implement encryption accordingly.
- Choose a vendor that uses standardized encryption algorithms (e.g. CC and CMVP supported modules).
- Review your IT lifecycle management plan and budget to include software and hardware updates for your encryption products.
- Update and patch your systems frequently.

Prepare and plan for the quantum threat to cyber security. For more information please see *ITSE.00.017 Addressing the Quantum Computing Threat to Cryptography*.

ENCRYPTION FOR HIGHLY SENSITIVE DATA

Systems that contain highly sensitive information (e.g. financial, medical, and government institutions) require additional security considerations. Contact us for further guidance on cryptographic solutions for high-sensitivity systems and information: **contact@cyber.gc.ca**

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