BIZCOMMUNITY

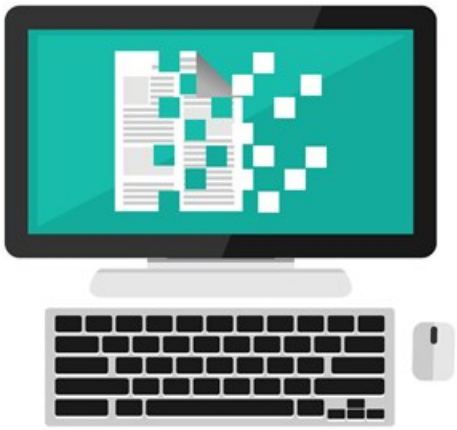
What is encryption, how does it work and why is it important?

By Carey van Vlaanderen

6 Mar 2017

More than any other security topic, encryption seems to perplex a lot of people.

Many may have seen it within their WhatsApp and view encryption as being infinitely complicated, and while it is certainly no small feat to create truly secure encryption algorithms, there are a lot of simple types of encryption that you might have implemented yourself without knowing it.



The history of encryption

As of late, encryption has become highly topical making the front pages of newspapers and websites all over the world, however, it is not a new concept. In fact, data encryption has been around for some time. Longer than a year, ten years, more than a hundred – even more than a thousand years.

Encryption was used by Julius Caesar during his reign of the Roman Empire, where he would change the first three letters of the alphabet to the last three thereby encrypting the messages he sent to his generals. Similarly, the Germans invented the Enigma machine to send encrypted messages during World War II, which meant the allies could not, at first, read the intercepted content.

Interestingly, the first prototype of the computer emerged from an investigation into figuring out how to decipher Enigma.

What are the benefits of encryption?

Encryption keeps sensitive and personal information secure and private. This includes all online data such as bank details, emails, and social networks – as well as offline data, such as information stored on hard-drives that only you can access.

With this security technique, you will not only prevent identity theft but in the case of losing a device such as a smartphone, tablet or computer, you can be confident that cyber criminals will still not be able to access your data.

What does it mean to encrypt a message and how does it work?

Although there are many encryption systems, the most common ones are the use of public and private keys.

In this system, all internet users have two keys – a public one that everyone can see and use and a private one that only a specific individual can use.

An alteration made by a mathematical algorithm transforms readable data (a message) into non-readable data. This means that when it is sent to a recipient, it is encrypted and in order to read it, a key is needed to decrypt it.

All the major operating systems and many popular software applications give you the option of encrypting files or folders on your device. When you use this option, you must choose a password that allows you (and anyone else you share the password with) to unlock and decrypt those files. As such, if a cybercriminal succeeds in intercepting one of the messages, he or she will not be able to read it without your private key, and your information remains secure.

Document in use

Encryption is great for when data is in storage or in transit, but there is one other situation that bears discussion; when your encrypted document is in use (when you have opened a protected document and are viewing or editing it). This includes any time the encrypted file is open, even if it is minimised or visually covered up in some way.

Unlocking the file means that it has been decrypted in your device's memory. If for example, someone has opened a backdoor into your machine with malware, they can access that data if it is unlocked.

This does not mean encryption is ineffective, in fact, liberally using encryption can really limit the amount of damage someone can do and it can also shrink the window of time in which an attacker has access to your decrypted data.

Therefore, layers of defences are a good thing: one technology can help bolster the effectiveness of another as each shrinks the opportunity for an attacker to steal data.

ABOUT CAREY VAN VLAANDEREN

Carey van Vlaanderen is CEO of ESET Southern Africa. ESET is a global provider of security software for enterprises and consumers and is dedicated to delivering instant, comprehensive protection against evolving computer security threats.

- 4 ways to manage the human threat to cybersecurity - 18 Jul 2023
- A cybercriminal's tricks and trades to get into your phone - 23 Mar 2018
- What is encryption, how does it work and why is it important? - 6 Mar 2017
- Five common security threats that demand attention - 9 Mar 2016
- Face 2016 with a proactive attitude of security awareness - 22 Jan 2016

View my profile and articles...