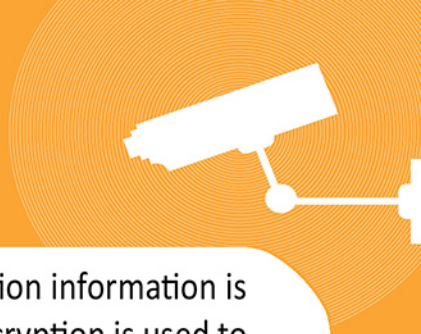
Encryption

Privacy Factsheet



ENCRYPTION makes our online activity more secure. Without encryption information is unsecure and vulnerable to theft, hacking, exploitation and abuse. Encryption is used to protect both internet communications and devices. More and more companies are using encryption to protect customer's communications. Although encryption can seem complicated there are many easy ways to encrypt your data and devices.

What is encryption?

Encryption is the process of scrambling data into an unreadable code which can only be unscrambled when it is delivered. Sometimes this is done using a special key.

Encryption is used to protect your digital data from prying eyes, middle man attacks, theft and vulnerability.

Encryption can be used to protect the content of messages when it travels from one person to another.

The content of a communication can be encrypted. The communications data; the who, where, when and how cannot be encrypted. This is so the content can be delivered correctly.

Different types of encryption

Not all websites are encrypted. It is important that you check the encryption being used by the service provider before using email, downloading an app, using the cloud, shopping online or buying a new device.

Hyper Text Transfer Protocol Secure (https): Also known as an SSL (Secure Sockets Layer) Connection. If you see https in the address of the website you are visiting it indicates that the site encrypts all data between your computer and the website's server. This protects the data from being read by a third party. Always look for https when you browse the internet to help keep your data and devices safe, this is particularly important when using public Wi-Fi. Https is also a guarantee that the website you are visiting is real and not a fake website.

PGP (Pretty Good Privacy): PGP is a form of encryption which requires you and the person you are communicating with to hold decryption keys. PGP has to be downloaded and installed on your device and the device of the person you are communicating with.

Lock symbol: If you see a lock symbol in your internet search bar click on it to get information about the security of the website you are visiting. It will tell you if the website you are visiting is encrypted.

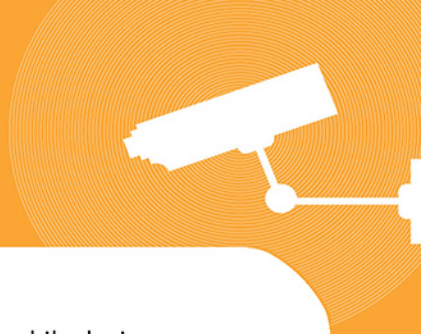
End to end encryption: Means your data is encrypted whilst it is travelling between devices. As soon as the data leaves your device it is encrypted and only unencrypted when it is delivered to the recipient's device. No-one can other than you and the recipient can see or read the messages.

Virtual Private Networks (VPN)

- A VPN creates a link between your device and other locations so internet traffic can travel securely.
- It uses encryption to protect and hide data as it travels around the internet.
- If you use public Wi-Fi a VPN is recommended to protect your device from hackers or identity thieves.
- A VPN doesn't guarantee absolute security of your communications so use it alongside https and other encryption.

Encryption

Privacy Factsheet



How to encrypt your devices

Mobile Devices (phones and tablets): Apple and Android allow you to encrypt your mobile devices. To do this you have to create a pin or passcode which will lock the device and allow only you to access its content. If you do not create a pin or passcode your device is not encrypted.

Apple Mac: To encrypt the hard disk on your Mac you can use the in-built software called FileVault.

Microsoft: Older versions of Windows use BitLocker or DiskCryptor to encrypt your device. For Windows 10 you must use the "device encryption" tool, which encrypts your drive through your Microsoft account and password. This method of encryption gives the encryption key to Microsoft, not to you.

* *

Is data encrypted in the cloud?

Some cloud services offer encryption, others don't. If your cloud provider offers encryption the quality of encryption can vary dramatically. It is important you check what level of encryption your provider offers, for example:

- Some encrypt stored data only.
- Some encrypt stored data and the data when it is travelling between devices.
- Some encrypt your data but hold the encryption key, which means they can access your files if they want to or if asked to by law enforcement.
- Some allow you to encrypt your data and provide you with the encryption key so only you can access your data. This is called client-side encryption.

* *

Are all online communications encrypted?

Although encryption is getting easier to use not all methods of communicating online are encrypted.

Messenger apps: Apps such as WhatsApp, Signal, Wickr and Telegram all provide end to end encryption.

Remember if you use an encrypted app your messages are only encrypted on your device if you have created a passcode or password. If you choose for the app to back messages up the messages the encryption is not always guaranteed.

Email: The most popular free email providers (Outlook, Gmail, Yahoo, AOL, mail.com, etc.) do not offer encryption as standard. Encrypted email providers require you and the people you are communicating with to hold encryption keys to unscramble the messages. These email providers use PGP as their encryption tool.

If you want to protect your email communications you can find encrypted email service providers online.

* *

Don't forget

- Only content can be encrypted, communications data; the who, where and what of a communication cannot.
- Look for https or the lock symbol in your internet search bar to ensure the website you are visiting uses encryption.
- Encrypt your mobile devices using a passcode.
- Data held in the cloud is not guaranteed to be encrypted.
- Without encryption your data is insecure and vulnerable to hacking, theft or misuse.