How Encryption Can Help Protect Your Data from Theft and Interception

0

Kevin Wells • September 6, 2016 • Feature Articles

More and more people are becoming aware of the risks to their data from theft, interception or compromise from third-parties.

Our data can be stolen from our devices as well as intercepted online by intelligence agencies such as NSA and the UK's GCHQ – as well as by hostile nations and terrorists.

As a result, many people are now interested in encrypting their data to keep it safe from these threats.

Is Data Encryption Secure?

It depends. There are different levels of encryption and some are easier for intruders to crack than others.

Advances in computer processing capacity now make it possible for ordinary members of the public to have access to high levels of encryption which a decade or two ago were unavailable.

Modern cryptographic techniques, as **Chris Soghoian of the ACLU** put it, "raise the cost of surveillance and make dragnet surveillance impossible."

So provided you use a robust encryption standard, your data should be pretty secure from most cracking attempts.

To quote Edward Snowden: "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."

Latest articles

How Encryption Can Help Protect Your Data from Theft and Interception
Feature Articles • no comments

Hacking Fears Could Keep 16 Million Americans from Voting
Feature Articles • no comments

Stop the Bleeding: How to Respond to a Cyberattack
Feature Articles • no comments

How Your Smartphone Can Keep You Safer
Feature Articles • no comments

How to Use a VPN to Watch the 2016 Summer Olympics
Guides • no comments

Recommended topics

- Internet Security
- Protect Your Information
- Phone and Tablet Security
- Protecting Your Children

How Should You Encrypt Your Data?

To be safe from interception, your data should be encrypted not only while stored on your devices (known as "**data at rest**"), but also when being sent across the Internet ("**data in motion**").

Any data you store with an online service should also be encrypted when "at rest" in the cloud.

The simplest form of encryption uses a single encryption key. When sending data to another person, you need to provide a copy of the key to the receiver. This is known as **symmetric encryption** and it's the easiest to implement – though it's not the safest.

A more secure form of protection is **asymmetric encryption**. This uses two keys: a public key, used to encrypt your data, and a separate private key, which you provide to the recipient so they can unlock the encrypted data.

The algorithm used to encrypt your data also needs to be robust. Opinions vary on what constitutes robust encryption and the level of encryption regarded as necessary is continually rising as computer processing power increases.

The current minimum recommended standard of encryption is at least 128-bit, ideally 256-bit and has asymmetric keys.

Some current examples of robust encryption algorithms are **RSA** which also uses asymmetric encryption and **Twofish** which uses only one (symmetric) key but with up to 256-bit encryption.

The US Government uses the **Advanced Encryption Standard (AES)** with at least 128-bit encryption. This is generally considered resilient to most cracking attempts.

How to Encrypt Your Data on Your Devices

There are a number of software tools available which will encrypt your hard drive or parts of your hard drive.

Popular examples are the open source **Veracrypt** and **Microsoft Bitlocker**. These tools basically provide encryption at the file system level.

Veracrypt can encrypt individual drive partitions or create an encrypted file container (known as a volume) which you then mount into your OS file system and can access just like a conventional hard drive partition. Veracrypt can encrypt both hard drives as well as USB thumb drives.

Veracrypt is available free for Windows, Linux and Mac OSX.

Veracrypt offers a great deal of functionality. For additional security you can also create a hidden volume within another volume with a separate password. The hidden volume cannot be easily identified by third-parties. This is known as "plausible deniability."

You can even boot a hidden operating system from within a Veracrypt volume or even, by installing a system such as Oracle Virtualbox, an entire virtualized computer.

Veracrypt is the successor to Truecrypt, for which maintenance and support ceased in 2015 when the developers closed the project. This means any subsequent security holes found in Truecrypt will not be fixed.

Veracrypt removed many vulnerabilities present in TrueCrypt, making it more robust against brute-force attacks.

Due to speculation about the circumstances under which maintenance of Truecrypt suddenly ceased in 2015, the **OSTIF** has commissioned a **code audit of VeraCrypt** scheduled to be completed in late 2016.

Bitlocker is Microsoft's proprietary disk encryption tool, supplied with Windows Vista, Windows 7, 8 and later (Enterprise/Ultimate/Pro) versions.

To use Bitlocker, your computer hardware also needs to possess a so-called TPM or Trusted Platform Module chip.

It's still possible to use Bitlocker without a TPM by modifying the Windows Group Policy Editor.

The main drawback with Bitlocker is that it is proprietary software. This means there's no sure way of knowing whether it contains any surveillance backdoors.

You can find out more about Bitlocker on the **Microsoft Tecnnet website**.

There are a number of other open source tools available, too numerous to list here, as well as commercial

software products such as Symantec Drive Encryption, Sophos SafeGuard and McAfee Endpoint Protection.

The next step up from file system level encryption is **full disk encryption (FDE),** which secures the entire hard disk to provide a higher level of security.

Both Veracrypt and Bitlocker also provide the option for FDE.

Make sure you remember the passwords you use to set up your encrypted drives. If you forget or lose these, then there's no way of recovering your encrypted data.

Protect Your Data While It Is in Motion

As Edward Snowdon said: "Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it."

Data drive encryption doesn't protect your data from interception and theft while in transit across the Internet. Intelligence authorities such as the NSA or UK's GCHQ are especially interested in "data in motion" as it travels across the Internet because this gives them the opportunity for easy interception.

End-to-end VPN connections can provide a solution here. The **open-source TOR system** can also be an option worth considering.

Backups Are a Security Risk – Especially in the Cloud

Data held in the cloud is at particular risk of compromise. Can you trust what your provider claims about their data integrity?

If you want to be certain, then you should transfer only your encrypted data to your online storage.

Kim Dotcom's **Mega.nz** online storage service uses a strong form of encryption whereby the encryption keys are said not to be known to the provider.

Also ensure when you back up your data to other storage devices that you do so in the encrypted format and not the unlocked, unencrypted version of your data.

It's Also Important to Encrypt Your Email

Email is at particular risk because it basically moves across the Internet in unencrypted form.

Many email clients such as Microsoft Outlook, Mozilla Thunderbird or Apple Mail now include built-in support for secure email encryption.

The **Transport Layer Security (TLS)** protocol provides for secure email encryption. However, for TLS to work, the email providers and email software of both sender and receiver have to support TLS. That being said, TLS is gradually becoming the accepted standard, as yet not every email provider uses it.

Why You Need Mobile Device Encryption

Your smartphone and your tablet hold valuable personal data. You need to protect this data – both when in transit as "data in motion" as well as data stored on your phone.

The most secure form of encryption for communications is end-to-end. This prevents even the app developers, mobile carriers or phone manufacturers from reading your messages. Apple's iMessages provides this, as does the messaging app service WhatsApp.

It's estimated while over 95 percent of iPhones are encrypted, barely 10 percent of the world's Android phones have encryption protection set by default.

All Apple devices running iOS 8 or later automatically encrypt the entire device when you create a passcode.

By contrast, Android phones do not yet automatically encrypt themselves. You should therefore make sure the settings on your Android device are explicitly configured for encryption.

What About the Risk from Backdoors?

It's no secret the FBI and NSA ideally want "backdoors" placed in devices, software and online services to give them access as and when they need it.

With proprietary products or hardware systems where the source code isn't publicly available, it can be difficult to ascertain if a backdoor is built in. This is where it's advantageous to use open-source software such as Veracrypt whenever possible.

Backdoors are a fundamentally flawed approach to security. It's like prohibiting households from installing intruder-proof locks on their doors for fear that law enforcement will not be able to enter if and when they need to.

Obviously households should be free to install the lock security necessary for their premises to be burglar-proof.

Backdoors create new problems by weakening data and device security. Backdoors can be discovered and exploited by criminals and others. If authorities have valid reasons for access, then access should be granted according to the law.

For an in-depth discussion of encryption and how it relates to government intelligence strategy, see the **Unlocking Encryption report** produced by the **ITIF Information Technology and Innovation Foundation**.

One encouraging sign is that US President Obama has publicly stated "There's no scenario in which we don't want really strong encryption."

So the President appears to be on our side regarding our rights to data confidentiality.

How do you feel about encryption? Are you concerned or intrigued about any of the information above? Please leave a comment below and share your thoughts with your fellow readers.

RELATED ARTICLES

Hacking Fears Could Keep 16 Million Americans from Voting

Stop the Bleeding: How to Respond to a Cyberattack

How Your Smartphone Can Keep You Safer

We will be happy to hear your thoughts

LEAVE A REPLY

Name E-mail Website

Post comment

Notify me of followup comments via e-mail. You can also subscribe without commenting.

Latest Articles

How Encryption Can Help Protect Your Data from Theft and Interception

Hacking Fears Could Keep 16 Million Americans from Voting

Stop the Bleeding: How to Respond to a Cyberattack

How Your Smartphone Can Keep You Safer

How to Use a VPN to Watch the 2016 Summer Olympics

Feature Guides

How To Watch Netflix Outside the USA
Best VPN Service Review Guide
Reviews

SECURETHOUGHTS
INTERNET SECURITY FOR EVERYDAY PEOPLE

Secure Thoughts is the industry leader in helping everyday people make sure their information and loved ones are protected online.

Your future and the future of those you love is too important to gamble with.

When you need the right advice, trust Secure Thoughts.