Sinclair
COPYWRITING

CYBERSHEATH
SERVICES INTERNATIONAL

WORK SAMPLE

CLIENT: CyberSheath Services International
PROJECT: Blog Posts on Cybersecurity (Encryption)

by Louise Sinclair | louise@sinclaircopywriting.com | www.sinclaircopywriting.com

HOW TO PROTECT YOUR DATA ONCE IT LEAVES YOUR HANDS

As part of your business cybersecurity practices, you go to great lengths to protect the sensitive data on your systems. But what happens when you send that data across the internet to another system?

There are two considerations here; you need to be sure that your data won't be intercepted as it traverses the internet, and you need to know that it will be protected at its final destination. You can achieve this with encryption.

Protecting sensitive data in transmission

Transport layer security (TLS) is a secure data transfer method that allows the sender and receiver to agree on an encryption method before data is sent.

The sender's system contacts the receiver's system over a standard connection to notify them that they want to transfer data, and to request a switch to a more secure TLS connection. The sender shares a list of protocols they understand, and the receiver chooses a protocol they have in common. The receiver then provides the sender with its security certificate, the receiver verifies the certificate, and a secure TLS connection is established.

All major email providers support TLS connections, but for particularly sensitive data, you may wish to choose a provider that offers end-to-end encryption.

End-to-end encryption means that the file is encrypted when you send it and can only be decrypted by the sender. Nobody else, not even the email or cloud provider through which you're sending the file, can decrypt it. How is this different from TLS?

When you send data through an email or cloud provider, the data will often be encrypted between you and the provider using TLS, and then again between the provider and the recipient. The provider decrypts and re-encrypts the message before passing it on, so if the provider is compromised, your data may be at risk too. End-to-end encryption protects against this.

The next consideration is whether you can trust the recipient to properly handle and protect your data once received.

Protecting sensitive data at its destination

It's important to remember that email and cloud storage reside on someone else's system. When your sensitive data is leaving your control, it can be hard to guarantee that the recipient will take the same measures to protect the data as you would. That's where tools like encrypted containers and files (herein referred to collectively as 'file-level encryption') come in.

File-level encryption refers to the encryption of the individual files themselves, rather than the systems on which the files are stored or transmitted. That means that whether the data is traversing a network via a cleartext protocol, or sitting on a computer that doesn't have whole-disk encryption, the file will always have a non-trivial layer of protection around it in its primary storage location.

This is not to say that the file's contents cannot be exposed while they sit in a clear cache, page file, hibernation file, or RAM. However, accessing these storage locations is slightly more difficult than simply reading the file from primary storage. It also requires a certain amount of luck, as any data stored in those areas is transient by nature.

Ultimately, how other people manage the computers that contain the data you send to them is beyond your control. This is why you shouldn't release sensitive data to people you don't trust to properly protect it. If you must release your sensitive data, though, file-level encryption is about the best you can do to ensure its safety.

A note on encrypting external drives

Storing your data on an encrypted external drive offers no more protection than that achieved by file-level encryption on an internal drive. As soon as you go to read that data, it'll get caught up in the same cleartext-by-default locations (caches, pagefiles, RAM, etc.) that it would if it were stored on the internal drive. For that reason, you should apply whole-disk encryption to systems that handle sensitive data wherever possible.

On top of this, whenever the external drive is mounted, the decryption key will also land in those same areas. This is why systems handling data that does warrant encryption should never be put to sleep — only shut down or hibernated — and should have full encryption of their system drives at the very least.

Don't take chances with your sensitive data

It can be tough to guarantee the security of your data once it leaves your hands, but the cost of a data breach can run into the millions. Don't take chances — contact us today to learn how CyberSheath's managed cybersecurity services can keep your data and your business safe.

END OF SAMPLE

by Louise Sinclair | louise@sinclaircopywriting.com | www.sinclaircopywriting.com