

The How & Why of Data Encryption

You are probably visiting encrypted websites every day without even knowing it. Everyone has seen the prefix on web addresses “HTTP” for years, even to the point where most of us don’t even notice it anymore. (HTTP stands for hypertext transfer protocol and is the technology that allows us to transfer the text we have been typing to others.) In recent years, you may have noticed the prefix “HTTPS”, which adds the word “secure” to the abbreviation. This additional layer of security (called a “secure socket layer”, or SSL, or “transport layer security”, or TLS) uses encryption to protect the site and its users from hackers who are constantly trying to break in, whether it is to steal personal emails containing info that can be used to attack bank accounts, or secret government documents. As in most things in the ever-morphing world of cyber-technology, securing emails and files is a complex matter.

How Secure is Today’s Encryption?

Without getting into the nitty-gritty, just understand that the Data Encryption Standard (DES) that was adopted in the 1970s used a 56-bit key, which was considered unbreakable. By the 1990s, however, modern computers were able to break these codes in days. DES was replaced with AES, ([Advanced Encryption Standard](#)). Today we can use up to 256-bit keys. Today’s most powerful computer would take approximately 1,000,000,000,000,000,000 years to crack just a 128-bit key. Every “bit” doubles the time, so, there isn’t enough room on this page to show how many years it would take to crack a 256-bit key. Yes, it’s secure.

A simple definition of data encryption states that the file or message in question has been encoded so that it can only be read by the people who are supposed to read it. This is accomplished by a software program called either an algorithm or a cipher. (Origin of the word “decipher.”) The encrypted file no longer contains the easy-to-read text or numbers you started with but has been transformed into gobbledygook that can only be read after it has been unscrambled using a “key”. This “cryptographic key”, which is a long data string, makes it understandable again.

Encryption takes two basic forms, using either symmetric keys or [asymmetric keys](#). With symmetric encryption, only one key is used to both encrypt and decrypt. With asymmetric, we use

two different keys: one that encrypts and another that decrypts. Asymmetric are also known as “public” and “private” keys because anyone who wants to receive encrypted data can allow others access to their public keys, while being the only ones who can decrypt the code using their private keys.

SSL and TLS

As we stated above, SSL and TLS require a bit more explanation. Basic symmetric key encryption does a good job of encoding the data, but sending it securely is another story. If you need to send a secure document to someone, you would have to first make sure they had your key. SSL and TLS were created to solve this. When you are on an SSL or TLS protected site, your outgoing message is encrypted using your public key, then again with the recipient's public key. Upon arrival, it is decrypted. A little convoluted, perhaps, but it works. Most of the time.

The truth is, neither SSL nor TLS works perfectly and the data only remains encrypted if the server being used supports the encryption. Older servers often have out-of-date versions of SSL or TLS, if they support them at all. This often allows emails to be captured by hackers, kind of defeating the whole purpose. They can do this by compromising the SSL/TLS or scamming a website by using a fake security certificate. This is why Client-Based Encryption is so important.


Client-Based Encryption

Based on what you just read, it should come as no surprise that the best way to keep data safe is to make sure it is encrypted as it is leaving your device and remains that way until it reaches the rightful recipient. To accomplish this, we use client-based (or client-side) encryption. An email should leave your device as a long, scrambled string so it won't matter whether or not a server through which it passes supports encryption. Any nefarious hacker who captures your email can't read it; they won't have the correct encryption key.

PGP and S/Mime

[PGP](#) (Pretty Good Privacy – yes, that's a real thing) and [S/MIME](#) (Secure/Multipurpose Internet Mail Extensions) are standards for public key encryption and signing of MIME data – (Wikipedia) have been around since the early to mid-1990s and do provide a “pretty good” level of protection for email, but they are inconvenient to use. The software for encryption has to be installed, then you have to use the software to create your public and private keys, register your own public key while receiving your recipient's public key, put his/her public key on your “keyring”, and then, at last, encrypt and send your message. There are also built in protections to make sure you are receiving a valid decryption key, not a fake generated from a hacker.

The best way to keep data safe is to make sure it is encrypted as it is leaving your device and remains that way until it reaches the rightful recipient. To accomplish this, we use client-based (or client-side) encryption. An email should leave your device as a long, scrambled string so it won't matter whether or not a server through which it passes supports encryption.



After examining a great number of cyber-security software programs, we are currently using two, selecting the right one for each client. While a lot of evaluation goes into each selection, we're going to discuss two basic premises and the likely selection for each.

PGP uses what they call a "Web of Trust". As you share your key with people and they let the PGP people know they trust you, your "web of trust" grows and newcomers come to understand they also can trust you. If you trust everyone with whom you share it, and they keep it secure, you're ok. If not, well...

There are drawbacks to both systems:

- > You can't send a secure email to anyone who has not created a public key.
- > You have to individually encrypt each message you want to send, so no group emails.
- > Some recipients may be using PGP while others use S/MIME so you have to have both installed and you have to have a working knowledge of both.
- > You must protect both your PGP and S/MIME private keys because if someone gets ahold of them, all your emails can be exposed.
- > You will have to take the time to set up both systems on all your devices.

While either system may provide you with the protection you need, neither provides the convenience required to be truly effective in today's technology world.

A Better Way

PGP and S/MIME are not the same programs that were originally developed in the latter part of the last century. They have progressed. But like so many other things in the tech world, entirely new technologies have been developed that take protective encryption to whole new level. One of the great things about being a [managed IT support](#) provider is that we have the technical know-how and staff bandwidth to investigate new solutions and dig deep in determining those that are best for our clients. After examining a great number of cyber-security software programs, we are currently using two, selecting the right one for each client. While a lot of evaluation goes into each selection, we're going to discuss two basic premises and the likely selection for each.

Mimecast

When a client is in need of [email security](#) that in our determination is best provided by encryption, we often choose [Mimecast](#). Many companies believe their email systems are secure. This is often not the case. Mimecast offers a much higher level of email protection than most companies now have and is currently serving almost 30,000 clients. Unfortunately, email can open the doors

to a tremendous amount of risk because, since virtually every business uses email, it is also the primary target of many cyber-criminals. To protect your business, you need to prevent attacks before they happen, minimize any disruptions that might happen if and when an attack is successful, and rapidly recover any lost email and data afterwards.

Mimecast's cloud-based service provides:

- > **Threat protection** – a multi-layered internal review system that pulls together unique 3rd party technologies and literally dozens of threat intelligence resources, both internal and external.
- > **Adaptability** – A major key to cyber-protection today is the ability to keep at least one-step ahead of the newest attacks. Mimecast is continually using 3rd party technologies to keep its clients prepared for the latest, along with ongoing employee education.
- > **Durability** – Cyber-attacks may result in email going offline, or it may be shut down by your IT department to prevent damage during such an attack. With Mimecast, your existing emails remain fully available during such times.
- > **Recoverability** – In the event that email is destroyed, the Mimecast system will allow simplified and automated recovery of all emails and data kept in your email system.

[This video](#) will help you understand more about the protections Mimecast offers.

Galaxkey

There are organizations that require more than email encryption and the other protections offered by Mimecast. Some organizations need every document they keep to be fully encrypted in case of data-theft. Galaxkey offers this protection, along with email security similar to that of Mimecast, however, it can also encrypt every file in your system

Galaxkey is an identity-based system, meaning that every user must register so that a secure and unique “user identity” can be created and attached to his/her email address. Once this identity is established, the user uses it on all devices with all files and all are secure. People who have received emails secured with the Galaxkey system can reply securely. The platform can be used on-premise, cloud, or in hybrid format.

Making the Choice:

The first thing you should do is conduct an [IT Network and Security Assessment](#) to determine where your network currently stands, then review your options with an experienced and technically qualified [managed IT support](#) company like [DynaSis](#).

Our assessment is complimentary and will give you a good look into your security strengths and weaknesses and allow us to discuss upgrades with you that may be advisable. Give us a call today at 678-373-0716.