Email Encryption

Technology with Integrity

By Tim Torian, Torian Group, Inc.

Summary: You should be encrypting email with sensitive information. Verify your email client is using a secure connection to the email server (using TLS or SSL). For occasional use, put sensitive information in a password protected zip file and send it as an attachment - communicate the password verbally. For frequent use, set up a portal for your clients with links sent via email. Enable encryption on mobile devices. If desired, store your email in an encrypted folder on your hard drive.

Background

Email is almost universally used. The email system was developed over 50 years ago, when security was not a concern. Authentication and confidentiality were added only as an afterthought. Sending information in an unencrypted email is the equivalent of writing it on a postcard for all to see. Up to 20% of all emails are routinely attacked, say researchers, after studying 700,000 email servers.

Once delivered, a single email can continue to reside on your computer, your computer's backup, your recipient's computer, his or her computer's backup, your email carrier's computers and its computer backups, and possibly on the computers of bad actors and/or government spy agencies that systematically intercept billions of email messages as they are delivered. Simply put, you can't undo an email.

If your company handles sensitive information, you may be required by law to secure your communications. As a business owner, you may be liable for what your employees are doing with their email. If security is an issue, there are no legitimate alternatives- you must encrypt your email.

A Definition of Email Encryption

Email encryption involves encrypting, or disguising, the content of email messages to protect potentially sensitive information from being read by anyone other than intended recipients. Email encryption can include authentication – verifying the source of the message.

Encryption renders the content of your emails unreadable as they travel from origin to destination, so even if someone intercepts your messages, they can't interpret the content.

There are three things you should consider protecting:

The connection from your email provider – Use TLS or HTTPS.
Your actual email messages – encrypt the message or encrypt an email attachment.
Your stored, cached, or archived email messages – encrypt the storage device.

How to Compare Email Encryption Methods

Multiple options to secure email differ in their security features and ease of use. Some were designed for compliance where both the sender and receiver are required by law to encrypt in a certain way. Some are for large companies that want to enforce security on

their employees' email usage. Ease of use or actual protection against modern attacks was not a concern. We want to select an email encryption option that's best for small business -easy to set up and easy to use. Here is what we should evaluate for each email encryption option:

Security

- **In transit:** Can the email be read by an attacker while travelling over the network?
- **On a server:** Will theft or unauthorized access to a storage device, such as a hard disk or a computer at your, or your receiver's email server, or any intermediate email relay cause your data to be leaked.
- **Stored on devices (phone, laptop, desktop):** Will theft, loss or unauthorized access to your device cause emails to be leaked?

Ease of use (for you and your clients)

- **Set up:** How easy is it for you to install, create an account or otherwise get started with using it?
- **Daily Use:** How easy is to send and receive emails after the correct setup?
- **Easy for clients to receive:** How easy is it for your clients to open your encrypted messages. How much setup to they need to do?
- **Easy for clients to send:** How easy is it for your clients to send you an encrypted message? Do they need to purchase and install an encryption product?

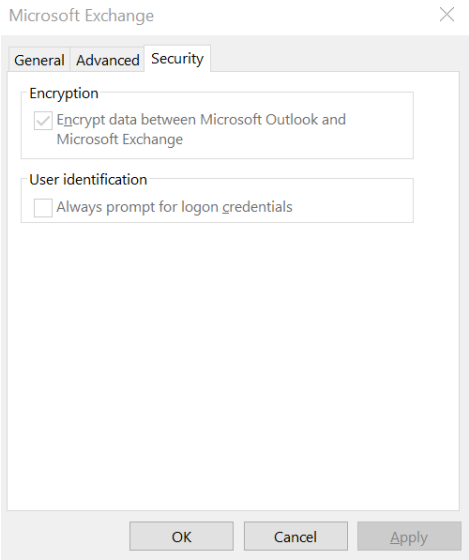
Encryption in Transit -The connection from your email provider.

Encryption in transit means that the email data is encrypted while it travels from one email server to another. This is based on a mail server configuration known as Transport Layer Security (TLS). It is being promoted by major email providers such as Gmail, Microsoft Exchange and others.

You need not do anything to set up. As long as your email provider uses it, you get this benefit automatically. You should verify that TLS is used for the connection from your device to the email server and consider changing providers if it is not.

In Outlook for desktop PCs, go to File > Account Settings. Select the account and then Change > More Settings > Security. Here you should see a setting that indicates "Encrypt data between Microsoft Outlook and [your mail server]." The exact words may vary based on your Outlook version and email server. This setting should be enabled.

Outlook SSL setting screenshot



If you connect to your email using a web browser, make sure you use HTTPS (not HTTP) at the start of the URL. In most cases this is automatically ensured by the webmail service. This also provides a secure connection.

If you check your email from an app, such as Outlook on a desktop or the iPhone Mail app on the phone, make sure that Secure Socket Layer (SSL) is enabled. SSL secures the connection from your device to the email server, much like TLS secures the connections between email servers.

If the recipient's email server does not provide a secure connection, your email will not be protected in transit on their end.

Setup: Confirm your email settings are correct.
Daily use: No change.
Easy for clients to receive: Seamless. TLS will be silently disabled if the recipient does not support it. Ease of use prevails over security here.
Easy for clients to send to you: Your clients email you normally.
Protected on Server? No.
Protected on Devices? No.

Encrypting an attachment

This is a good solution for most small businesses, but still requires an extra step. Rather than encrypting the entire email message, you put the sensitive message in a document, encrypt the document, and send it as an attachment via normal email. The recipient then decrypts the document using a password you have sent them separately.
We recommend using 7-zip – it is free and fairly easy to use. Create a password-protected archive (with AES-256 encryption) and add your message as a document along with any other documents you want to send. Let the recipient know the password (not via email). Make sure they have 7-zip installed.

Vendors offer tools to automate the attachment encryption process. All require that the recipient have a password or key to retrieve the attachment. To reply securely, they would also need to sign up and possibly configure their (compatible) email software with the plug-in. It automated the process of encrypting email attachments. It is easier to use, but harder to set up.
Here are a couple:
https://www.sendsafely.com/features/
https://www.sendthisfile.com/features/outlook-plugin/index.jsp

Setup: Moderate. Install and learn to use 7-zip or other file encryption software.
Daily use: Inconvenient. Requires an extra step to send or receive.
Easy for clients to receive: Requires that they use a program and password.
Easy for Clients to Send: Requires that they use a program and password.
On Server: N/A
On Device: Once decrypted and saved, it is unprotected.

Secure Webmail

These look a lot like other webmail services such as Gmail, Yahoo! Mail or Hotmail, except that they support encryption. You sign up for one of these services and get a new email address just like you would get with any other webmail service.
The big advantage here is that it is very easy to use. The problem is that the recipient also needs to sign up for an account and use a web interface to retrieve the message.
Vendors include: SendInc, safe-mail.net, and MDOfficeMail.com, among others
Additional setup may be required to integrate with Outlook or your email program. Once you have an account, you need to select a password or password like question for every recipient - a question that only your recipient will be able to answer.

Setup: Account creation is like signing up for webmail.
Daily use: Easy.
Easy for clients to receive: No. Requires that they create an account on the same service.
Easy for Clients to Send: No. Encrypted webmail services do not allow your clients to send you an encrypted message unless they create their own account.
On Server: depends on vendor
On Device: If saved outside of the web browser, it is unprotected.

Web Portals

Some websites implement their own document or message portal that customers sign into. Online banking websites and some hospitals use this.
Portal systems work by keeping communication within the boundaries of the portal itself. You have to log in to access the outgoing mail service, and the receiver has to log in to access incoming mail.
Some variations of this provide a link in traditional email to access the secured message, but still require an account for the client to login and retrieve the message.

Setup: Setup is as easy as signing up. Everyone you email must also sign up.

Daily use: requires that you (and the recipient) log in and use the portal for all email. This may limit integration with other software. It also may not integrate with your business email domain.
Easy for clients to receive: Difficult - requires that they create an account and log in.
Easy for Clients to Send: No. portal based services do not allow your clients to send you an encrypted message unless they create their own account. Some provide an upload link to save to your portal, but still require an account/login.
On Server: secure
On Device: If saved outside of the portal, it is unprotected.

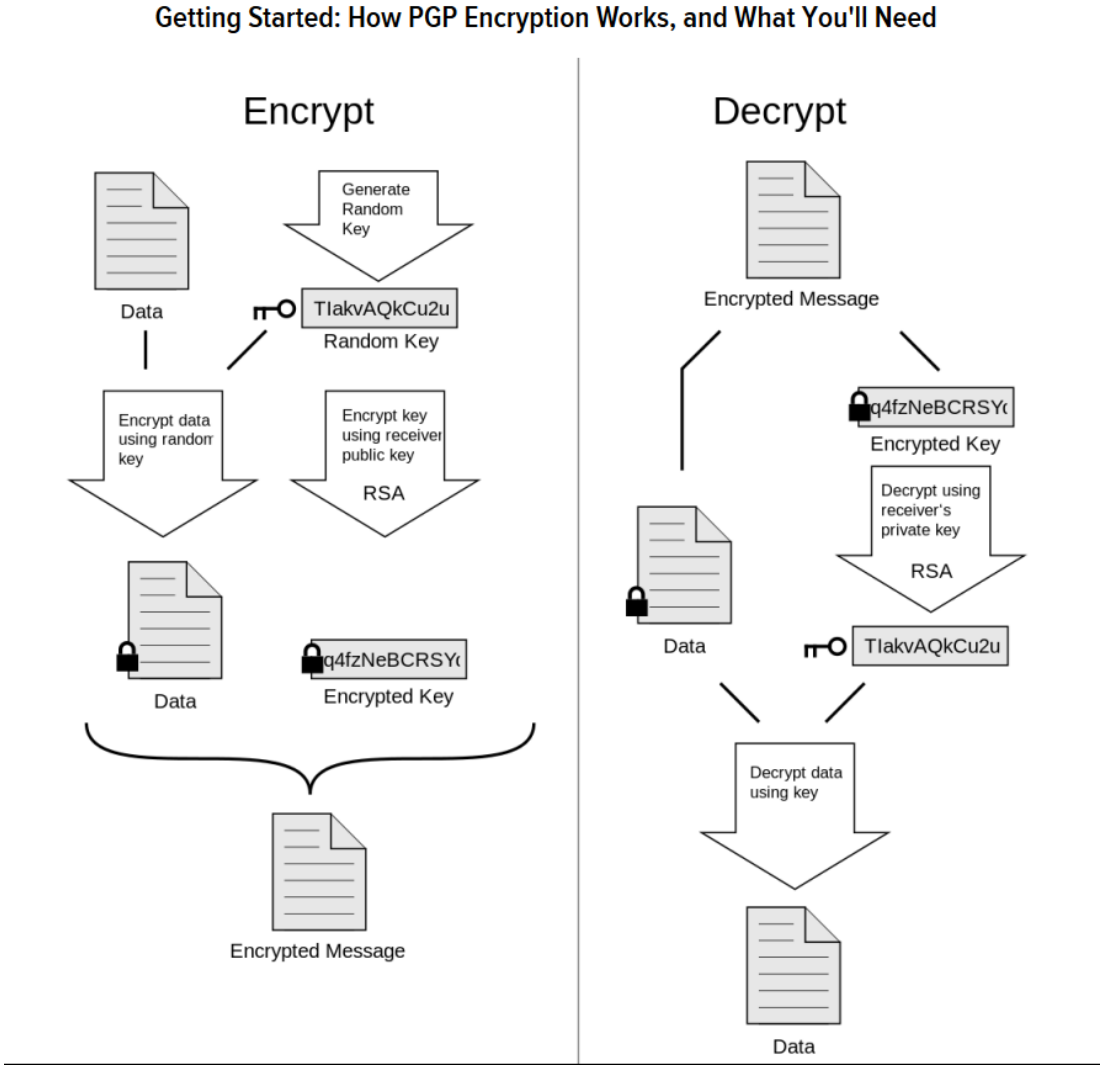
Linked File Storage

This is a variation on a web portal where the email contains a link to a secured document. The document is uploaded to a secure portal, and the link allows the recipient to retrieve the attachment.
One popular portal is sharefile.com Many file storage sites offer add-ins to allow sharing files via emailed links, including DropBox.com, Box.com, OneDrive, and Google Drive (with Gmail).

Setup: Setup is as easy as signing up. Everyone you email must also create an account.
Daily use: requires that you save the attachment for retrieval.
Easy for clients to receive: Moderate - requires that they create an account and log in.
Easy for Clients to Send: Moderate. Some provide an upload link to save to your portal, but still require an account/login.
On Server: secure
On Device: If saved outside of the portal, it is unprotected.

Key Based Email Encryption

This will only be relevant if it is required for compliance – otherwise it is generally too much trouble. Setup will likely require assistance from an IT professional. Each person you email securely will need to be set up separately.
You create a public key and a private key. The key is usually from a vendor (such as Comodo). The public key, shared with the world, allows anyone to encrypt a message that they are sending you (once they have the public key, which you must provide to them). The private key, known only to you, allows a decrypting of those messages. So, if you are sending someone an encrypted message, your receiver will need a public and private key pair. You will also need to know their public key. Each person you email will need to set this up separately on both ends.
Some products such as InfoCrypt, Enigmail, iSafeguard, Mailvelope, and SafeMess try to make the encryption steps easier. But you still need to communicate the keys to your email recipients separately.
The big advantage here is that only you know the encryption keys. So, no other organization, such as the National Security Agency (NSA) could read your email easily.
There are laws that may prevent you from sending emails encrypted in this manner across international boundaries, so be aware.



Ease of Use: Difficult
Setup: Very hard.
Daily Use: Difficult.
Easy for Clients to Receive: Difficult for most recipients.
Easy for Clients to Send: Forget about it!
On Server: stays encrypted in transit
On Devices: Normally decrypted on send / receive. Stored decrypted – not protected.

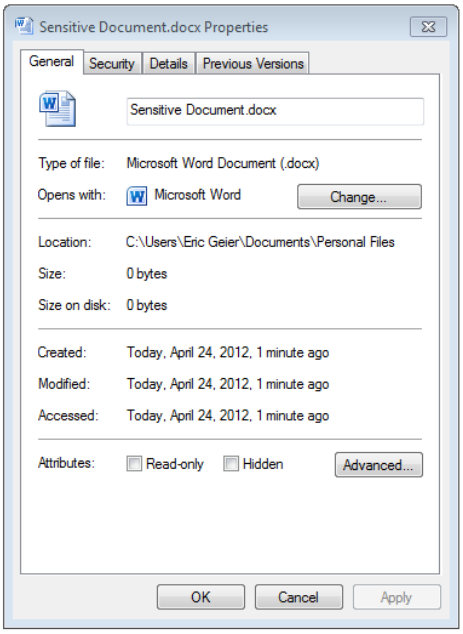
How to Encrypt Email stored on your Computer

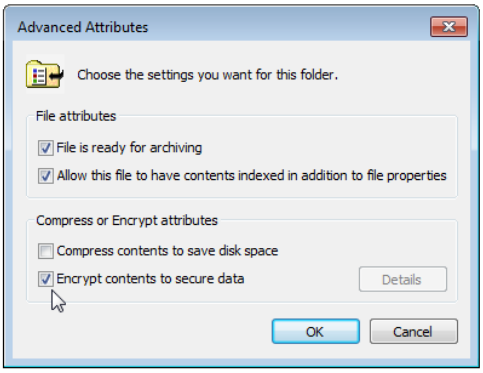
If you use an email client or app on your computer or mobile device, rather than checking your email via a Web browser, and you are concerned about it being accessed should your computer get stolen or compromised, you can encrypt your stored email data. This will need to be done on each device you use for email. If the encrypted folder gets damaged or you lose the encryption key, the data is lost.

For mobile devices it's best to use an operating system that provides full device encryption by setting a PIN or password to protect your email and other data. Android (3.0 and later) BlackBerry, and iOS (iPhone, iPad, and iPod Touch) devices offer this type of encryption.

For desktops and laptops, you can encrypt just your email data files if you prefer not to encrypt the whole computer. Once you've determined where your email client stores your data, right-click the file(s) or the folder that contains them, select *Properties*, click *Advanced*, and select *Encrypt contents to secure data*.

Encrypting files with the Encrypted File System (EFS) feature of Windows.





That's all you have to do. The EFS feature will open and automatically decrypt file(s) when you're logged into your Windows account. Remember to disable encryption before reinstalling Windows or changing your Windows account, or you'll risk being unable to decrypt the files later.

You can also encrypt specific folders using Veracrypt, AxCrypt or GNU Privacy Guard.

Backup software should be set to store the encrypted file, not decrypt and then backup. Be sure to store any encryption keys somewhere safe and separate from your computer.

In summary, be aware that email is insecure, and take the right level of precautions for your business needs.

Tim Torian has his degree in Computer Science, and has been consulting on technology for business for the past 30+ Years. He has multiple industry certifications including Microsoft and Cisco. He has taught computer networking at the College of Sequoias and Cal Poly Extension. He was awarded “Entrepreneur of the year” by the Tulare County EDC in 2008. Torian

Group was awarded “Technology Business of the Year” by the SBDC in 2011. He is president of Torian Group, Inc. which provides a full range of Technology Consulting services to local business, including computer services, networking, web design and Internet marketing. www.toriangroup.com