How to encrypt email

If not encrypted, your email is at risk of being hacked and read at any time, or you may lose your account. This article will give you an overview of how to encrypt email, help you understand and choose the right encryption solution.

If not encrypted, your email is at risk of being hacked and read at any time, or you may lose your account. This article will give you an overview of how to encrypt email, help you understand and choose the right encryption solution.

Even if you have never emailed sensitive information - such as bank account information, business secrets - you should also consider using encryption. In addition to *"intercepting"* email content and attachments, scammers can take over the entire email account if you don't have reasonable security. This article will help you know what you need to code for and start, regardless of which email service you are using.

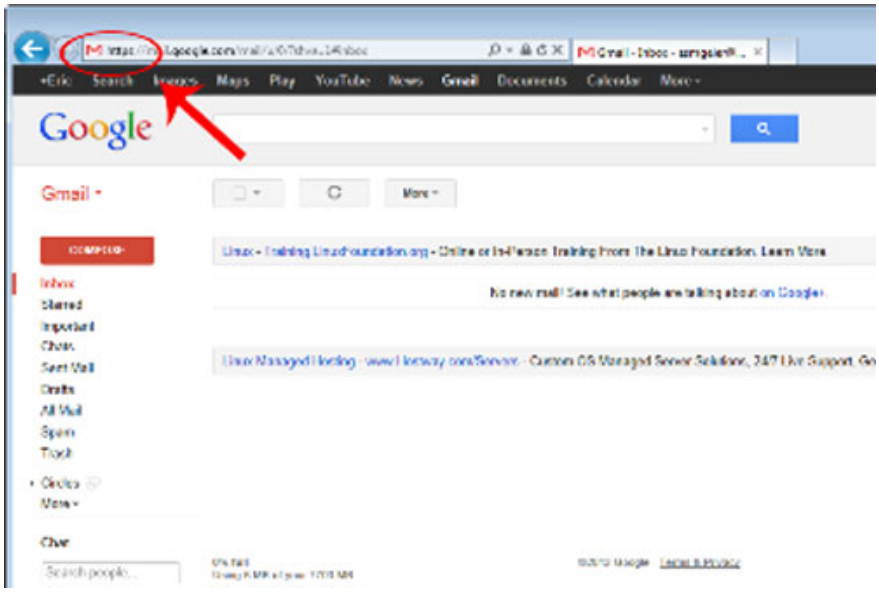
Need to encrypt what?

To secure your email effectively, you should encrypt 3 things: that is, encrypt the connection from your email service provider, encrypt the outgoing email content and encrypt the archived email content. If you do not encrypt the connection from your email service provider to your computer or another device while checking or sending a message, other users in your network can easily *'grab'* the login account. or any content you send or receive.

The danger is often when you access the internet in a public place (such as accessing a Wi-Fi in a cafe), but connecting without encryption can also cause problems in your work or when using the network. private. The content of your email has been easily compromised when they are on the Internet, after the message has just *'left'* the email server's server. Bad guys can block a message when it has just moved from one server to another on the Internet.

Therefore, encrypting content before sending will make it impossible for crooks to read it, from the moment the content starts *'walking'* on the Internet until it reaches the recipient to open the message. If you save or back up email (from an email application like Microsoft Outlook) on your computer or device, hackers can *'sniff'* to access that content, even if you set it Password protected on email programs and on Windows or mobile devices. Again, encryption makes an attacker unable to read the email content.

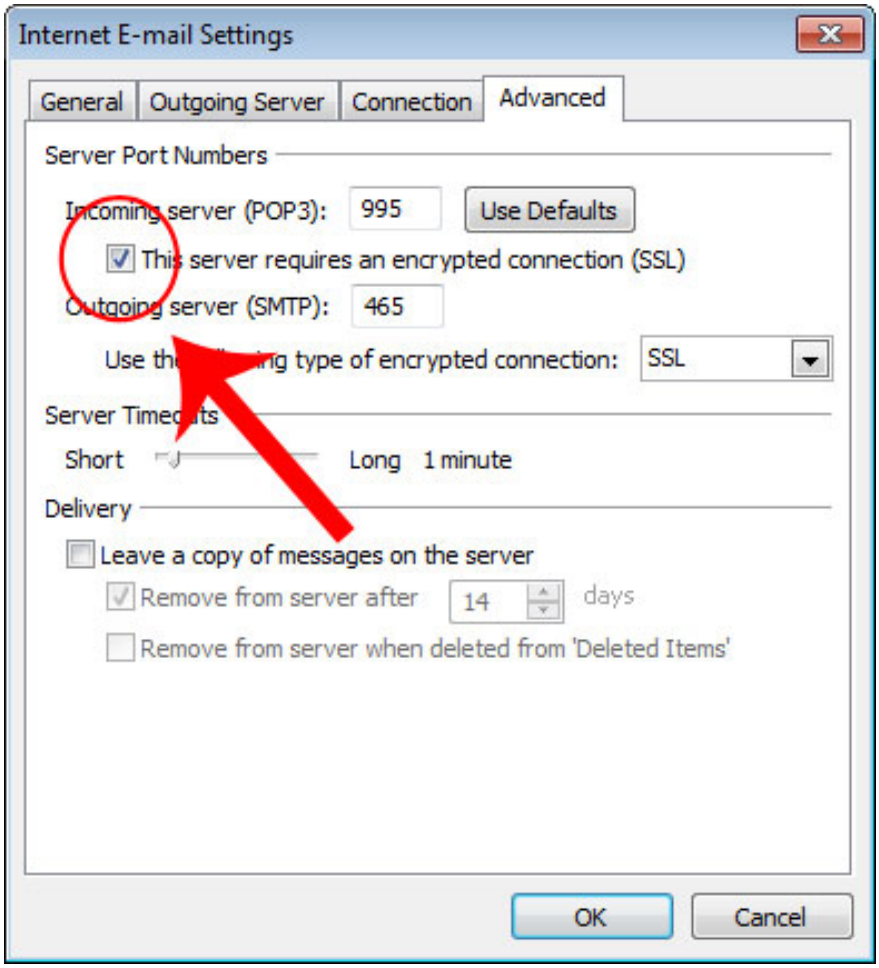
Encrypt connection



To ensure the connection between an email service provider and another computer or device, you need to install SSL (Secure Socket Layer) and TLS (Transport Layer Security) encryption - similar to the protection which you use when checking your bank account or doing online transactions.

If you check email via a web browser (whether on a desktop, laptop, smartphone or tablet), it may take a while to make sure that the SSL / encryption protocol is TLS is enabled. If done correctly, the website address will start with https instead of http. Depending on the browser, you will see some additional signs, such as a notification next to the address bar or a yellow padlock icon on the status bar at the bottom of the browser window.

If you don't see the https address and other indicators after logging into the email program on the web, type one more letter at the end of '**http**' and press **Enter.** If the email service provider supports the SSL / TLS protocol, this way will help encrypt your current connection. Then, browse your account settings to see if you can enable encryption by default, or whether you can edit bookmarks or create shortcuts to webmail using the *'https' address* . If you cannot *'* encrypt *' the* encryption, check your email service provider because they may not support the SSL / TLS protocol.



If you use an email program like Microsoft Outlook to receive email or an email application on a smartphone or tablet, you should try to use SSL / TLS encryption.

However, in such situations, it will be more difficult to validate or establish encryption. To do so, open the email program or application and navigate to the setup menu; There, your account is *'labeled'* POP / SMTP, IMAP / SMTP, HTTP or Exchange account. Find options to enable encryption, usually in advanced settings where you can specify the port number for incoming and outgoing connections.

If you use an Exchange email account for work, you will see a section for security settings, where you can see whether encryption / security is enabled for incoming and outgoing connections as well as for accounts. Your Exchange or not. If it is not enabled, check your email service provider to see if they support this encryption and can search for other providers that support SSL / TLS encryption.

Encrypt sent email

You can encrypt personal email content during email migration, but both you and the recipient must perform some operations to ensure security is secured. You can use the encryption features integrated in the email service or you can download encryption software or auxiliary applications using the OpenPGP method.

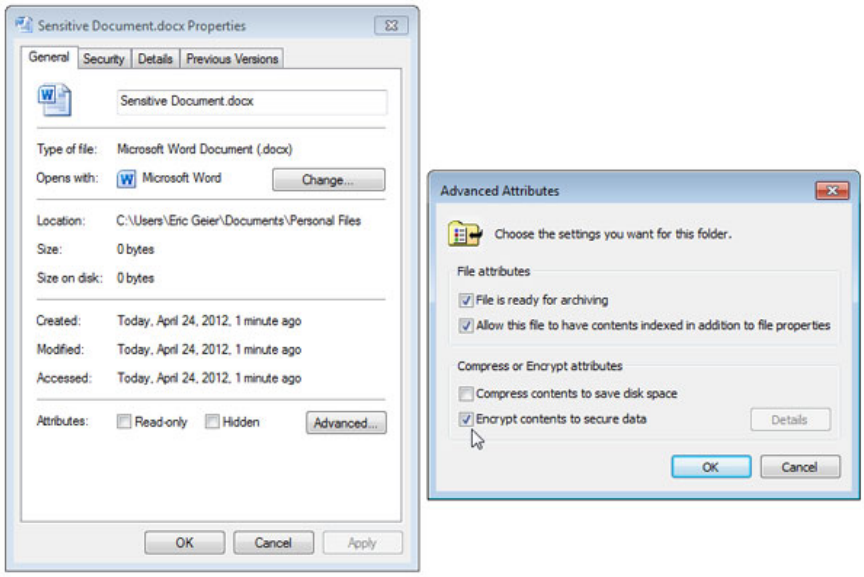
In urgent cases, you can use web-based encrypted email services such as Sendinc or JumbleMe, although you must delegate to third parties. Most methods of encrypting email content, including S / MIME (Secure /

Multipurpose Internet Mail Extensions) and OpenPGP, require you to install a security certificate on your computer and provide your contacts via a string of characters, called public keys before you receive them. encrypted content. Similarly, your mail recipients must also install a security certificate on their computer and the recipient will provide you with their public key first.

Support for S / MIME standards is built into many email programs, including Microsoft Outlook. In addition, web browser utilities, such as Gmail S / MIME for Firefox, also support web-based email service providers.

OpenPGP email encryption standard has several variants, including PGP and GNU Privacy Guard (GnuPG). You can find free or commercial software and add-ons, such as Gpg4win, PGP Desktop Email, to support OpenPGP standard encryption.

Encrypt archive email



If you prefer to use an email client on your computer or a mobile application rather than through a web browser, you should make sure that the email data is stored encrypted so that the attackers on the network cannot access it. saved email content, if you miss or have someone steal your device.

The best way is to encrypt the entire content on a laptop or mobile device, because mobile devices often fall into the special case of being lost or stolen. For mobile devices, it is best to use an operating system that provides full encryption on the device by setting up a PIN or password to protect your email and other data.

BlackBerry and iOS devices (such as iPhone, iPad and iPod Touch) have provided this type of encryption for years; Android supports only version 3.0 or higher. Older Android devices can use 3rd party email applications, such as TouchDown, that provide encryption for Exchange accounts.

For desktop and laptop computers, you can encrypt email data files if you don't want to encrypt the entire content on your computer. The encryption functions of each email program are different, so check the documentation for each program and the specific version. If your email program does not provide reliable encryption, select the encryption option under the directory where your email is stored.

For example, if you use the Professional, Business or Ultimate versions of Windows, you can encrypt email content, regardless of the email program you use, thanks to Windows' Encrypted File System (EFS) feature. . First of all, find the file types that your email program uses to store email content; Microsoft Outlook uses the .PST file to save the content, or .OST file for Exchange accounts. In Windows XP, you will find the file in *C: Documents and SettingsyourusernameLocal SettingsApplication DataMicrosoftOutlook.* In Windows Vista and 7, that's *C: UsersyourusernameAppDataLocalMicrosoftOutlook.*

Once you have determined where your email is stored, right-click on the file or folder containing the content, select Properties, click Advanced and choose Encrypt for encryption. That's all you need to do. The EFS feature will help open files and decode automatically when you log in to your Windows account.

Remember to disable encryption before reinstalling Windows or changing your Windows account or you'll risk being unable to decrypt files later!