Published on *Security In A Box* (https://security.ngoinabox.org)

7. How to keep your Internet communication private

The convenience, cost-effectiveness and flexibility of email and instant messaging make them extremely valuable for individuals and organizations with even the most limited access to the Internet. For those with faster and more reliable connections, software such as *Skype* [1] and other *Voice-over-IP VoIP* [2] tools also share these characteristics. Unfortunately, these digital alternatives to traditional means of communication can not always be relied upon to keep sensitive information private. Of course, this is nothing new. Postal mail, telephone calls and text messages are all vulnerable as well, particularly when used by those who may have been targeted for surveillance by the authorities.

One important difference between digital, Internet-based communication techniques and more traditional methods, is that the former often allow you to determine your own level of security. If you send emails, instant messages and *VoIP* [2] conversations using insecure methods, they are almost certainly less private than letters or telephone calls. In part, this is because a few powerful computers can automatically search through a large amount of digital information to identify senders, recipients and specific key words. Greater resources are required to carry out the same level of surveillance on traditional communication channels. However, if you take certain precautions, the opposite can be true. The flexibility of Internet communication tools and the strength of modern *encryption* [3] can now provide a level of privacy that was once available only to national military and intelligence organizations.

By following the guidelines and exploring the software discussed in this chapter, you can greatly improve your communication security. The *RiseUp* [4] email service, the Off the Record *OTR* [5] plugin for the *Pidgin* [6] instant messaging program, Mozilla *Firefox* [7] and the *Enigmail* [8] add-on for the Mozilla *Thunderbird* [9] email client are all excellent tools. While using them, however, you should keep in mind that the privacy of a given conversation is never one hundred percent guaranteed. There is always some threat that you did not consider, be it a *keylogger* [10] on your computer, a person listening at the door, a careless email correspondent or something else entirely. The goal of this chapter is to help you reduce even the threats that do not occur to you, while avoiding the extreme position, favoured by some, that you should not send anything over the Internet that you are not willing to make public.

Claudia and Pablo work with a human rights NGO in a South American country. After spending several months collecting testimonies from witnesses to the human rights violations that have been committed by the military in their region, Claudia and Pablo have begun taking steps to protect the resulting data. They have kept only the information they need, which they store in a TrueCrypt partition that is backed up in several physical locations. While preparing to publish certain aspects of these testimonies in a report, they have found that they must discuss sensitive information with a few of their colleagues in another country. Although they have agreed not to mention names or locations, they still want to ensure that their email and instant messaging conversations on this topic remain private. After calling a meeting to discuss the importance of communication security, Claudia has asked if anyone in the office has questions.

What you can learn from this chapter

- Why most webmail and instant messaging services are not secure
- How to create a new and more secure email account
- How to improve the security in your current email account
- How to use a secure instant messaging service
- What to do if you think someone might be accessing your email
- How to verify the identity of an email correspondent

Securing your email

There are a few important steps that you can take in order to increase the security of your email communication. The first is to make sure that only the person to whom you send a given message is able to read it. This is discussed in the *Keeping your webmail private* [11] and *Switching to a more secure emailaccount* [12] sections, below. Going beyond the basics, it is sometimes critical that your email contacts have the ability to verify that a particular message truly came from you and not from someone who might be attempting to impersonate you. One way to accomplish this is described under *Advanced email security* [13], in the *Encrypting and authenticating individual email messages* [14] section.

You should also know what to do if you think the privacy of your email account may have been violated. The *Tips on responding to suspected email surveillance* [15] section addresses this question.

Remember, too, that secure email will not do you any good if everything you type is recorded by spyware and periodically sent over the Internet to a third party.*Chapter 1: How to protect your computer from malware and hackers* [16] offers some advice on how to prevent this sort of thing, and *Chapter 3: How to create and maintain secure passwords* [17] will help you protect your accounts for the email and instant messaging tools described below.

Keeping your webmail private

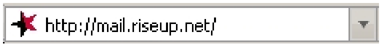
The Internet is an open network through which information typically travels in a readable format. If a normal email message is intercepted on the way to a recipient, its contents can be read quite easily. And, because the Internet is just one large, worldwide network that relies on intermediary computers to direct traffic, many different people may have the opportunity to intercept a message in this way. Your *Internet Service Provider* *ISP* [18] is the first recipient of an email message as it begins its journey to the recipient. Similarly, the recipient's *ISP* [18] is the last stop for your message before it is delivered. Unless you take certain precautions, your messages can be read or tampered with at either of these points, or anywhere in between.

Pablo: I was talking to one of our partners about all this, and she said that she and her colleagues sometimes just save important messages in the 'Drafts' folder of a webmail account where they all share a password. It sounds kind of strange to me, but would it work? I mean, wouldn't that prevent anyone from reading the messages, since they're never actually sent?

Claudia: Any time you read an email on your computer, even if it's just a 'draft,' its contents have been sent to you over the Internet. Otherwise, it couldn't appear on your screen, right? The thing is, if someone has you under surveillance, they don't just monitor your email messages, they can scan all readable information going to and from your computer. In other words, this trick wouldn't work unless everyone connects securely to that shared webmail account. And, if they do, then it really doesn't hurt to create separate accounts or to go ahead and hit that 'send' button.

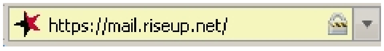
It has long been possible to secure the Internet connection between your computer and the websites that you visit. You often encounter this level of security when entering passwords or credit card information into websites. The technology that makes it possible is called Secure Sockets Layer *SSL* [19] *encryption* [3] . You can tell whether or not you are using *SSL* [19] by looking closely at your Web browser's **address bar**.

All Web addresses normally begin with the letters **HTTP**, as can be seen in the example below:



http://mail.riseup.net/

When you are visiting a secure website, its address will begin with **HTTPS**.



https://mail.riseup.net/

The extra **S** on the end signifies that your computer has opened a secure connection to the website. You may also notice a 'lock' symbol, either in the **address bar** or in the **status bar** at the bottom of your browser window. These are clues to let you know that anyone who might be monitoring your Internet connection will no longer be able to eavesdrop on your communication with that particular website.

In addition to protecting passwords and financial transactions, this type of *encryption* [20] is perfect for securing your webmail. However, many webmail providers do not offer secure access, and others require that you enable it explicitly, either by setting a preference or by typing in the **HTTPS** manually. You should always make sure that your connection is secure before logging in, reading your email, or sending a message.

You should also pay close attention if your browser suddenly begins to complain about invalid *security certificates* [21] when attempting to access a secure webmail account. It could mean that someone is tampering with the communication between your computer and the server in order to intercept your messages. Finally, if you rely on webmail to exchange sensitive information, it is important that your browser be as reliable as possible. Consider installing Mozilla *Firefox* [7] and its security-related add-ons.

Hands-on: Get started with the *Firefox Guide* [22]

Pablo: One of the guys who's going to be working on this report with us tends to use his Yahoo webmail account when he's not in the office.And I seem to remember somebody else using Hotmail. If I send a message to these guys, can other people read it?

Claudia: Probably. Yahoo, Hotmail and plenty of other webmail providers have insecure websites that don't protect the privacy of their users' messages. We're going to have to change some people's habits if we want to be able to discuss these testimonies securely.

Switching to a more secure email account

Few webmail providers offer *SSL* [19] access to your email. Yahoo and Hotmail, for instance, provide a secure connection while you log in, to protect your password, but your messages themselves are sent and received insecurely. In addition, Yahoo, Hotmail and some other free webmail providers insert the *IP address* [23] of the computer you are using into all of the messages you send.

Gmail accounts, on the other hand, can be used entirely through a secure connection, as long as you login to your account from *https://mail.google.com* [24] (with the **HTTPS**), rather than *http://mail.google.com* [25] . In fact, you can now set a preference that tells Gmail always to use a secure connection. And, unlike Yahoo or Hotmail, Gmail avoids revealing your *IP address* [23] to email recipients. However, it is not recommend that you rely entirely on Google for the confidentiality of your sensitive email communication. Google scans and records the content of its users' messages for a wide variety of purposes and has, in the past, conceded to the demands of governments that restrict digital freedom. See the ***Further reading*** [26] section for more information about Google's privacy policy.

If possible, you should create a new *RiseUp* [4] email account by visiting *https://mail.riseup.net* [27].*RiseUp* [4] offers free email to activists around the world and takes great care to protect the information stored on their servers. They have long been a trusted resource for those in need of secure email solutions. And, unlike Google, they have very strict policies regarding their users' privacy and no commercial interests that might some day conflict with those policies. In order to create a new *RiseUp* [4] account, however, you will need two 'invite codes.' These codes can be given out by anyone who already has a *RiseUp* [4] account. If you have a bound copy of this booklet, you should have received your 'invite codes' along with it. Otherwise, you will need to find two [*RiseUp*]/glossary#RiseUp) users and ask them each to send you a code.

Hands-on: Get started with the *RiseUp Guide* [28]

Both Gmail and *RiseUp* [4] are more than just webmail providers. They can also be used with an email client, such as Mozilla *Thunderbird* [9] , that supports the techniques described under ***Advanced email security*** [13] . Ensuring that your email client makes an *encrypted* [3] connection to your provider is just as important as accessing your webmail through **HTTPS**. If you use an email client, see the ***Thunderbird Guide*** [29] for additional details. A the very least, however, you should be sure to enable *SSL* [19] or *encryption* [3] for both your incoming and outgoing mail servers.

Pablo: So, should I switch to using RiseUp or I can keep using Gmail, and just switch to the secure 'https' address?

Claudia: It's your call, but there are a few things you should definitely consider when choosing an email provider. First, do they offer a secure connection to your account? Gmail does, so you're OK there. Second, do you trust the administrators to keep your email private and not to read through it or share it with others? That one's up to you. And, finally, you need to think about whether or not it's acceptable for you to be identified with that provider. In other words, will it get you in trouble to use an email address that ends in 'riseup.net', which is known to be popular among activists, or do you need a more typical 'gmail.com' address?

Regardless of what secure email tools you decide to use, keep in mind that every message has a sender and one or more recipients. You yourself are only part of the picture. Even if you access your email account securely, consider what precautions your contacts may or may not take when sending, reading and replying to messages. Try to learn where your contacts' email providers are located, as well. Naturally, some countries are more aggressive than others when it comes to email surveillance. To ensure private communication, you and your contacts should all use secure email services hosted in relatively safe countries. And, if you want to be certain that messsages are not intercepted between your email server and a contact's email server, you might all choose to use accounts from the same provider. *RiseUp* [4] is one good choice.

Additional tips on improving your email security

- Always use caution when opening email attachments that you are not expecting, that come from someone you do not know or that contain suspicious subject lines. When opening emails like this, you should ensure that your anti-virus software is up-to-date and pay close attention to any warnings displayed by your browser or email program.
- Using anonymity software like *Tor* [30], which is described in ***Chapter 8: How to remain anonymous and bypass censorship on the Internet*** [31], can help you hide your chosen email service from anyone who might be monitoring your Internet connection. And, depending on the extent of Internet filtering in your country, you may need to use *Tor* [30], or one of the other *circumvention* [32] tools described in ***chapter 8*** [31], just to access a secure email provider such as *RiseUp* [4] or Gmail.
- When creating an account that you intend to use while remaining anonymous from your own email recipients, or from public forums to which you might post messages by email, you must be careful not to register a username or 'Full Name' that is related to your personal or professional life. In such cases, it is also important that you avoid using Hotmail, Yahoo, or any other webmail provider that includes your*IP address* [23] in the messages you send.
- Depending on who might have physical access to your computer, clearing email-related traces from your temporary files might be just as important as protecting your messages as they travel across the Internet. See ***Chapter 6: How to destroy sensitive information*** [33] and the ***CCleaner Guide*** [34] for details.

Tips on responding to suspected email surveillance

If you suspect that someone is already monitoring your email, you may want to create a new account and keep the old one as a decoy. Remember, though, that any account with which you have exchanged email in the past may now be under surveillance as well. As a result, you should observe some additional precautions:

- Both you and your recent email contacts should create new accounts and connect to them only from locations, such as Internet cafes, that you have never used before. We recommend this strategy in order to prevent connections from your usual computer, which may be monitored, from giving away the location of your new account. As an alternative, if you must login to your new account from your normal location, you can use one of the tools described in ***Chapter 8: How to remain anonymous and bypass censorship on the Internet*** [31], to hide these connections.
- Exchange information about these new email addresses only through secure channels, such as a face-to-face meetings, secure instant messages or encrypted *VoIP* [2] conversations.
- Keep the traffic on your old account mostly unchanged, at least for a while. It should appear to the eavesdropper as if you are still using that account for sensitive communication. Presumably, you will want to avoid revealing critical information, but you should try not to make it obvious that you are doing so. As you can imagine, this may be somewhat challenging.
- Make it difficult to link your actual identity to your new account. Do not send email between the new account and your old accounts (or the accounts of any contacts whom you think may also be monitored).
- Be aware of what you write when using your new account. It is best to avoid using real names and addresses or phrases like 'human rights' or 'torture.' Develop an informal code system with your email contacts and change it periodically.
- Remember, email security is not just about having strong technical defences. It is about paying attention to how you and your email contacts communicate with each other, and about remaining disciplined in your non-technical security habits.

Securing other Internet communication tools

Much like email, instant messaging and *VoIP* [2] software can be secure or insecure, depending on the tools you choose and how you use them.

Securing your instant messaging software

Instant messaging, also called 'chat,' is not normally secure, and can be just as vulnerable to surveillance as email. Luckily, there are programs that can help secure the privacy of your chat sessions. Just like with email, though, a secure communications channel requires that both you and your instant messaging contacts use the same software and take the same security precautions.

There is a chat program called *Pidgin* [6] that supports many existing instant messaging protocols, which means that you can easily begin using it without having to change your account name or recreate your list of contacts. In order to have private, *encrypted* [3] conversations through *Pidgin* [6] , you will need to install and activate the *Off-the-Record OTR [5]* plug-in. Fortunately, this is a fairly simple process.

Hands-on: Get started with the Pidgin Guide [35]

Skype [1], which is a common *VoIP* [2] tool, also supports instant messaging. While using *Skype* [1] is probably more secure than using one of the alternatives without the *OTR* [5] plugin, it has two important drawbacks. First, it only allows you to chat with other *Skype* [1] users, whereas *Pidgin* [6] can be used to communicate securely with nearly all other instant messaging services. Second, because it is closed-source, it is impossible to verify the strength of its *encryption* [3]. ***Chapter 1: How to protect your computer from malware and hackers*** [16] addresses the virtues of *Free and Open-Source Software *FOSS* [36] in the ***Keeping your software up-to-date*** [37] section. In short, you are better off using *Pidgin* [6], with the *OTR* [5] plugin, for secure instant messaging.

Pablo: If Yahoo webmail is insecure, does that mean that Yahoo Chat is insecure, too?

Claudia: The thing to remember is that, if we want to use instant messaging to discuss this report, we need to make sure that everyone involved has Pidgin and OTR installed. If they do, we can use Yahoo chat or any other chat service.

Securing your VoIP software

VoIP [2] calls to other *VoIP* [2] users are generally free of charge. Some programs allow you to make inexpensive calls to normal phones as well, including international numbers. Needless to say, these features can be extremely useful. Some of today's more popular *VoIP* [2] programs include Skype [38], Gizmo [39], Google Talk [40] , Yahoo! Voice [41] , and MSN Messenger [42] .

Normally, voice communication over the Internet is no more secure than unprotected email and instant messaging. Only *Skype* [1] and *Gizmo* [43] offer encryption for voice conversations, and then only if you are calling another *VoIP* [2] user, as opposed to a mobile or landline telephone. In addition, because neither application is open-source, independent experts have been unable to test them fully and ensure that they are secure.

Advanced email security

The tools and concepts discussed below are recommended for experienced computer users.

Using public key encryption in email

It is possible to achieve a greater level of email privacy, even with a non-secure email account. In order to do this, you will need to learn about public key *encryption* [3]. This technique allows you to encode individual messages, making them unreadable to anyone but the intended recipients. The ingenious aspect of public key *encryption* [3] is that you don't have to exchange any secret information with your contacts about how you are going to encode messages in the future.

Pablo: But how does all this work?

Claudia: Clever mathematics! You encode messages to a given email contact using her special 'public key,' which she can distribute freely. Then, she uses her secret 'private key,' which she has to guard carefully, in order to read those messages. In turn, your contact uses your public key to encrypt messages that she writes to you. So, in the end, you do have to exchange public keys, but you can share them openly, without having to worry about the fact that anybody who wants your public key can get it.

This technique can be used with any email service, even one that lacks a secure communication channel, because individual messages are *encrypted* [3] before they leave your computer.

Remember that, by using *encryption* [3], you could attract attention to yourself. The type of encryption [3] used when you access a secure website, including a webmail account, is often viewed with less suspicion than the type of public key *encryption* [3] being discussed here. In some circumstances, if an email containing this sort of *encrypted* [3] data is intercepted or posted to a public forum, it could incriminate the person who sent it, regardless of the message'sÂ content. You might sometimes have to choose between the privacy of your message and the need to remain inconspicuous.

Encrypting and authenticating individual messages

Public key *encryption* [3] may seem complicated at first, but it is quite straightforward once you understand the basics, and the tools are not difficult to use. The Mozilla *Thunderbird* [9] email program can be used with an extension called *Enigmail* [8] to encrypt and decrypt email messages quite easily.

Hands-on: Get started with the *Thunderbird Guide* [29]

VaultletSuite 2 Go [44], a freeware encrypted email program, is even easier to use than Thunderbird if you are willing to trust the company that provides it and allow them to do some of the work for you.

Hands-on: Get started with the *VaultletSuite 2Go Guide* [45]

The authenticity of your email is another important aspect of communication security. Anyone with Internet access and the right tools can impersonate you by sending messages from a fake email address that is identical to your own. The danger here is more apparent when considered from the perspective of the recipient. Imagine, for example, the threat posed by an email that appears to be from a trusted contact but is actually from someone whose goal is to disrupt your activities or learn sensitive information about your organisation.

Because we cannot see or hear our correspondents through email, we typically rely on a sender's address to verify her identity, which is why we are so easily fooled by fake emails. *Digital signatures* [46], which also rely on public key *encryption* [3],provide a more secure means of proving one's identity when sending a message. The ***How to use Enigmail with Thunderbird*** [47] section of the ***Thunderbird Guide*** [29] explains in detail how this is done.

Pablo: I had a colleague once who received email from me that I didn't send. We decided, in the end, that it was just spam, but now I'm imagining how much damage could be done if a fake email appeared in the wrong person's inbox at the wrong time. I've heard you can prevent this kind of thing with digital signatures, but what are they?

Claudia: A digital signature is like a wax seal over the flap of an envelope with your letter inside. Except that It can't be forged. It proves that you are the real sender of the message and that it hasn't been tampered with along the way.

Further reading

- To learn more about faking an email identity, refer to the Spoofing [48] section of the Digital Security and Privacy for Human Rights Defenders [49] book.
- In addition to the *Riseup* and *Thunderbird* Hands-on Guides, there are a number of websites that explain how to use your email program with various popular email providers while leaving a copy of your messages on the mail server:
  - The Riseup website [50]
  - Instructions on using Gmail [51] .
  - Instructions on how to import your gmail contacts into Thunderbird [52]
  - For details on how to use other email services in this way, search the help section of the provider's website for keywords like 'POP', 'IMAP' and 'SMTP'.
- There is a well-known attack on the security of SSL encryption known as the Man in the Middle attack [53].
- The Gmail Privacy Policy [54], which you must accept when creating a Gmail account, explains that, "Google maintains and processes your Gmail account and its contents to provide the Gmail service to you and to improve our services." In fact, all email providers scan your messages, to some extent, so that they can offer anti-spam services and other such features. Gmail goes a bit futher, however, in order to provide 'targeted advertising' based on the actual content of your email. This could be dangerous if information stored by Google were to be intentionally or accidentally exposed.
- A series of interviews in 2008 addressed the privacy and encryption policies [55] of several major instant messaging services.

How-To Booklet

Source URL (retrieved on *05/12/2011 - 18:51*): https://security.ngoinabox.org/en/chapter-7

Links:
[1] https://security.ngoinabox.org/glossary#Skype
[2] https://security.ngoinabox.org/glossary#VoIP
[3] https://security.ngoinabox.org/glossary#Encryption
[4] https://security.ngoinabox.org/glossary#RiseUp
[5] https://security.ngoinabox.org/glossary#OTR
[6] https://security.ngoinabox.org/glossary#Pidgin
[7] https://security.ngoinabox.org/glossary#Firefox
[8] https://security.ngoinabox.org/glossary#Enigmail
[9] https://security.ngoinabox.org/glossary#Thunderbird
[10] https://security.ngoinabox.org/glossary#Keylogger
[11] https://security.ngoinabox.org/chapter_7_1#Keeping_your_webmail_private
[12] https://security.ngoinabox.org/chapter_7_1#Switching_to_a_more_secure_email_account
[13] https://security.ngoinabox.org/chapter_7_4
[14] https://security.ngoinabox.org/chapter_7_4#Encrypting_and_authenticating_individual_email_messages
[15] https://security.ngoinabox.org/chapter_7_2
[16] https://security.ngoinabox.org/chapter-1
[17] https://security.ngoinabox.org/chapter-3
[18] https://security.ngoinabox.org/glossary#ISP
[19] https://security.ngoinabox.org/glossary#SSL
[20] https://security.ngoinabox.org/discussion#Encryption

[21] https://security.ngoinabox.org/glossary#Security_certificate
[22] https://security.ngoinabox.org/firefox_main
[23] https://security.ngoinabox.org/glossary#IP_address
[24] https://mail.google.com
[25] http://mail.google.com
[26] https://security.ngoinabox.org/chapter_7_5
[27] https://mail.riseup.net
[28] https://security.ngoinabox.org/riseup_main
[29] https://security.ngoinabox.org/thunderbird_main
[30] https://security.ngoinabox.org/glossary#Tor
[31] https://security.ngoinabox.org/chapter-8
[32] https://security.ngoinabox.org/glossary#Circumvention
[33] https://security.ngoinabox.org/chapter-6
[34] https://security.ngoinabox.org/ccleaner_main
[35] https://security.ngoinabox.org/en/pidgin_main
[36] https://security.ngoinabox.org/glossary#FOSS
[37] https://security.ngoinabox.org/chapter_1_4
[38] http://www.skype.com
[39] http://www.gizmoproject.com/
[40] http://www.google.com/talk
[41] http://voice.yahoo.com/
[42] http://get.live.com/messenger
[43] https://security.ngoinabox.org/glossary#Gizmo
[44] https://security.ngoinabox.org/glossary#VaultletSuite
[45] https://security.ngoinabox.org/vaultletsuite_main
[46] https://security.ngoinabox.org/glossary#Digital_signature
[47] https://security.ngoinabox.org/thunderbird_usingenigmail
[48] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_5.html#2_5b
[49] http://www.frontlinedefenders.org/manual/en/esecman/
[50] http://help.riseup.net/mail/mail-clients/
[51] http://mail.google.com/support/bin/topic.py?topic=12805
[52] http://email.about.com/od/mozillathunderbirdtips/qt/et_gmail_addr.htm
[53] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_7.html#2_7c
[54] http://mail.google.com/mail/help/intl/en/privacy.html
[55] http://news.cnet.com/8301-13578_3-9962106-38.html