# Keeping your webmail private ? HTTPS

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.

## Keeping your webmail private ? HTTPS

HTTPS, (also referred to as SSL or TLS), encrypts your communications so that it cannot be read by other people on your network. This can include the other people using the same Wi-Fi in an airport or at a café, the other people at your office or school, the administrators at your ISP, malicious hackers, governments, or law enforcement officials. Communications sent over your web browser, including the web pages that you visit and the content of your emails, using HTTP rather than HTTPS are very easy for an attacker to intercept and read.

Most email providers give you a way of accessing your email using a web browser, such as Firefox or Chrome. Of these providers, most of them provide support for HTTPS. You should always make sure that your connection is secure before logging in, reading your email, or sending a message. You can tell that your email provider supports HTTPS if you log in to your webmail and the URL at the top of your browser begins with the letters HTTPS instead of HTTP (for example: https://mail.google.com).

If your email provider supports HTTPS, but does not do so by default, try replacing HTTP with HTTPS in the URL and refresh the page. If you?d like to make sure that you are always using HTTPS on sites where it is available, download the [HTTPS Everywhere](https://www.eff.org/https-everywhere) browser add-on for Firefox or Chrome.

Webmail providers that use HTTPS by default include Gmail, RiseUp and Yahoo.

Some webmail providers give you the option of choosing to use HTTPS by default by selecting it in your settings, such as Hotmail.

HTTPS is the most basic level of encryption for your web browsing that we recommend for everybody. It is as basic as putting on your seat belt when you drive.

# Switching to a more secure email account

While using HTTPS protects your communications from other people on your network, there are some things that it does not do. When you send email using HTTPS, your email provider still gets an unencrypted copy of your communication. Governments and law enforcement may be able to access this data with a warrant.

Yahoo and Hotmail, for instance, provide a secure connection only while you log in, to protect your password, but your messages themselves are sent and received insecurely. They also insert the IP address of the computer you are using into all of the messages you send. We do not recommend that you use them for secure communications.

## Gmail

Gmail accounts, on the other hand, use a secure connection during log-in and all the way until you log out and, unlike Yahoo or Hotmail, Gmail avoids revealing your IP address to email recipients. One way to make Gmail (or Yahoo) even more secure is to turn on 2-step-verification. This is one of the safest and simplest computer-security measures. To break into an account with 2-Step Verification, intruders would not only have to know your username and password, they'd also have to get a hold of your phone, or codes you hold with you. Setting it up is simple: [see here](https://support.google.com/accounts/answer/185839?hl=en).

However, it is not recommend that you rely on Google for the total 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.

## RiseUp

If possible, you should create a new RiseUp email account by visiting <https://mail.riseup.net>. RiseUp offers free email to activists around the world and takes great care to protect the information stored on their servers. 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 account, however, you may need two 'invite codes.' These codes can be given out by anyone who already has a RiseUp account. Otherwise, you will need to tell RiseUp about yourself and they may give you access.

# Recipient security

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 messages 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 is one good choice.

# Tips on improving your email security

* Always be careful 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. See more about this in the [Malware](umbrella://lesson/malware) lesson.
* Using anonymity software like Tor, which is described in the [Internet](umbrella://lesson/the-internet) lesson, can help you hide your chosen email service from anyone who might be monitoring your Internet connection.
* 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 to avoid using Hotmail, Yahoo, or any other webmail provider that includes your IP address in the messages you send.
* You may consider using several different, anonymous email accounts for communicating with different groups of people to protect of your contact network. You may also use different email accounts for signing up to Internet services which require email accounts.
* After all above precautions it is still very important to beware of what you write in the messages and what impact would it have if it fell into the wrong hands. One way of increasing the security of information exchange is to develop a code system for sensitive information exchange, so you would not use real names of the people, real addresses of places, etc.
* Remember 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. The [Malware](umbrella://lesson/malware) lesson and offers some advice on how to prevent this sort of thing, and the [Passwords](umbrella://lesson/passwords) lesson will help you protect your accounts.

# Email on Smartphones

In the first instance, consider if you really need to use your smartphone to access your email. Securing a computer and its content is generally simpler than doing so for a mobile device such as a smartphone. A smartphone is more susceptible to theft, monitoring and intrusion.

* If it is absolutely vital that you access your email on your smartphone, there are actions you can take to minimize the risks.
* Do not rely on smartphone as your primary means for accessing your email. Downloading (and removing) emails from an email server and storing them only on your smartphone is not advised. You can set up your email application to use only copies of emails.
* If you use email encryption with some of your contacts, consider installing it on your smartphone, too. The additional benefit is that encrypted emails will remain secret if the phone falls into wrong hands. See the Advanced section of this lesson for details on how to do so.

# Signs your email has been hacked

## Signs

If you suspect your email account has been hacked or compromised, you can take steps to reduce the damage done. While it is difficult to be certain, there may be clues such as:

* You notice any changes to your email account content or settings that you didn't make;
* Your email contacts notify you that they have received an email that you didn't send;
  + You are regularly not receiving some email messages from your colleagues that they insist that they sent to you;
* Some private information that was sent or received exclusively by email was made known to a third party, though neither you nor your correspondent shared it with anyone else;
* If on your account activity log (if your email provider offers one) you see that your account was accessed at time that you do not remember or from a place (or IP address) that you did not go to.

# What to do if your email is hacked

In such situations you may want to take some cautionary action:

* **Stop using this email account for sensitive information exchange**, at least until you understand the situation better.
* **Change your password** for this and all other accounts with a similar password as soon as possible.
* **Change your security question answers** (if you use them) for all accounts, so they are impossible to guess, or find the answer through researching information about you.
* **If you are not able to log in** to your account to change the passwords, consider getting in contact with your email provider to try to reclaim your account.
* **Mitigate information loss and impact** to your community. Determine what kinds of sensitive information and contacts you had in your account and decide whom you should alert. Determine what services (web, financial, etc.) you need to revisit or cancel. It is important that you **check the folders of your account** to research on what could have been sent from your account and to act accordingly.
* **Review your account settings** to see possible changes that has been made. Check accounts signature option for links and malware, forwarding options that would allow to copy emails that you receive to third account, away message, display name, etc.
* **Research how your account was compromised.** Was it because of having a weak password, or due to malware infection, etc. The more you will establish about this, the better you will be able to respond to the situation and better you will be able to protect your contacts.
* **Review security of all of your devices** that access emails from this account, and devices on which you stored the password to this email account. Scan your computer: learn how in the [Malware](umbrella://lesson/malware) lesson. Consider switching to more secure programs like Firefox, Thunderbird, LibreOffice and other Free and Open Source Programs. After making the above improvements to the security of your devices, change your account passwords again to new, stronger ones.
* **Consider reporting hacking** of your account to your email provider.
* **Consider using a more secure account**, e.g. one that notifies you of and prevent access from unusual places or devices. Consider using account that is hosted outside of your country. Consider using email encryption, such as PGP, outlines in the Advanced section of this lesson.
* **Consider avoiding storing read emails.**

It is important that you act quickly and precisely in the situation like this. Having a prepared and rehearsed plan may help you.

Swipe right for this lesson's checklist

Go to the Advanced lesson for advice on how to send encrypted emails for sensitive information.

[Go to Advanced Lesson](umbrella://lesson/email/1)

### RELATED LESSONS/TOOLS

* [Malware lesson](umbrella://lesson/protecting-files)
* [Internet lesson](umbrella://lesson/the-internet)
* [Passwords lesson](umbrella://lesson/passwords)

### FURTHER READING

* [Security in a Box - Secure communication guide](https://securityinabox.org/en/guide/secure-communication)