Institute for Development
of Freedom of Information

HOW TO USE E-MAIL SAFELY

Contact Information:
#3 A. Griboedov Street,
Georgia, 0180, Tbilisi
Tel: + 995 32 2 92 15 14
Email: info@idfi.ge
Website: www.idfi.ge

2018

Content

INTRODUCTION

E-mail has become an integral part of modern life. Neither professional nor civic activity is possible without it. This is also the reason why email is often used for carrying out cyberattacks that range from relatively harmless spam to more serious crimes, e.g. hacking of e-mails, stealing financial information or extortion.

Even though it is impossible to completely negate the risk of cybercrime, there are ways to minimize it; ways offered by e-mail service companies themselves:

1. USE STRONG PASSWORDS

A password enables you to protect your e-mail account from attacks and unauthorized access. It is preferable for your e-mail password to contain 16 characters.

Trick: Come up with a simple sentence, and make it more difficult with various symbols (e.g. thebestpasswordintheworld - tHebest,p@ssw0rdintHewOrd)

✓ Change passwords regularly (e.g. once every three months).

✗ Do not use your personal data (name of your child or address…) as a password.

✗ Do not share your password with others.

✗ Avoid using passwords on public access computers or places where security cameras are installed.

✗ Do not use the same password for various accounts and websites.

Additional Support

In order to make sure that your password is safe, you do not have to create it yourself. It is better if you use online services, which generate passwords that are difficult to crack on your device. One such generator is Identity Safe, which creates passwords randomly, with a variety of symbols and difficulty of your choice.

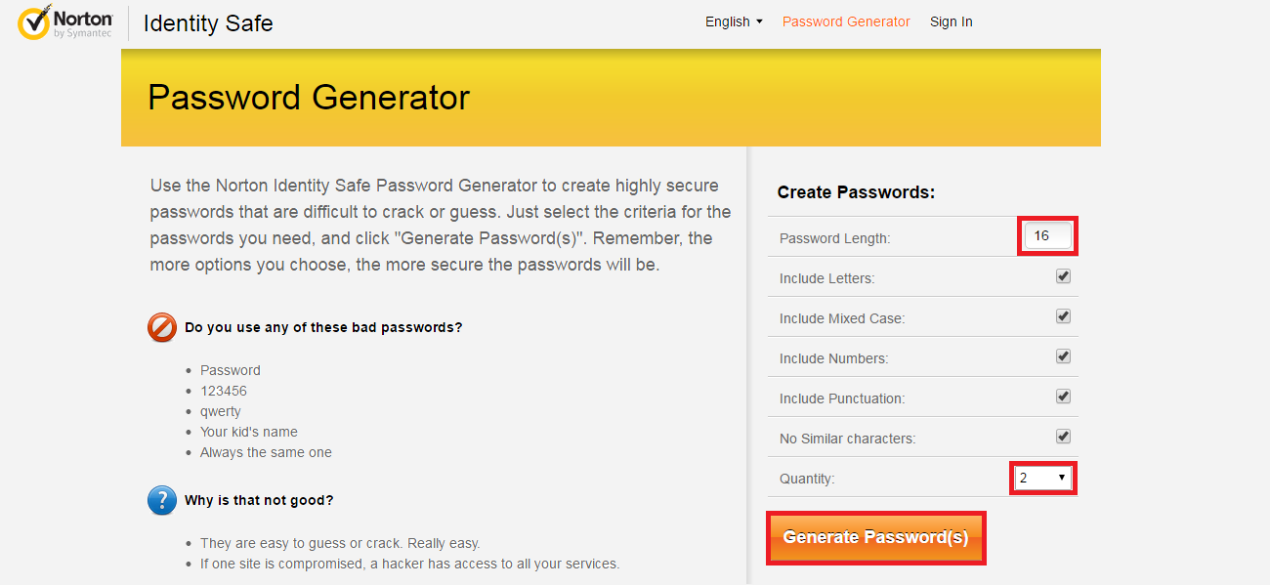


Image 1: *How to use Identity Safe: choose the number of symbols that you want in your password and how many passwords you want to generate. Then click "Generate Password(s)"*

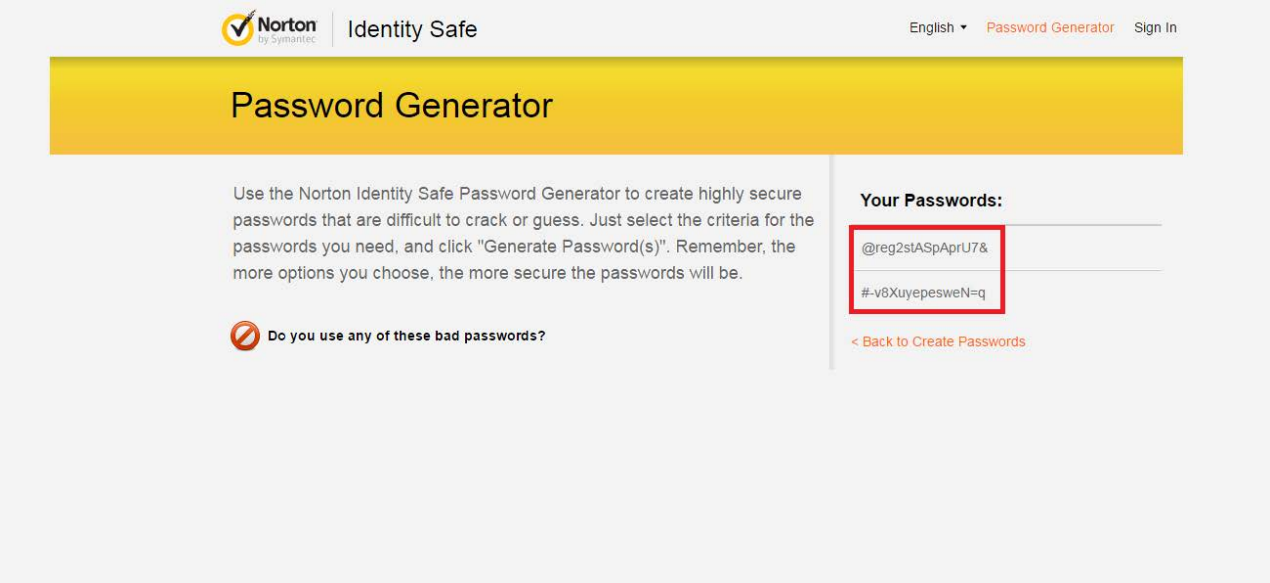


Image 2: *Generated passwords will be shown in the upper right corner*

Password Manager Applications

Password manager applications, such as LastPass or KeepPass, can be used to save complex and large number of passwords. These applications also have a function to generate complex passwords. Install the application on your electronic device and collect all passwords created for various websites.

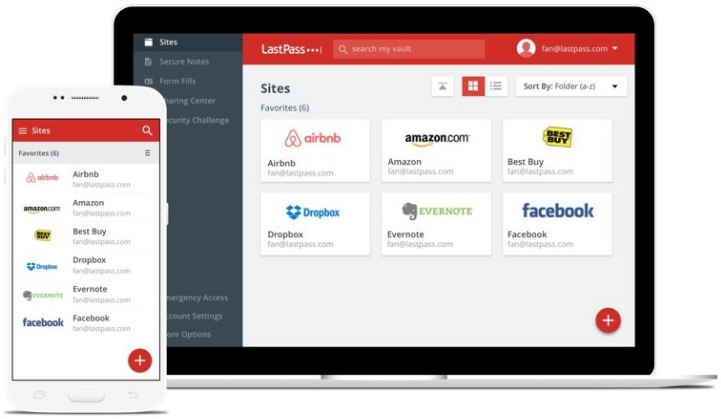


Image 3: *In order to save complex passwords you can use the application LastPass - www.lastpass.com*

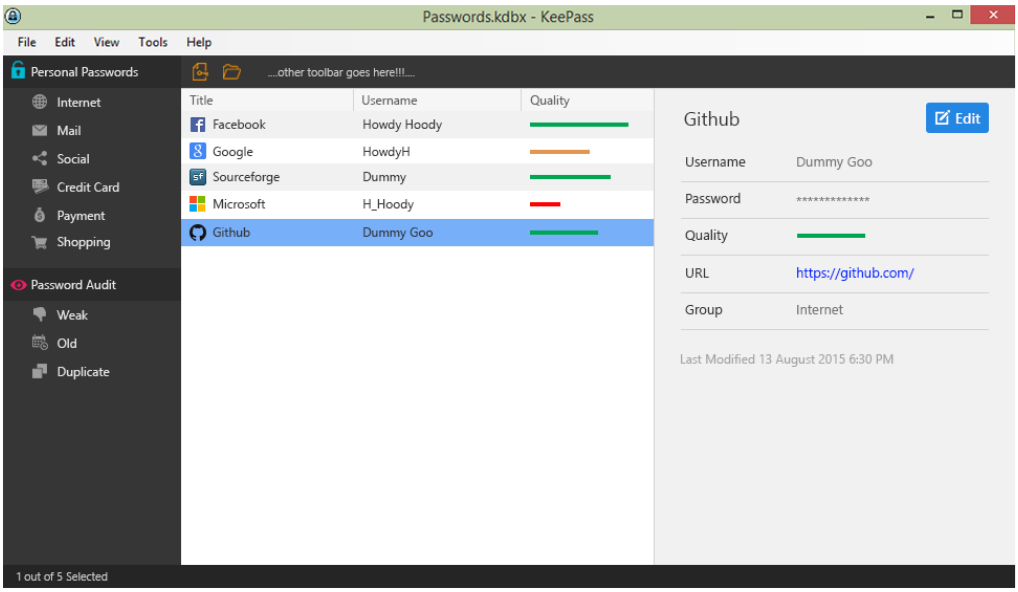


Image 4: *In order to save complex passwords you can use the application KeepPass - www.keepass.info*

Change passwords regularly. For additional security, do not enter your passwords in public spaces, and in places where cameras are installed. Also, do not use the same password for different applications or websites.

2. ONLY USE SECURE WEBSITE ADDRESSES (URL)

While using e-mail, check to what extent it is secure to open your account. To this end, check whether the website address contains „https://" (where "s" stands for "Secure").

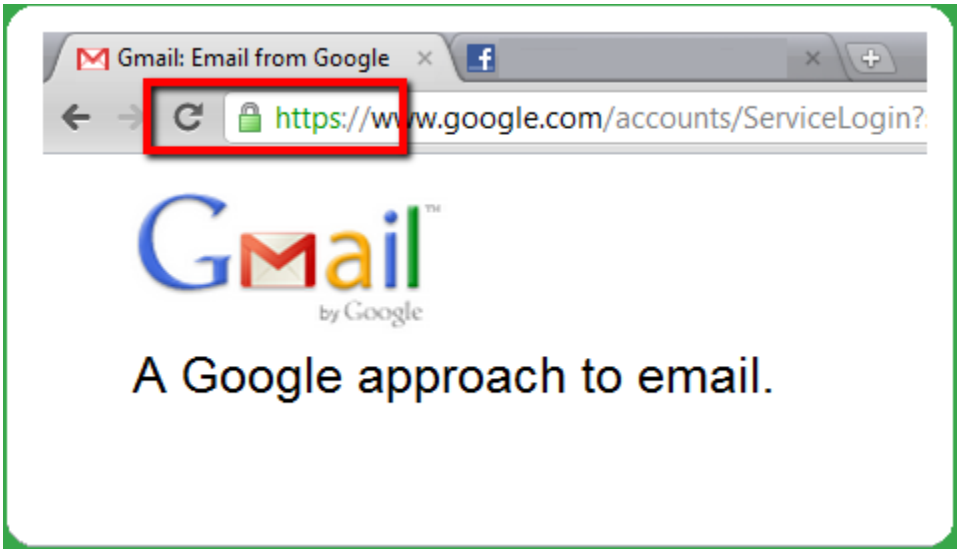


***Image # 5**: An example of a secure website address, which starts with „https://*

3. DO NOT OPEN SUSPICIOUS LINKS

Messages often contain links (URL), which lead to websites containing malicious code. Even clicking a link can infect your computer. Always be cautious about any links in the message. Never click on links found in messages received from unknown or suspicious addresses.

***Image #6:** An example of a suspicious link in a received email.*

4. DO NOT OPEN FILES ATTACHED TO E-MAILS RECEIVED FROM UNKOWN ADDRESSES

Suspicious messages often contain attachments with infected code. Such malicious code can be hidden in any type of file, including PDF and ZIP files.

Never open attached files, received from unknown or suspicious addresses.

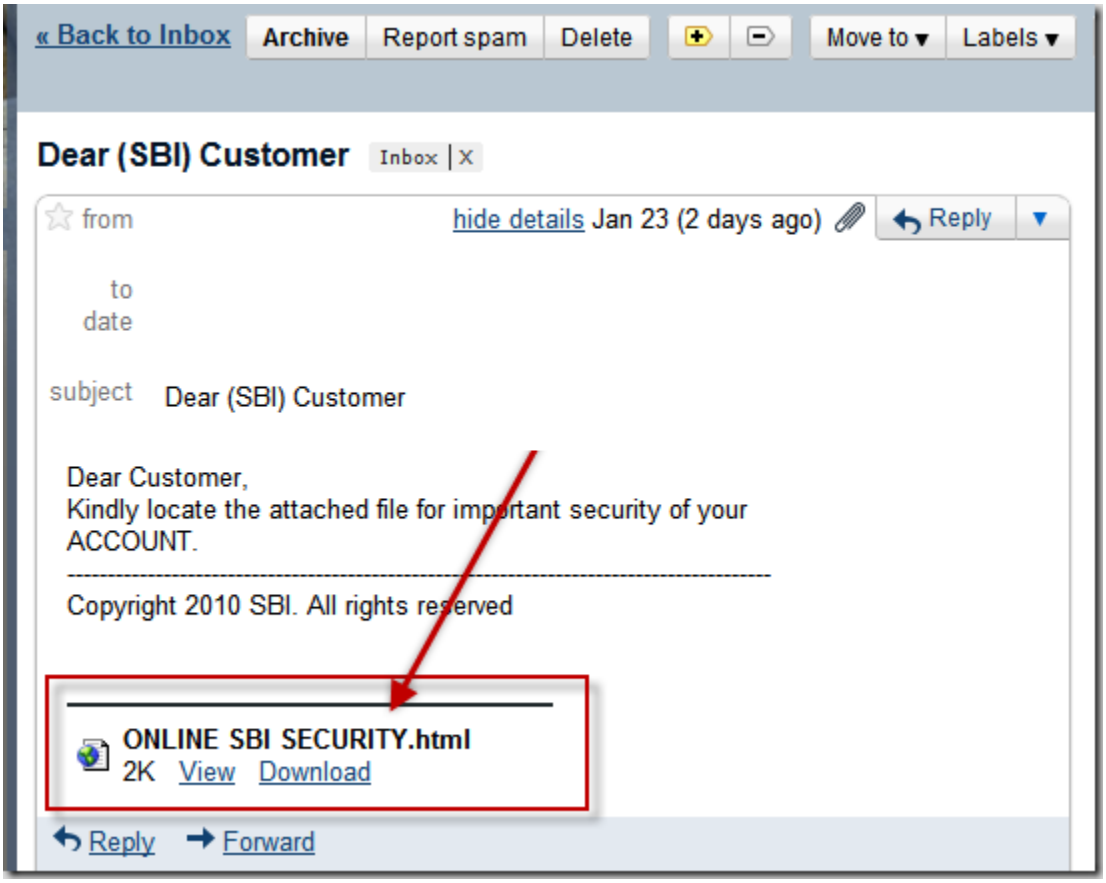


Image #7: *An example of a suspicious document attached to the e-mail received from an unknown address.*

5. TURN OFF AUTO-DOWNLOAD ATTACHMENT FUNCTION

Auto-download of attachments is risky. Downloading of attachments may come with malicious code, or may notify untrustworthy senders that your account is active.

To ensure better protection, it is recommended to block all types of dynamic attachments and activate the option to display all e-mail messages in plain text format. The following images show how to change your browser settings to avoid auto-download of attachments in your computer.

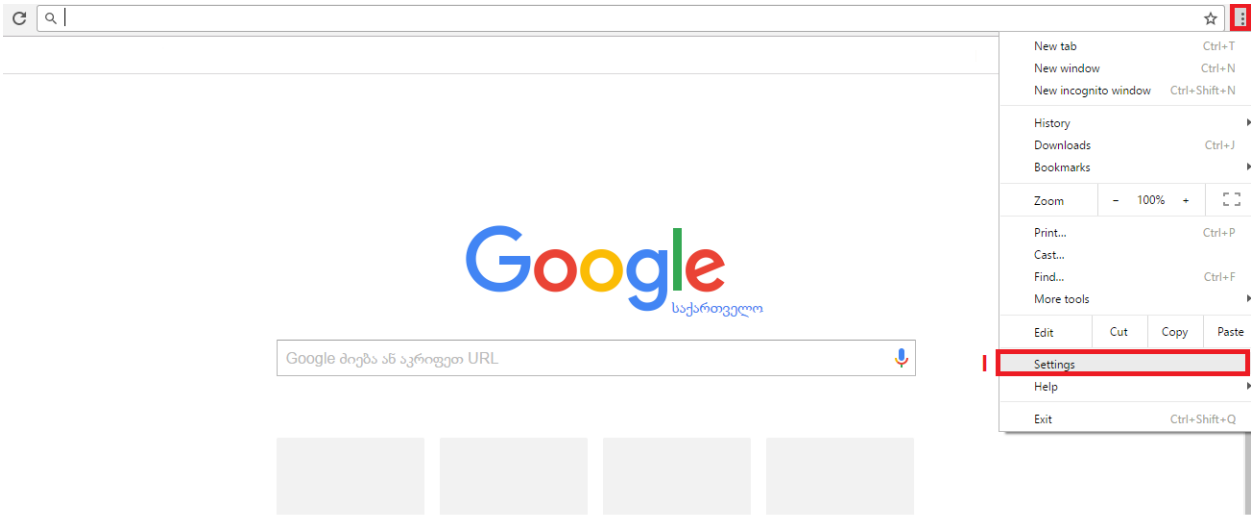


Image #8: *Automatic download of attachments in your e-mails can be turned off through browser settings. (In case of Chrome) Select "Settings" with the button in the right corner of the browser*

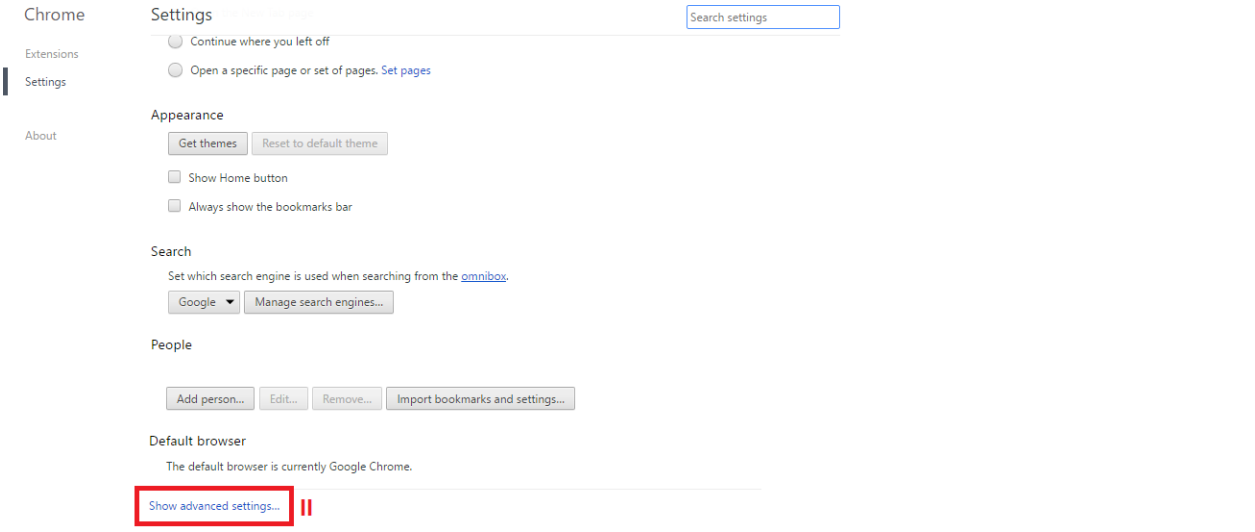


Image # 9: *Select "Show Advanced Settings"*

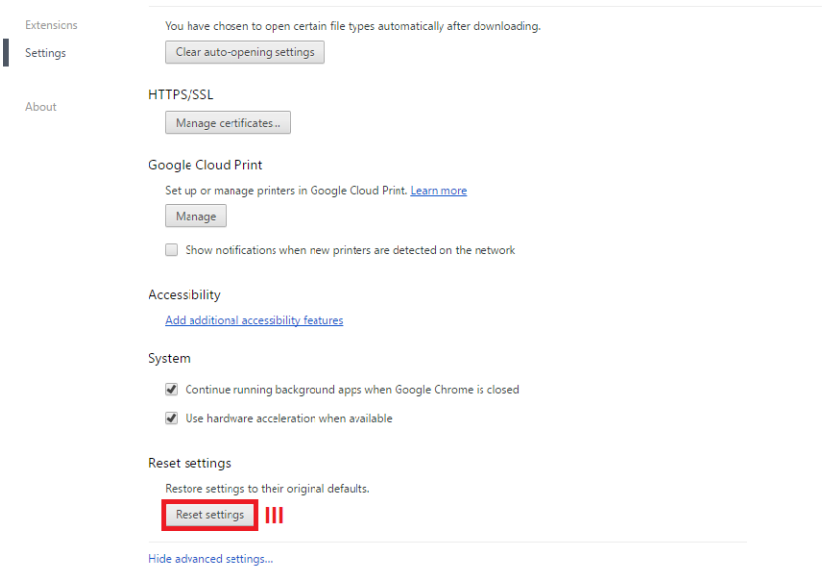


Image #10: *Select "Reset settings"*

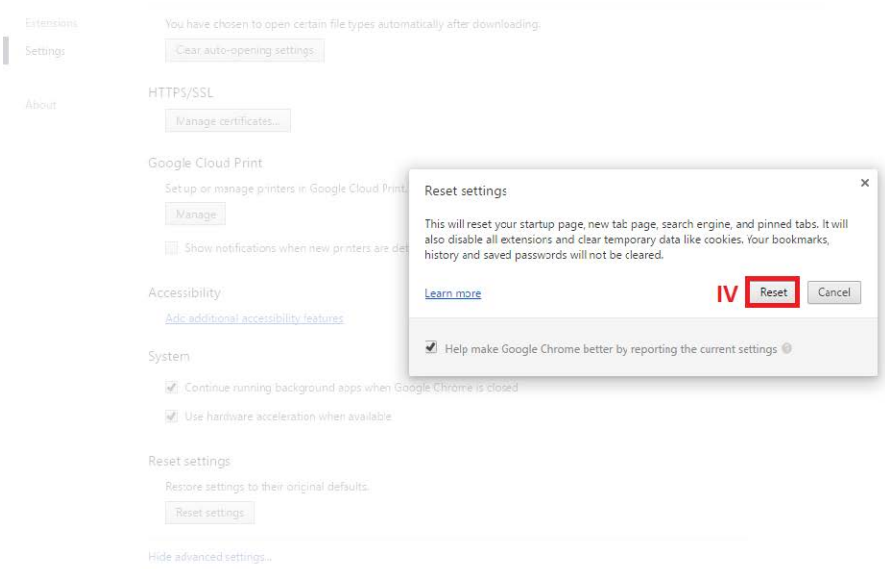


Image #11: *Click on "Reset"*

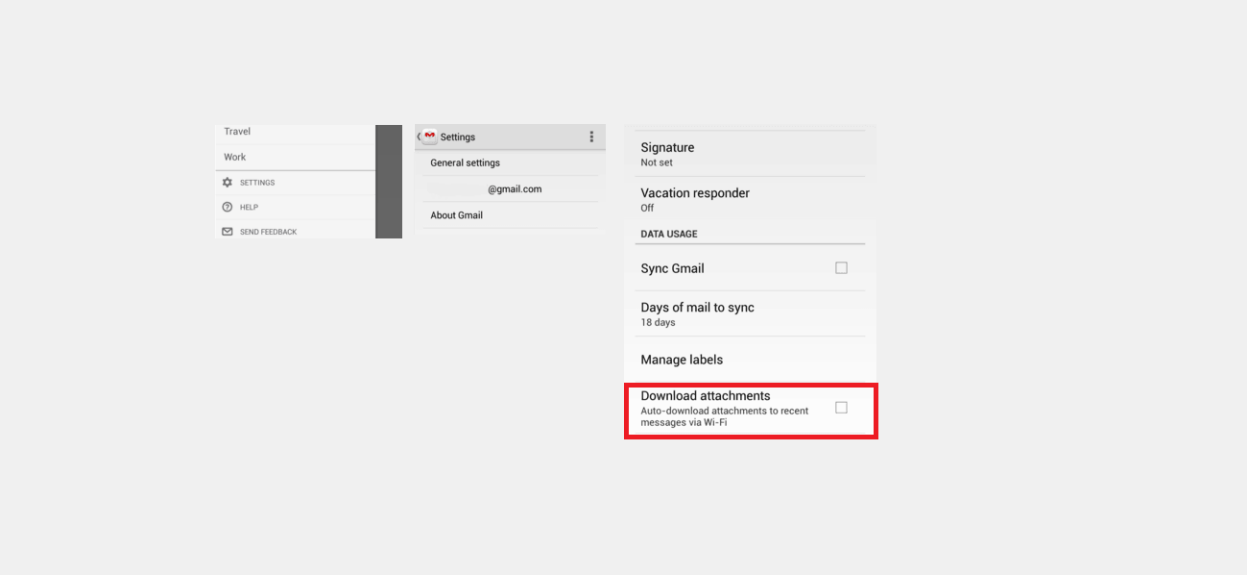


Image #12: *In case of Gmail application on Android, visit application settings and make sure that "Download attachments" function is not selected/activated*

6. TWO-FACTOR VERIFICATION

Two-factor verification adds another step to sign in to your e-mail, e.g. code that you receive on your phone. This code is generated anew every time, deterring unknown people from signing in to your account.

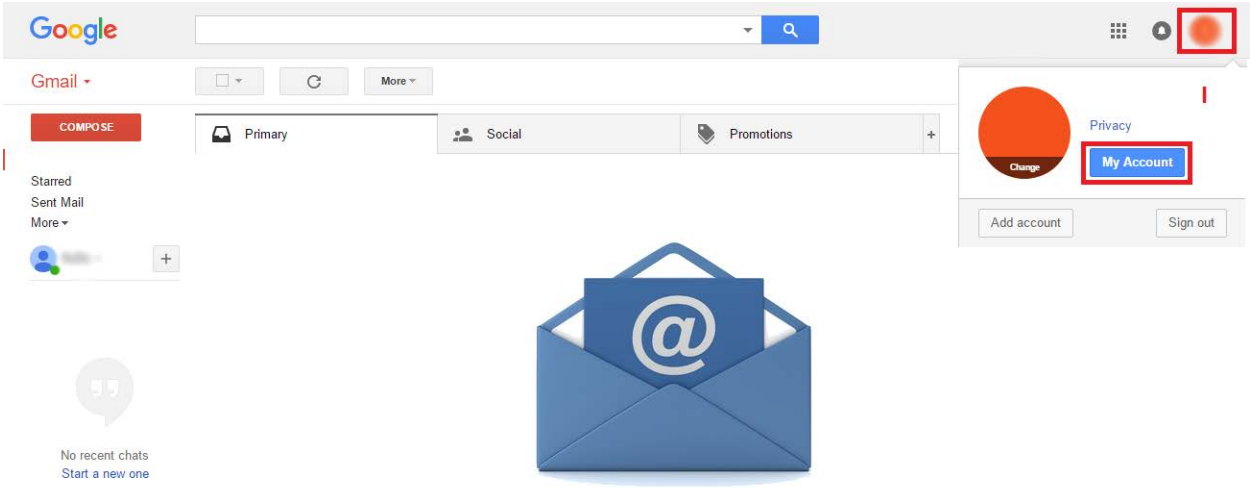


Image: #13: *Log into your e-mail account and select "My Account" in the upper right corner of the panel.*

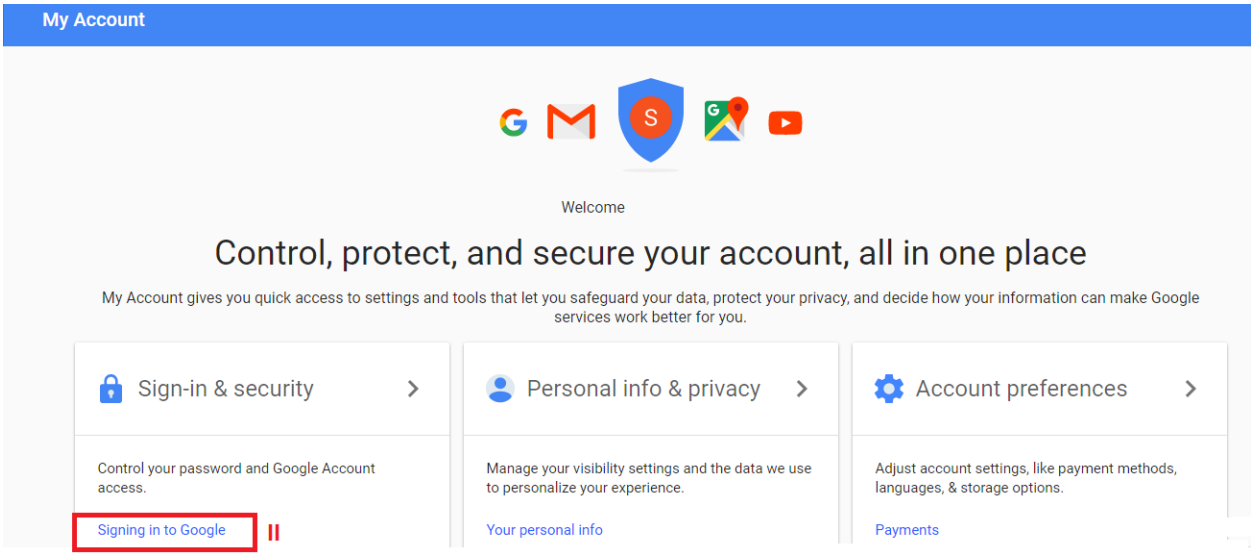


Image #14: *Select "Signing in to Google"*

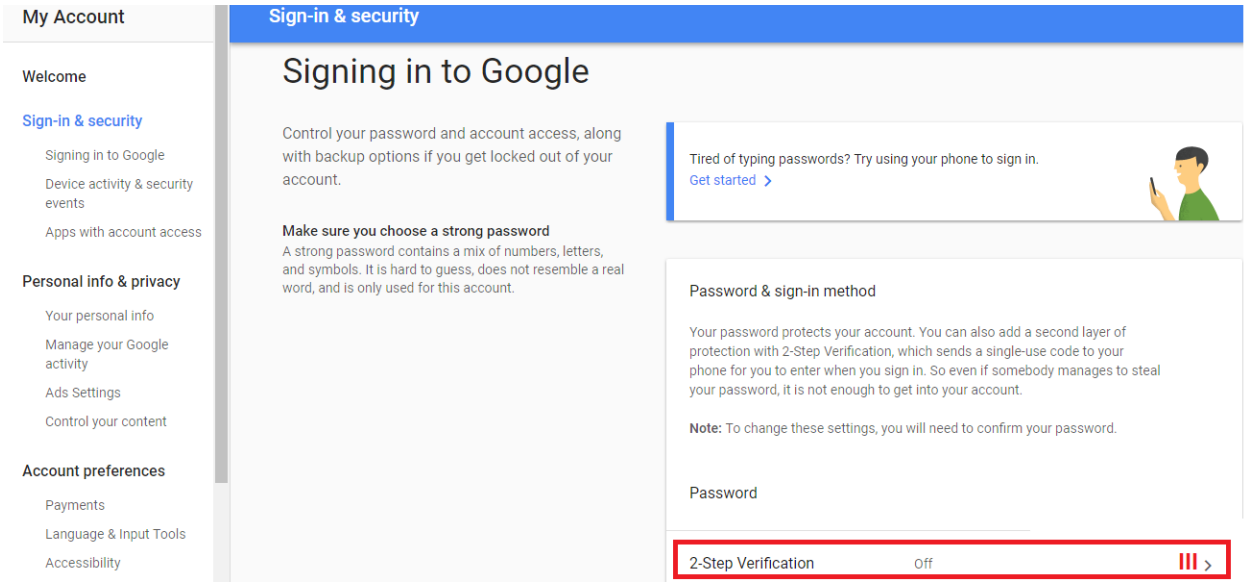


Image #15: *Clock on "2-Step Verification"*

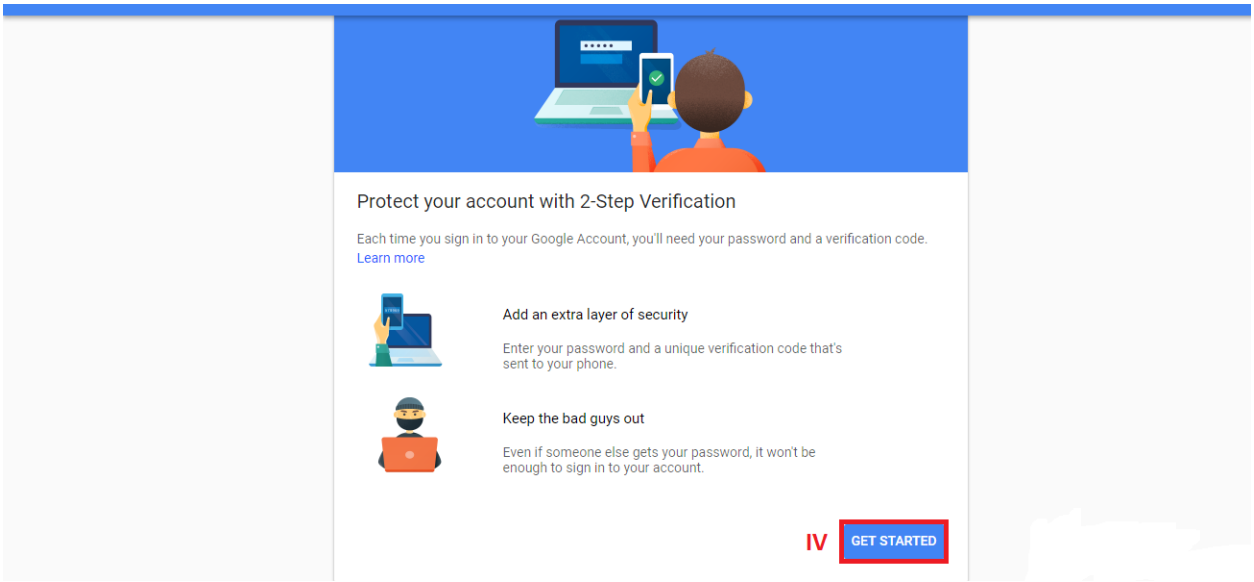
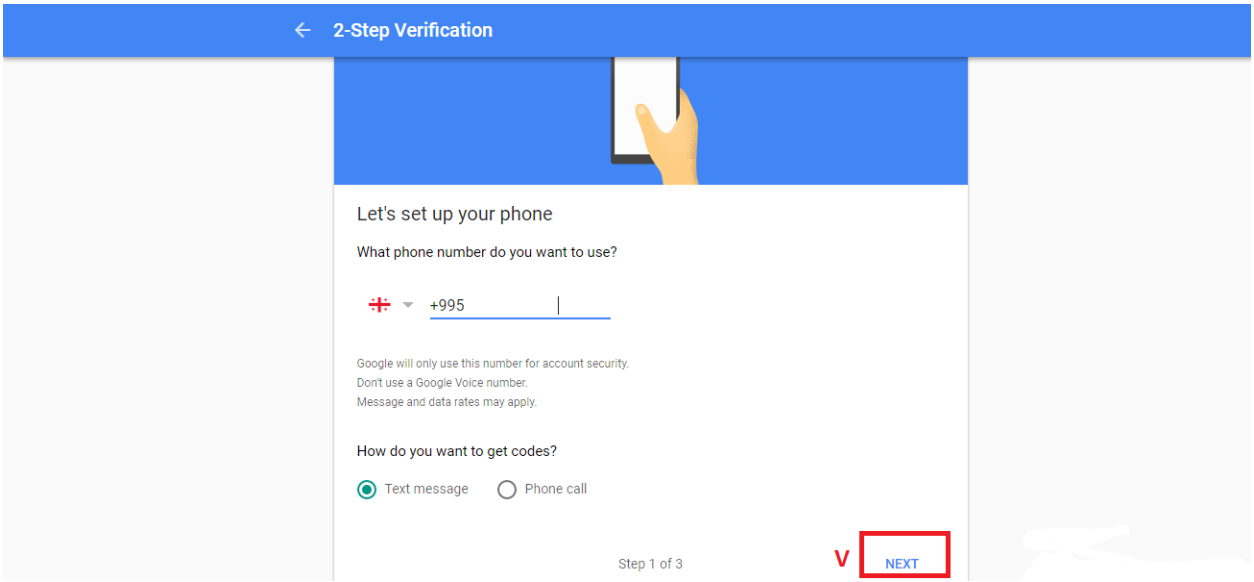


Image #16: *Clock on "Get Started"*



Image#17: *Enter your telephone number where you want to receive SMS code. You can also indicate how you want to receive the code, as a text massage or a phone call. Then select "Next". You will get a code, which you must confirm before activating the function.*

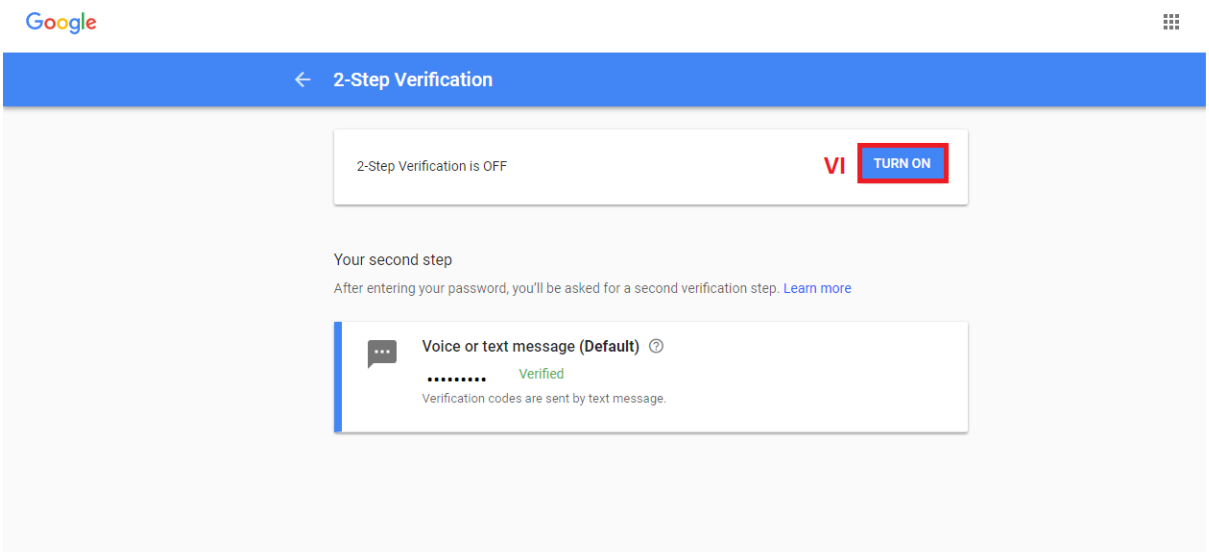


Image #18: *Activate the function by clocking on the following button.*

7. TURN OFF "PREVIEW PANE" OR "READING PANE"

Many e-mail services have a message Preview Pane, also known as the Reading Pane. It shows the content of received messages, which is the same as opening messages. Hence, your computer may be infected with malicious code.

By disabling the function of Preview Pane, you will avoid opening potentially virus-infected messages. Below you can see how to turn off Preview Pane on Outlook.

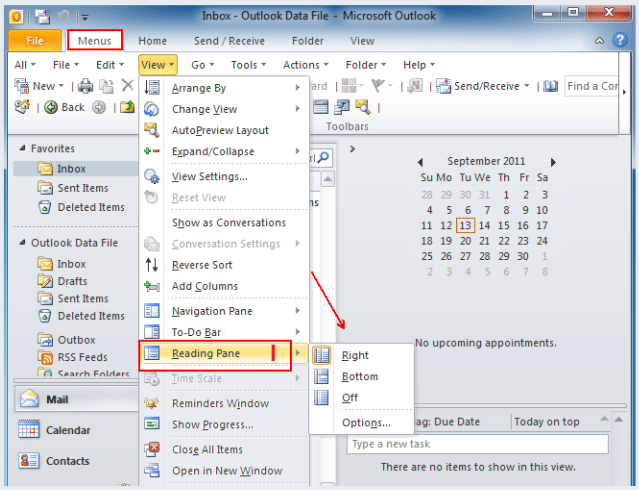


***Image #19**: Click on "View", then select "Reading Pane"*

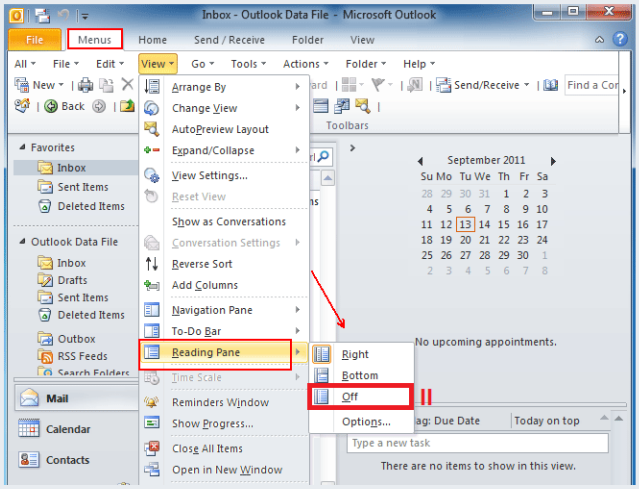


***Image #20:** Select "Off"*

8. DO NOT FORGET TO LOG OUT

After using your e-mail account, do not forget to log out, especially from devices that do not belong to you or the ones you share with others. Otherwise, others will have the opportunity to review your account and the information kept there. Below is a simple instruction on how to log out of Gmail.

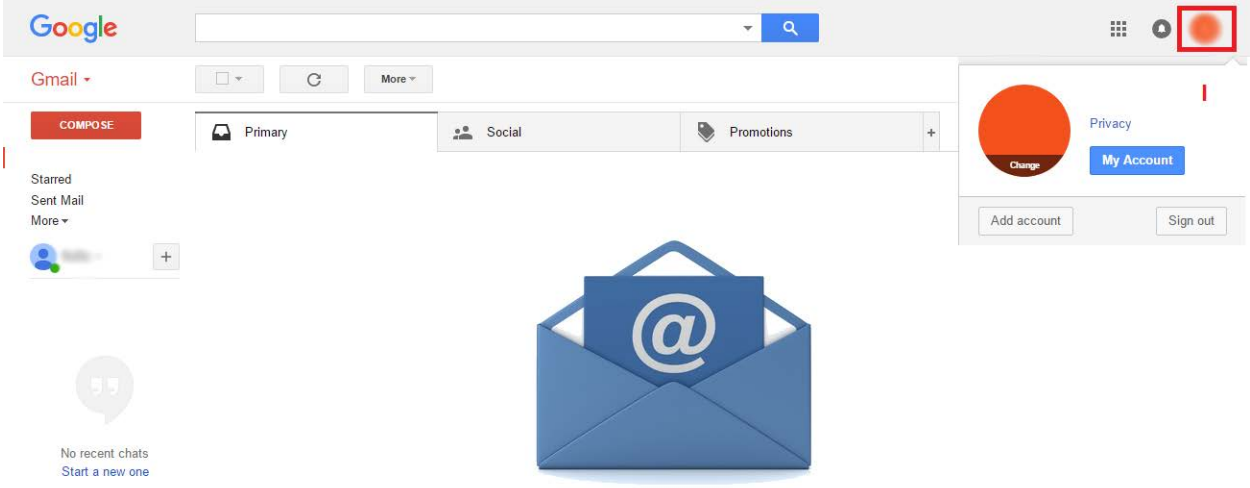


Image #21: *Click on the button in the upper right corner of the panel.*

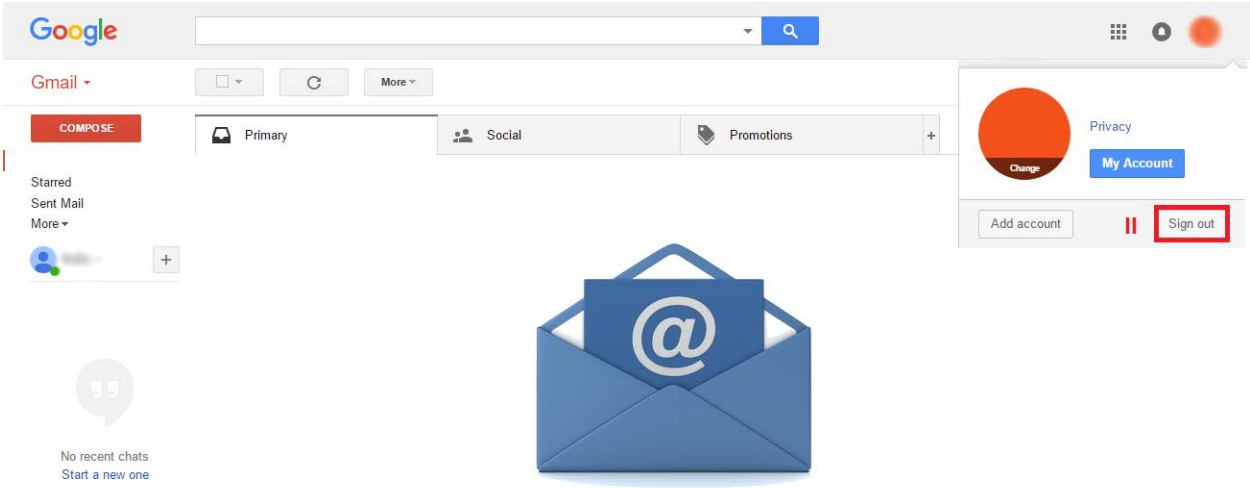


Image #22: *Select "Sign out"*

9. DELETE OR ARCHIVE OLD MESSAGES

If you have been using one particular e-mail account for a long time, it is likely that it contains a large number of important information about you and your organization.

Do not keep messages for years. Delete or archive safely all those messages you do not need.

10. ENCRYPT YOUR E-MAIL

E-mail often becomes a target of phishing (phishing – a type of internet fraud, an attempt to obtain personal information). E-mail encryption is the best way to secure your private communication from phishing.

To encrypt your e-mail use PGP (Pretty Good Privacy) technology. This technology encrypts the message before sending it and only persons with a special password are able to decrypt it. Even if your message is accessed by others, its content will remain secret.

How does PGP work?

With the help of a special program installed on your computer (e.g. MailVelope for Browsers or Enigmail for e-mail) you create open and closed keys for your Inbox, and also choose a strong password to encrypt these e-mails. When you want to send someone an encrypted e-mail, you first exchange the open keys with this person. Afterwards, you enter your Inbox with activated PGP technology:

- Write the text of the message
- Specify the recipient
- Encrypt the text with the installed program (using open keys)
- Send the message

If you are unable to encrypt an important e-mail, you can copy its content into a file, encrypt the file, attach to the e-mail and send it.

In order to decrypt received encrypted e-mail you need to enter the password while opening the Inbox.

Below you can find detailed instructions on how this encryption service (PGP) works on an example of MailVelope, a program, which can be added as an extension to Chrome and Firefox.

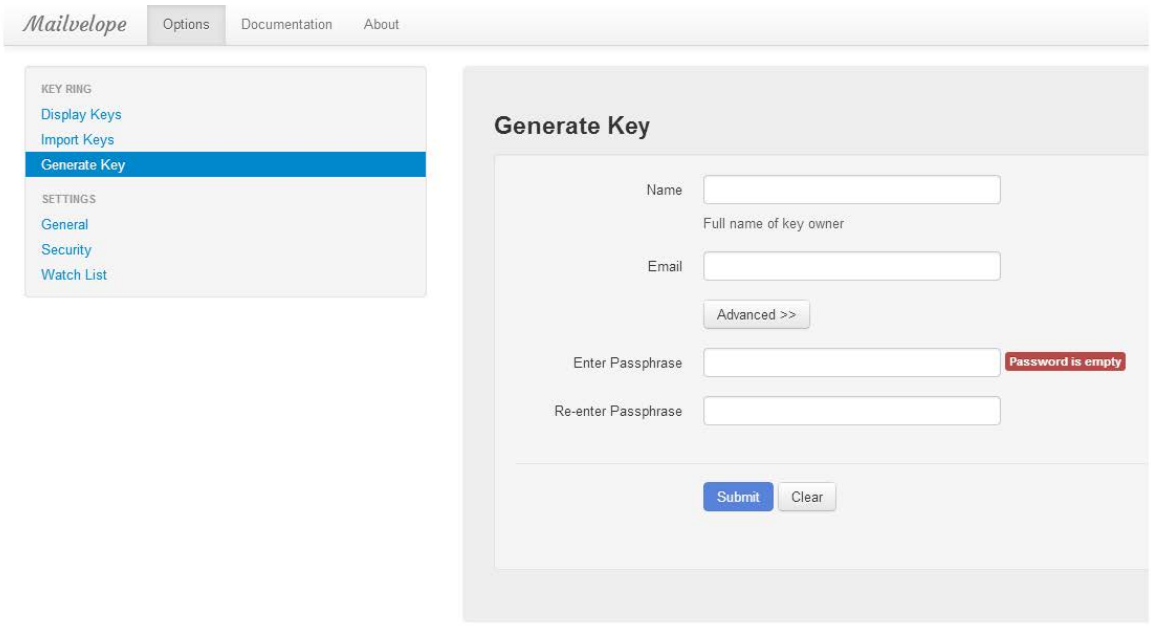


Image #23: *How to use PGP technology, in case of MailVelope: it can be added as an extension to Chrome and Firefox*

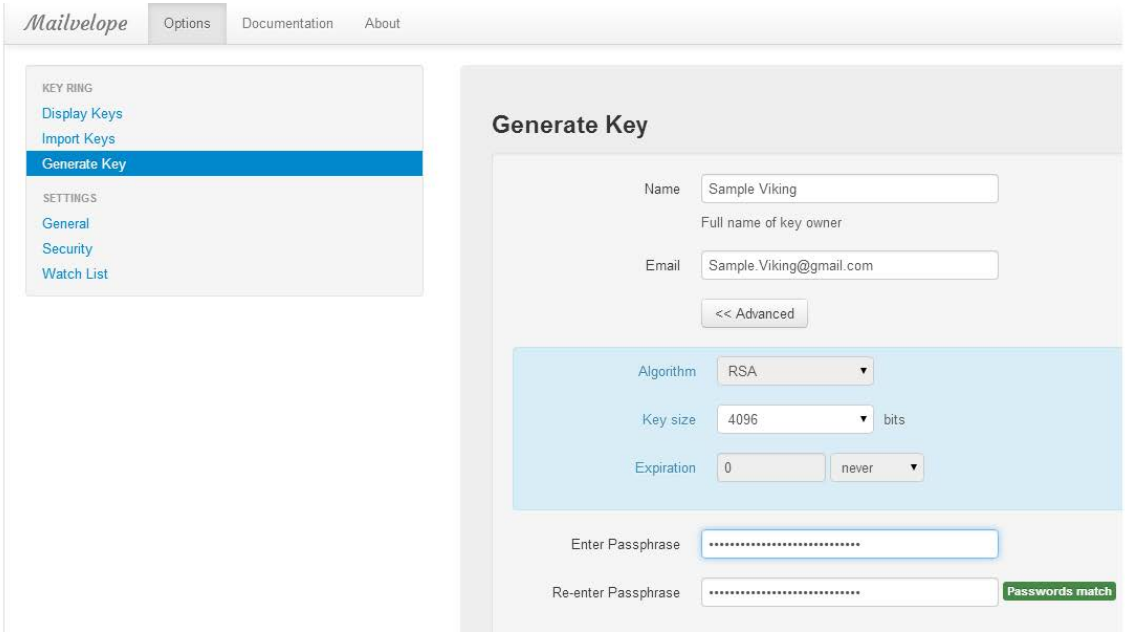


Image 24: *To create new key, click "Generate Key", and enter your data. Also, choose passphrase and encryption algorithm.*

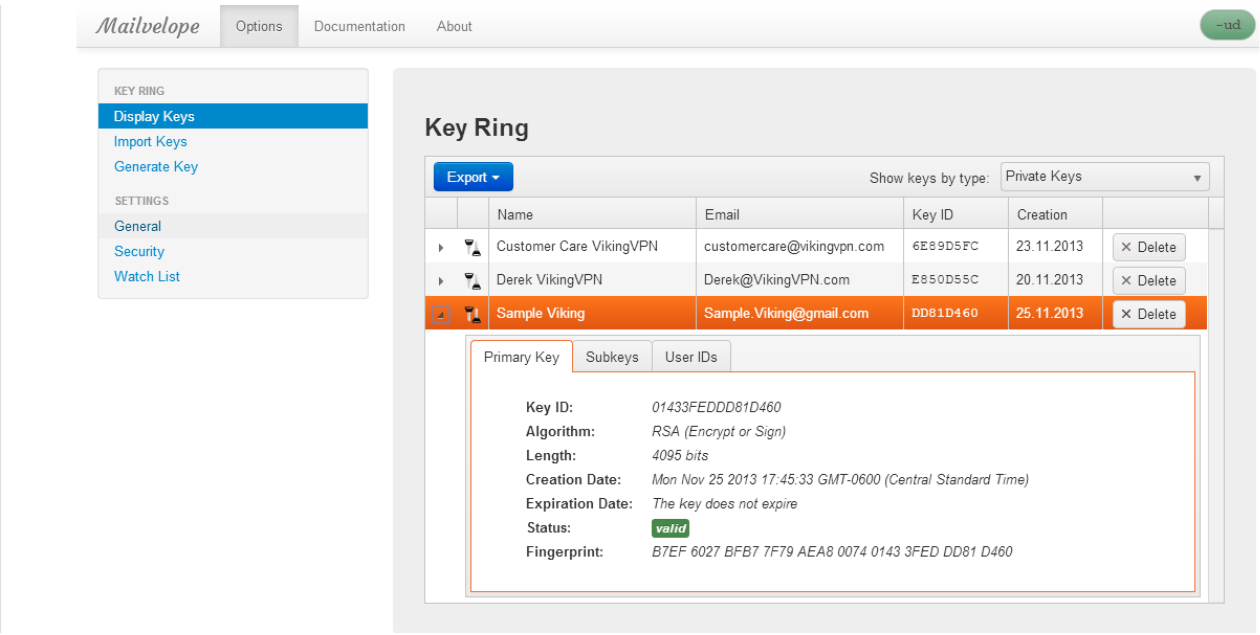


Image #25: *Choose "Display Keys" to view all your keys, date of their creation, expiration dates etc. Choose your newly created key from this list and press "Export". This way you will get a public key, which can be shared with the person from whom you would like to receive encrypted correspondence.*

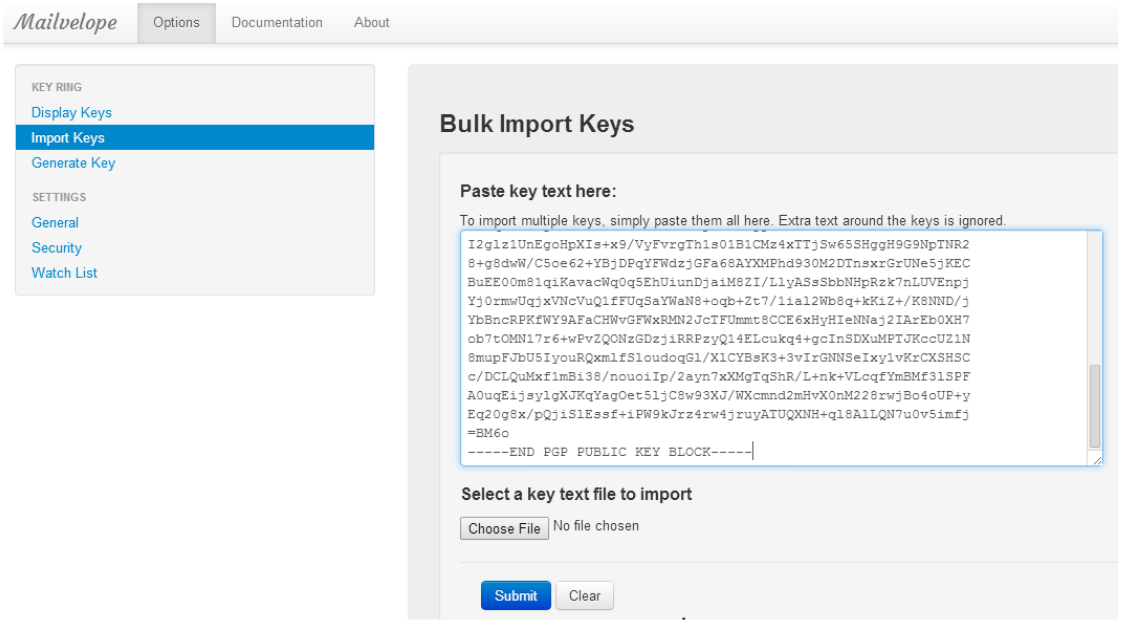


Image #26: *Select "Import Keys" and save the keys, received from the person to whom you would like to send encrypted e-mail.*

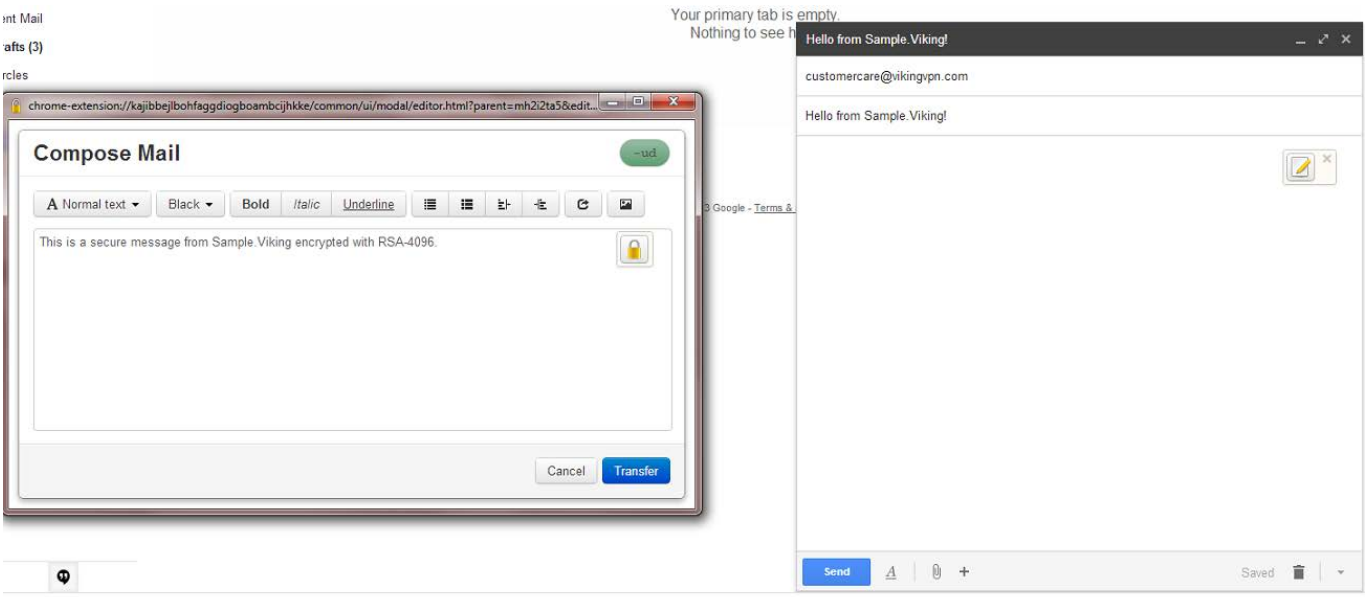


Image #27: *Press the "lock" icon before sending the e-mail*

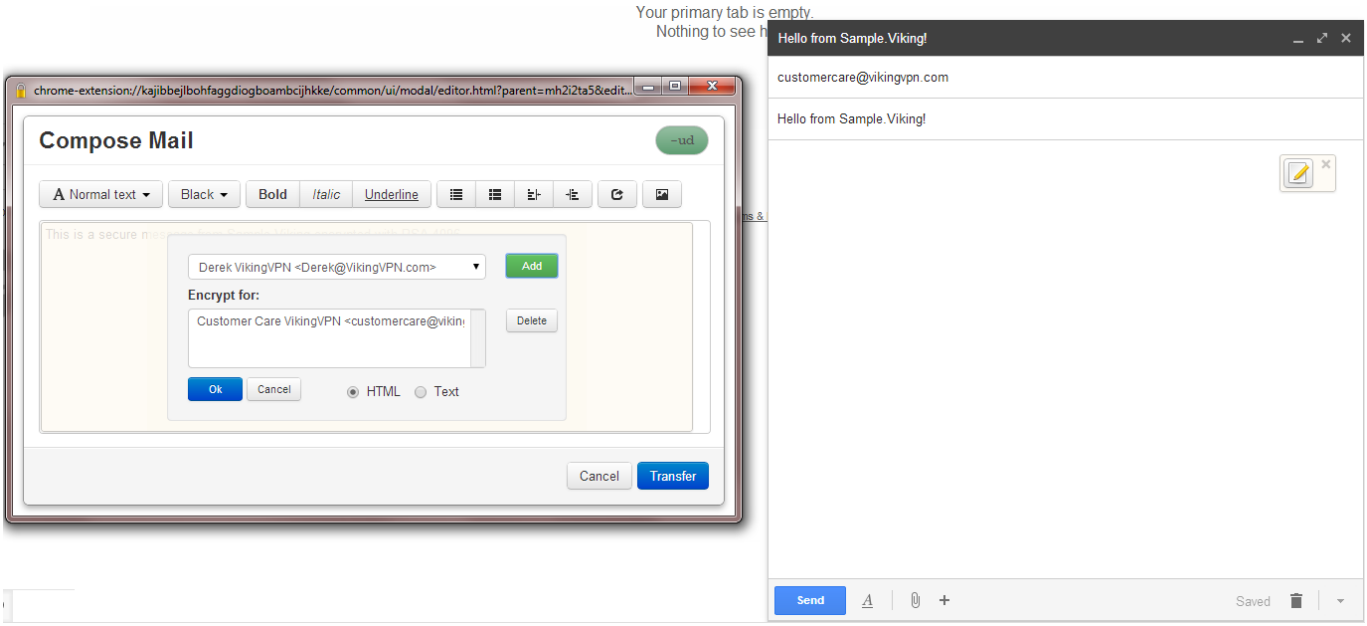


Image #28: *Choose recipient and enter public key. Then press "Transfer"*

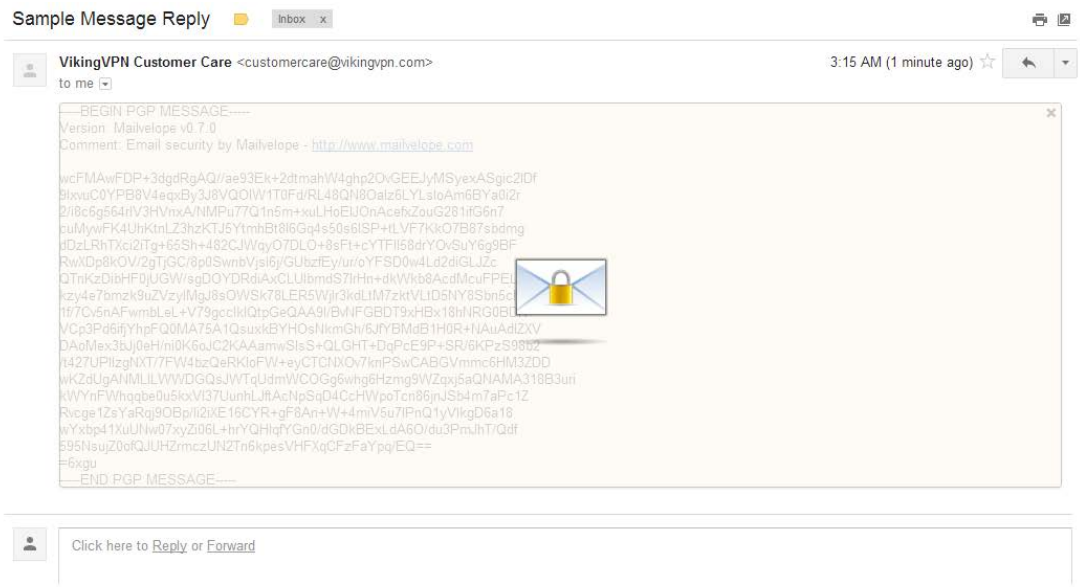


Image #29: *To read the encrypted message you will need to enter the password.*

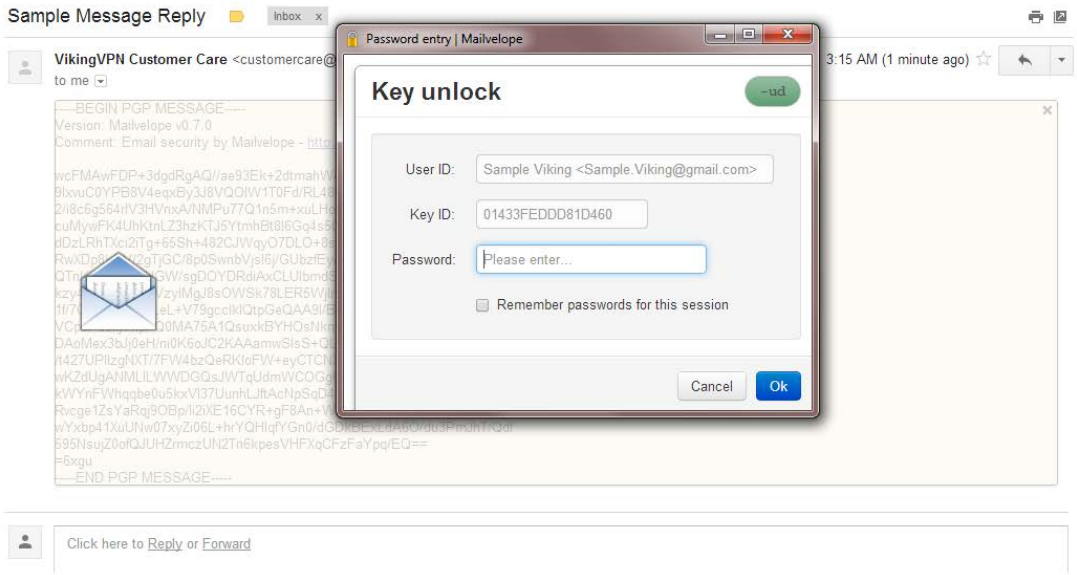


Image #30: *Enter the password.*

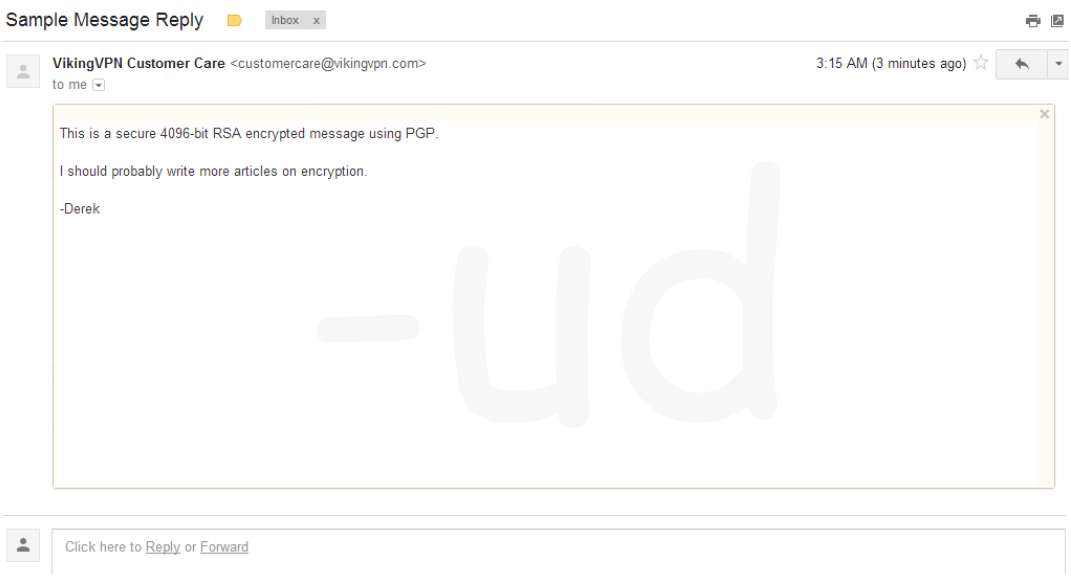


Image #31: *After entering the password, you will be able to read the encrypted message.*

11. USE GOOGLE'S NEW ADVANCED PROTECTION FEATURE

Security Key – Recently, Google has offered its users an advanced protection feature. The function is especially important for those most at risk of targeted attacks — like politicians, activists and journalists. However, any Gmail account owner can activate it as well.

Security Key is similar to Bluetooth and USB keys that you have to carry with you. Nobody will be able to log in to your account without connecting it to a computer. Advanced protection feature also makes it difficult to recover your password and for third-party (non-Google) apps to automatically access your data.

In case of Security Key, it won't be possible to restore access to your account through "forgot password". If you forget your key, you will have to go through additional steps to restore access to your account, which may take a few days.

12. CHECK TRUSTWORTHYNESS OF YOUR E-MAIL SERVICE PROVIDER

To ensure online security, checking the trustworthiness of e-mail service provider is of equal importance, so that they do not misuse and hand over your personal data to third parties (e.g. government of a foreign country) without your consent. As of April 2017, the most famous e-mail services are Apple, Gmail and Outlook; in case of Georgia, Mail.ru is also popular.

According to the 2017 Corporate Accountability Index, Google (Gmail) and Microsoft (Outlook) performed the highest in terms of protection of their users' freedom of expression and personal data. According to the same index, Mail.ru took the 12th position and lags significantly behind other companies in terms of confidentiality and freedom of expression. Mail.ru does not inform its users in advance about what kind of personal data it can process.

13. CONSIDER ALTERNATIVES FOR ABSOLUTE SECURITY

If you need advanced protection, forget about famous e-mail services and consider using relatively small alternatives:

Swiss ProtonMail – is one of the leading e-mail services in terms of security. It was created at the CERN research facility in 2013 and as of now has about 2.5 million users. The company's servers are located in Switzerland under 1,000 meters of granite rock in a bunker. ProtonMail has a free version that provides 500 MB of storage space and 150 messages per day. If you switch to ProtonPlus, you'll have 5 GB space and you'll be able to send 300 messages per hour and 1,000 per day.

ProtonMail fully encrypts your data and does not keep a key for decryption, meaning that it cannot access your data and transfer it to third parties. User confidentiality is mathematically secured, so that restoration of data is impossible, even in case you lose your password.

German Tutanota – automatically encrypts each sent message. The main advantage of this e-mail service is that users of other e-mail services can safely answer the encrypted messages sent by Tutanota users. It is designed to send e-mail from mobile applications.