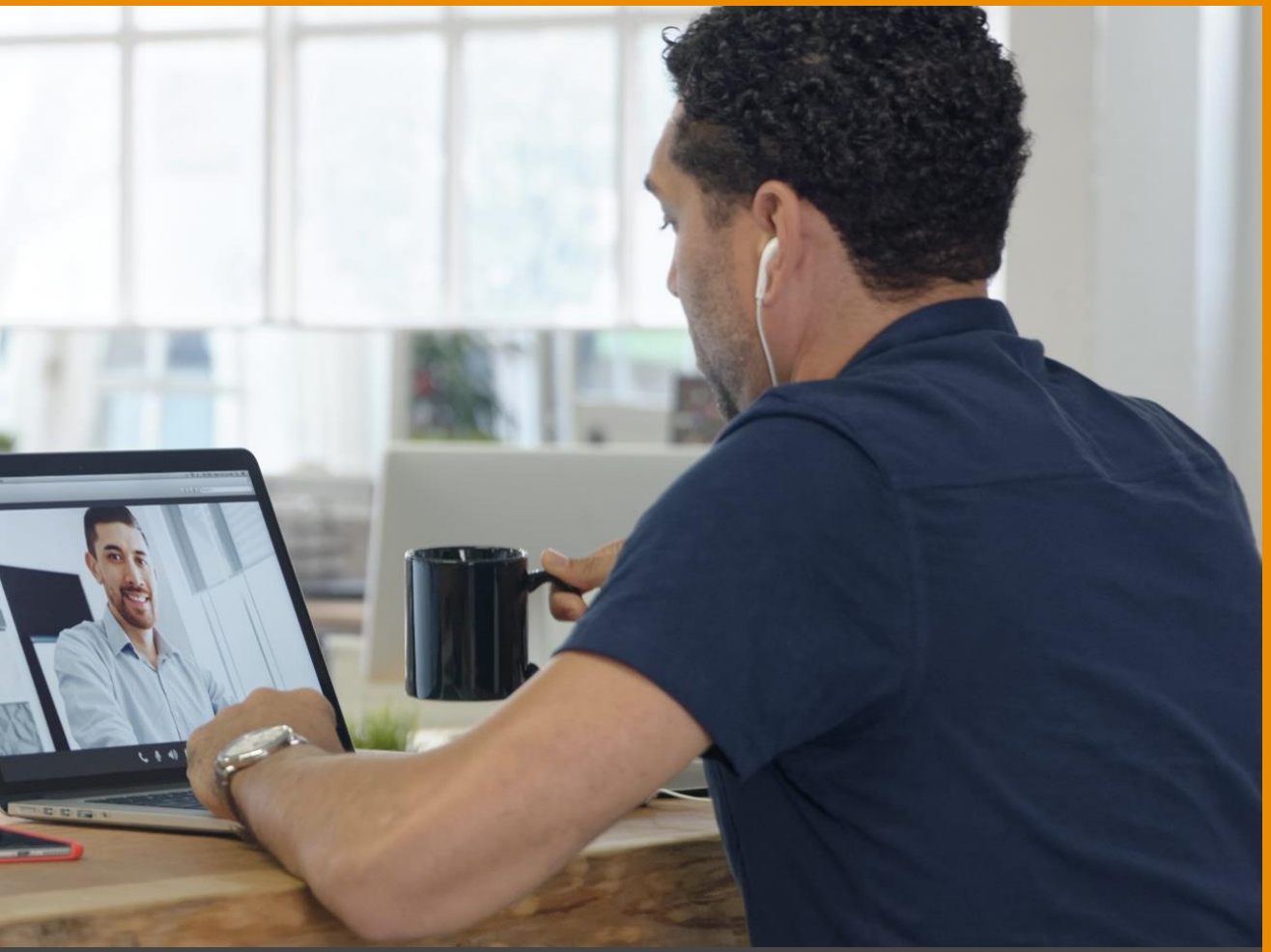
Information security while working remotely

April 2020

Contents



Social engineering

Social engineering is a set of different approaches to obtain confidential information by means of psychological manipulation. Attackers usually try to gather information through direct communication with the target and by convincing the target to use malicious software. We recommend to follow the safety measures listed below to counteract social engineering:

- Never disclose personal and confidential data to anyone (passwords, PIN codes, bank card numbers, codes from SMS confirmations, etc.). Be extremely careful with people who introduce themselves as special service representatives and demand for that kind of information.

- Do not connect storage devices to the computer, except for those that should be used under the business processes established in the organization.

- Do not use corporate storage devices (flash drives, portable disks, etc.) when working with personal devices, as malicious software can transfer from a personal device to a storage device and subsequently to corporate devices.

- More information on the various types of social engineering can be obtained from relevant publicly available materials on the Internet.

Phishing emails

Phishing is a cybercrime in which a target is contacted through a fake email or a fake web site by someone posing as a legitimate institution to lure individuals into providing sensitive data (banking and credit card information, passwords, account numbers, etc.). COVID-19 pandemic caused many people to work from their homes and it also made them vulnerable to phishing attacks. We recommend to follow the safety measures listed below to reduce the risks associated with phishing attacks:

When you receive a letter with a link to an external source that is not an official portal of the organization, you need to check where this link leads, or confirm with the sender that he did send a letter with this link.

If the letter was sent by an unfamiliar addressee, it is not recommended to follow the links in the letter and download attachments, be especially careful with extensions like .zip, .rar, .7z, .exe, .src, .dll, .sys, .bat, .js , .vbs, .js, .mht, .cmd, .xlsm.

You must report to the organization’s IT security service if you encounter frequent phishing attacks.

Phishing email example

From: SAP Support<jonathan.woods@ema1l.org> 1
Subject: Password change required

We would like to notify you that we have noticed the high amount of failed logins to your SAP account. 3
We appeal to you to change your password through the link below as soon as possible. In case that you do not change your password in 24 hours, your account will be blocked due to precautionary measures. This is sensitive information, do not disclose.
5 4

http://official.accounts.sap.org/change_password_id1290d129 2

Thank you,
John Doe 6

1) Examine the sender's email address to ensure it's from a legitimate account. Scammers typically use a randomly generated email addresses
2) HTTPS indicator is missing which means the website is not secure. Don't click on links or open attachments from such emails
3) Attackers insist you follow the link as soon as possible
4) Asking not to tell anyone because it's confidential or private
5) Establishing restrictions to cause urgent action
6) The name in the signature does not match the address of the sender

More information on the various types of phishing attacks can be obtained from the relevant publicly available materials on the Internet.

Malicious software

Malicious programs are created specifically for the destruction, blocking, modifying or copying information, disruption of computers, or computer networks, which is unauthorized by the user. We recommend you to follow the safety measures listed below to reduce the risks associated with malicious software:

- Do not disable or restrict the functioning of the device’s security systems (firewall, antivirus). Do not disable the automatic system/application updates.

- Run-on a computer exclusively under the rights of the user, not the administrator, which will greatly prevent the installation of malicious software and changing system settings without the knowledge of the user.

- During the period of remote work, it is extremely important to restrict access to the device from which the workflow is carried out: set a password for the account and restrict physical access to the device.

- If work is carried out from a device to which children have access, it is recommended to create a separate account for them and limit the ability to install programs/games, as well as close access to folders with working files.

- Install only licensed software. Do not run unknown files, especially with the extension .zip, .rar, .7z, .exe, .src, .dll, .sys, .bat, .js, .vbs, .js, .mht, .cmd, .xlsm, .docm.

Password theft

A password is a set of characters, symbols, and numbers that are used to protect access to a user account. Passwords represent valuable information for attackers. We recommend to follow the safety measures listed below to reduce the risks associated with password theft:

- Create complex passwords (minimum length of 8 characters, containing letters (uppercase and lowercase), numbers, special characters (! # $, etc.)). Do not use the automatic password filling functionality.

- Do not click on suspicious links (for example, links provided in WhatsApp chats that lead to unverified sources).

- When receiving information about the need to change the password from any service, do not delay with changing the password. Do not use the same passwords for different services.

- Use two-factor authentication whenever it's available for all the services you use: when the process of logging in requires an additional code, for example, a one-time PIN code via SMS, apart from the use of a password.

- Change passwords regularly (once every 2-3 months); regularly check the availability of accounts in the corresponding databases of compromised accounts available on the Internet, do not use previously compromised (hacked and published) passwords.

Leakage of confidential information

The number of risks associated with the threat of confidential information leakage rises significantly when employees are working remotely. We recommend to follow the safety measures listed below to reduce the number of such risks:

Do not open confidential files/emails on an unincorporated device. Protect your device from viruses by installing the latest available operating system updates and antivirus software.

Email

When exchanging information with other employees/clients, encrypt files using archivers. If you set up a password to protect the file it must be transmitted via a separate communication channel, for example, by a separate letter. The file encryption algorithm using the 7-Zip archiver is shown in slides 9-10.

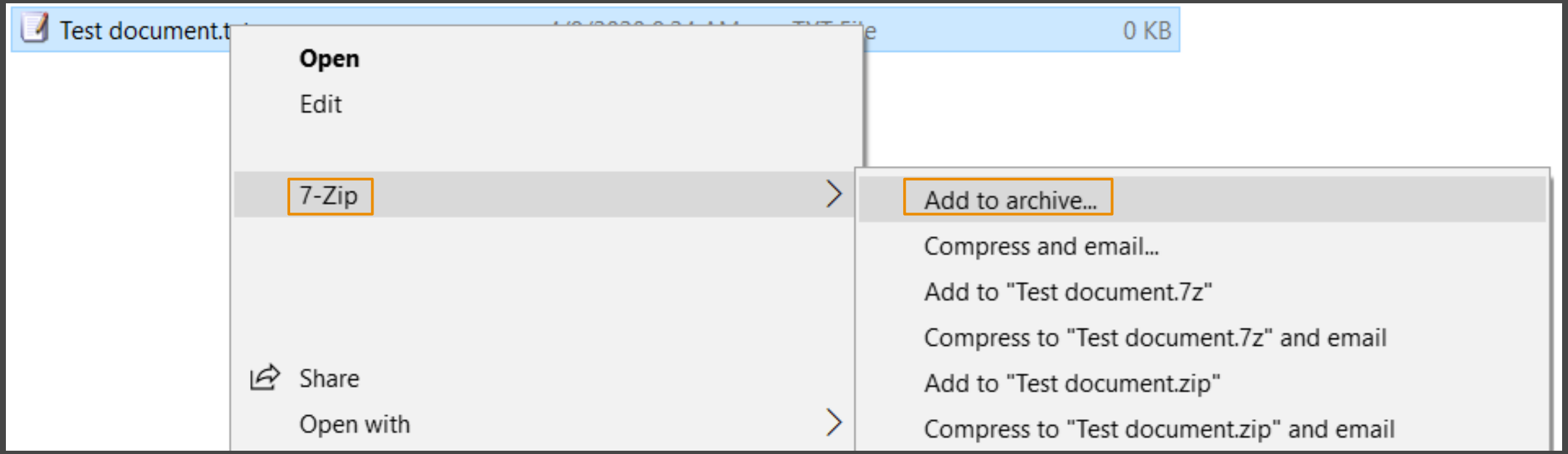
ZIP

When you print any documents at home, you must make sure that no one else has access to these documents. Documents should be stored in a secure place with limited access, for example, in a locked cabinet.

If the document is no longer needed or was printed by mistake, then it must be destroyed securely. Use a paper shredder if you have one, otherwise, use a corporate shredder in the office when it will be possible. Keep the documents in a secure place until you destroy them. if there is no other possibility, chop the document yourself and dispose of it, preferably in different garbage bags.

File encryption algorithm using the 7-Zip archiver

Step 1.



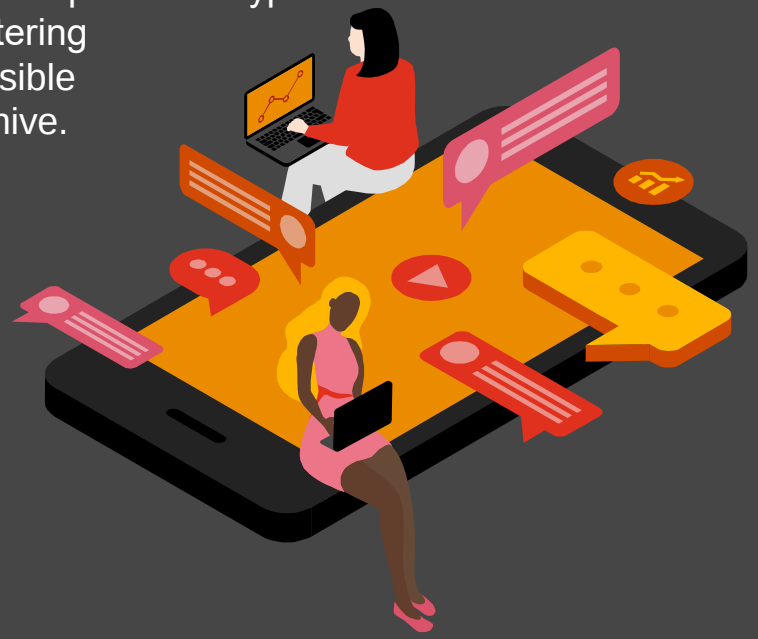
In order to create a folder (or a set of files and directories), just right-click on the file you want to encrypt and select from the menu items “7-Zip” - “Add to archive...”.

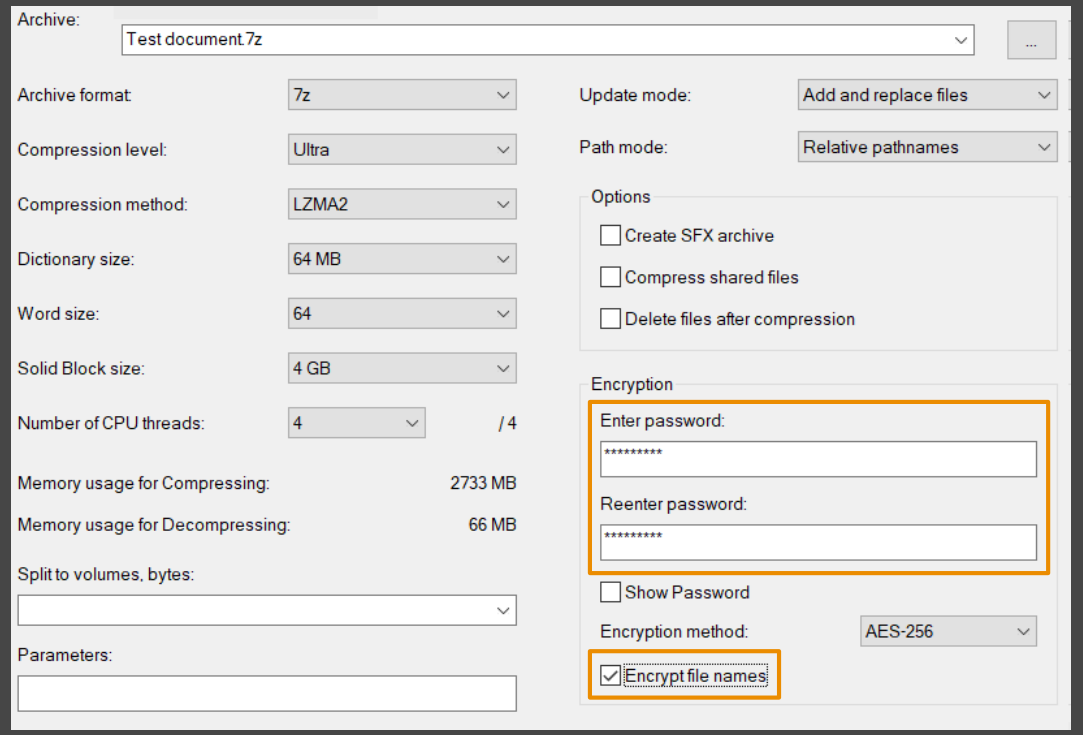
File encryption algorithm using the 7-Zip archiver

Step 2.

As a result, you will see the archiving settings window where you can set a password for access to this file, or you can rather encrypt all contents of the folder (archiving it at the same time), and this password will be the key to decryption.

It is also necessary to select the option “Encrypt file names” so that without entering a password it would be impossible to see the contents of the archive.





Internet security

Since the remote mode of operation involves the active use of the Internet, special attention should be paid to security procedures during its use. We recommend to follow the safety measures listed below to work safely on the Internet:

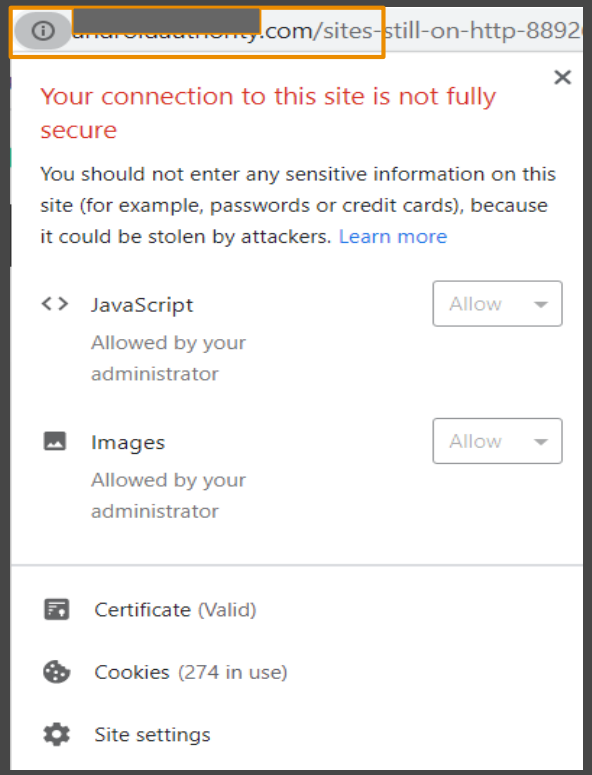
Do not ignore warnings from a web browser or antivirus about a poorly protected site. Do not visit sites that do not have security certificates. A corresponding icon at the beginning of the address bar (with HTTPS) indicates the presence of a security certificate. Examples of safe and unsafe connections can be seen on slide 12.

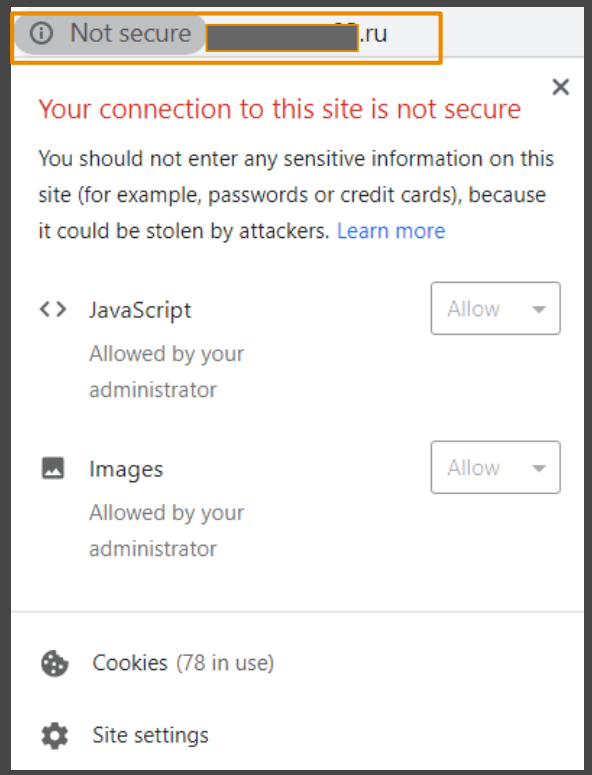
Whenever you can connect to the corporate network via VPN, check for a successful connection each time you use the device.

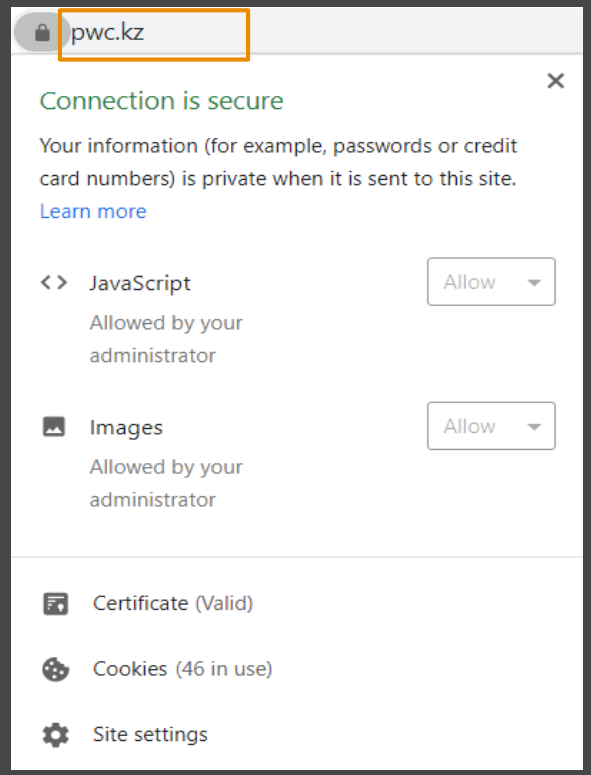
Do not trust unknown Wifi connections that do not require a password. In most cases, attackers use this kind of network to steal user's data. Instructions on how to check the connection used can be seen on slides 13-14.

We recommend setting up a complex password for your wireless network at home and choosing a more complex Wi-Fi network protection algorithm (WPA2). For more information on how to properly configure Wifi on a router, see the device manufacturer’s website.

Examples of not fully secured, not secured and secured connections in Google Chrome

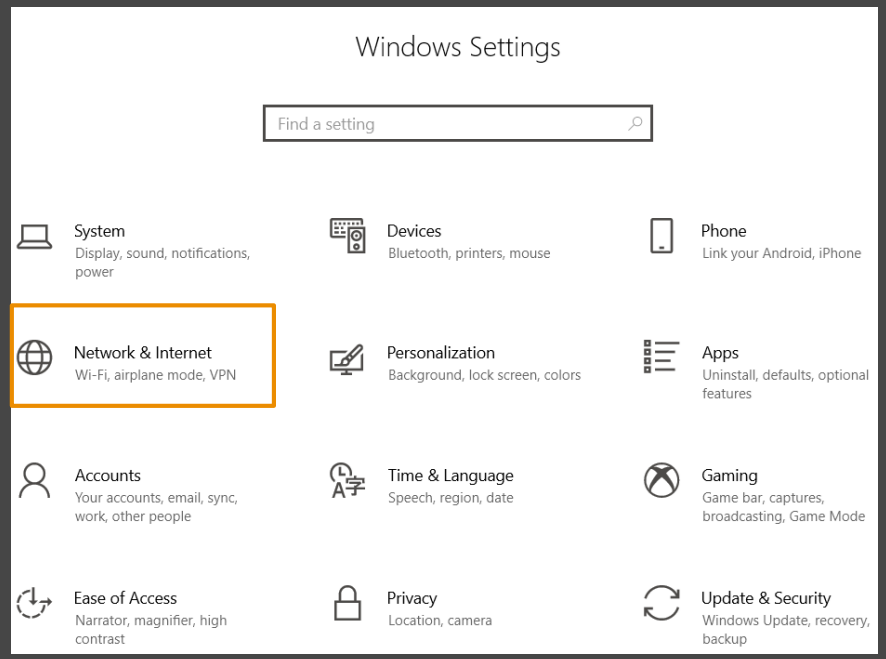


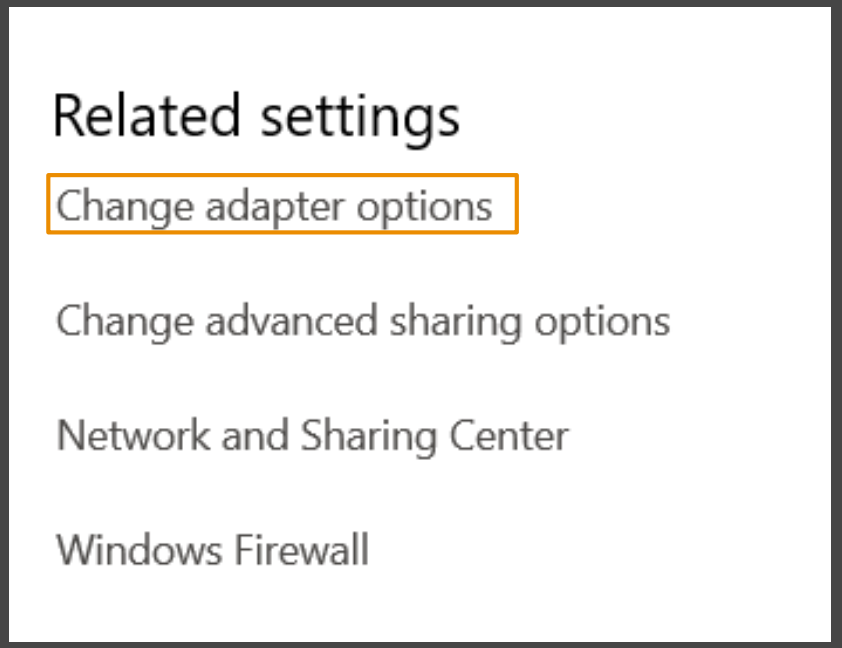




Certificates are verified by special organizations or systems and have confirmation that they were formed by the real owner of the site. Another element of website security is the advanced HTTPS protocol.

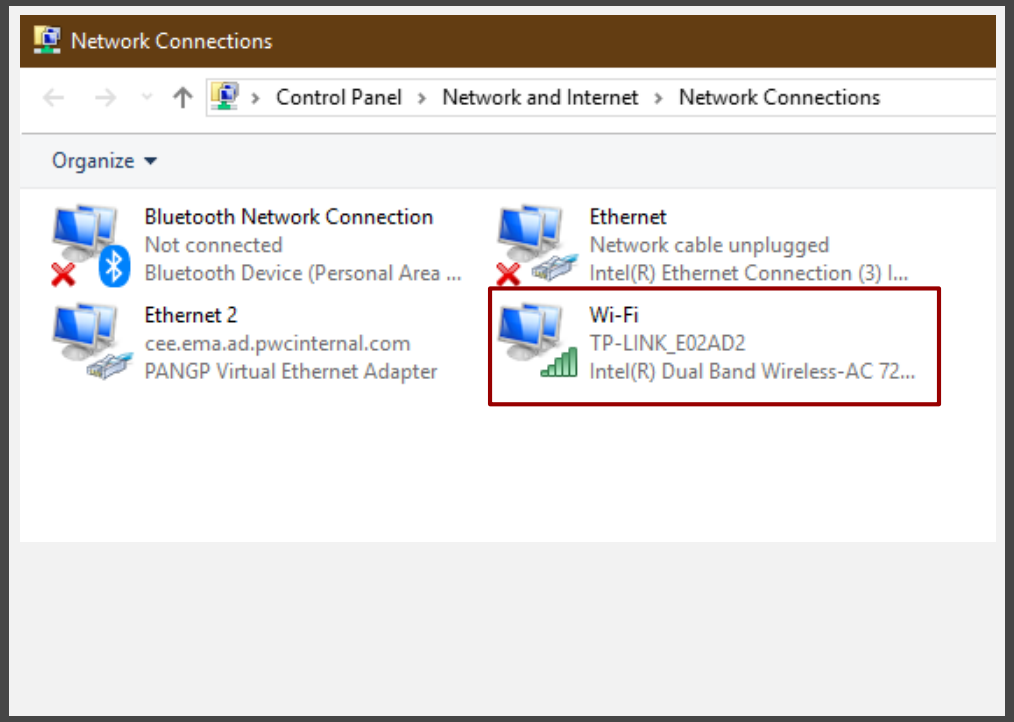
How to find out the WiFi security type on PC?

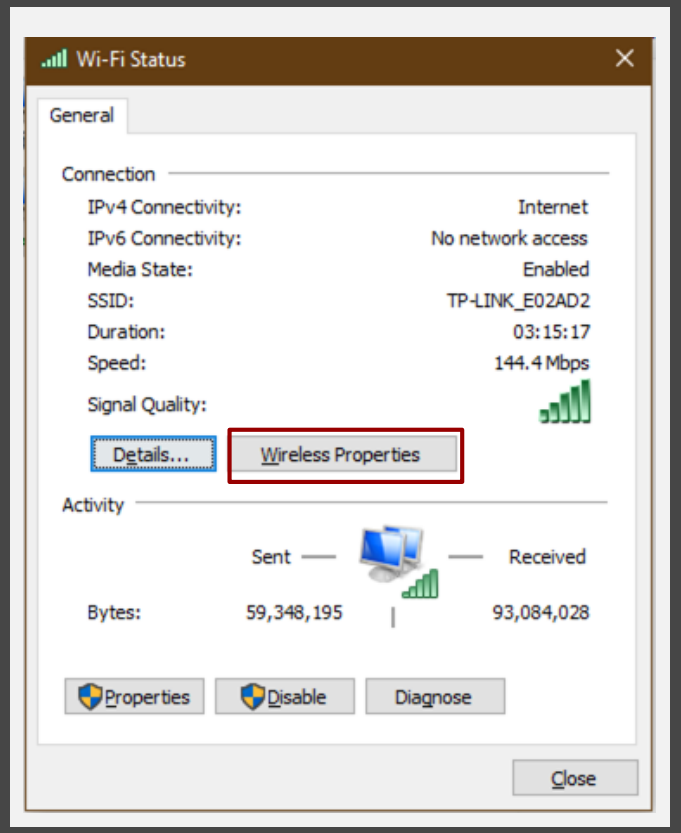


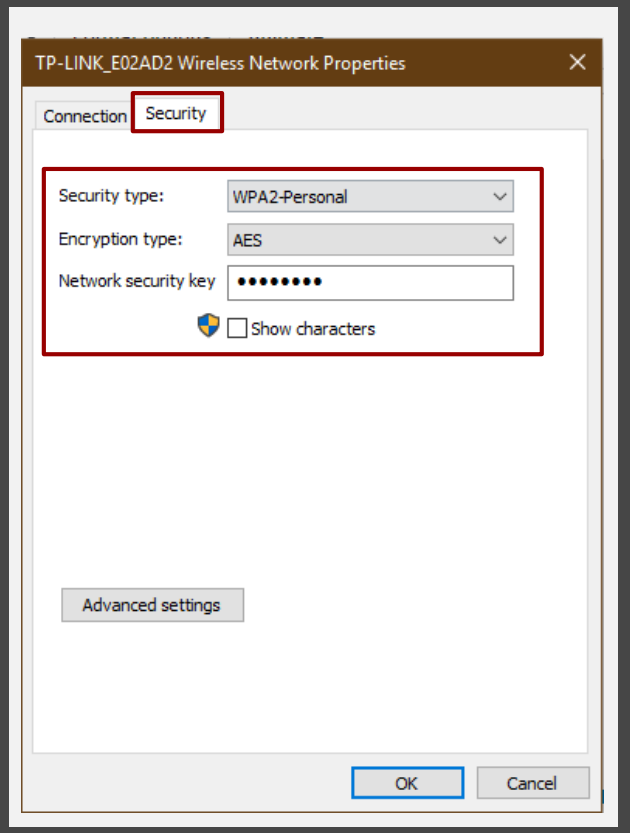


First, you need to go to the Settings panel, then select Networks & Internet. Next, choose the WiFi tab and on this tab you will need to select Change adapter options.

How to find out the WiFi security type on PC? (continued)







After that, the Network Connections window will appear on the screen, select WiFi. In this window, we can see the Status of the Wireless network. Further, select Wireless Properties. In the Security tab, we recommend setting up a complex password and choosing WPA2 as the security type.

Corporate property damage

Due to the quarantine caused by COVID-19, access to IT support is limited, so you should be extremely careful with the corporate devices that are used for work. Replacement of a laptop or additional device is not possible under the current circumstances. Our recommendations for protecting your work device are presented below:

- Be responsible for the firm’s property.

- Do not leave your device in direct sunlight or humid environment.

- Be extremely careful with any liquids near the operating device.

- Do not eat while working on the computer.

Work mode

Tiredness from overworking can significantly reduce attention and lead to non-compliance with information security measures. We recommend to follow these simple steps to work efficiently from home:

Allocate time for working, eating and rest. Discipline yourself and respect your schedule.

Regularly exercise your eyes while working on a computer and warm-up your muscles by doing stretches and short walks.

Thank you

pwc.kz