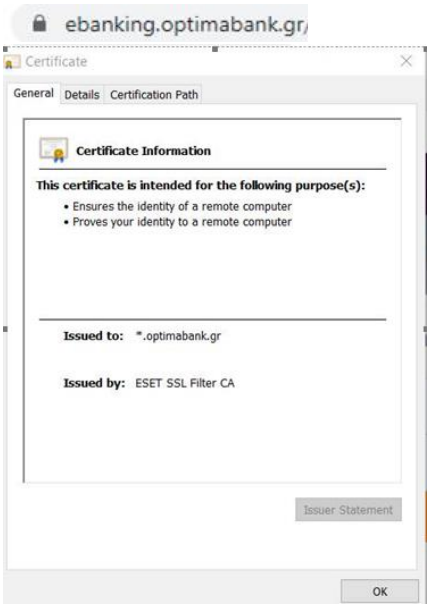
Useful Security Information

Access to our e-banking service is ensured by using internationally recognised practices, both at technical and user level:

- The e-banking service is accessed with the combined use of your personalized security credentials (User ID and Password) which should comply with specific security rules notified to you by Optima bank from time to time. For additional security, in case you suspect loss or interception of your security credentials , you may prohibit access to your e-banking by entering incorrect security credentials three consecutive times (you may reset your security credentials online). Every 6 months you are required by the system to change your password, even though you can do so on your own initiative at any time.
- We promptly notify you by free email in the following cases:
    - Failed attempt to log in to the e-banking system;
    - Security credentials locked after 3 consecutive failed login attempts;
    - Password change.
- On a technical level, we use the latest technologies, offering you maximum security. Our e-banking system uses a digital encryption certificate issued by *ESET SSL Filter CA (as shown in the lock icon before the URL)*, an internationally recognised provider of encryption certificates:



In addition to the measures we take for your security, we urge you to follow the below basic safety rules:

- **Make sure that you visit the Optima bank website.** Before each connection, make sure for your own safety against malware that you connect to the correct URL.
- **Check that you are using anti-virus and anti-malware security programs.**
- **Keep your secret codes…secret.** Do not share your security credentials with anyone. The habit of keeping them written on paper, a notebook or even on your mobile phone is equally dangerous.
- **Do not use the same codes for our e-banking system and other websites**.
- **Do not save your security credentials in the browser or other applications (e.g. Password Managers), especially if you use public computers or computers belonging to third parties.**
- **Delete the computer's temporary Internet files.** Go to the settings page of the search engine you used to log into the e-banking and choose "History" to delete the relevant files. Alternatively, use the shortcut CTRL + SHIFT + DEL on your keyboard (applies to all browsers).
- **Beware of phishing attempts.** These attempts typically involve a misleading message (email/text) which, in response to an alleged emergency (e.g. "your account will be locked"), leads you to a fake website that visually resembles your e-banking website. By visiting this website and entering your security credentials, you are practically disclosing them to malicious third parties. You should log in to your e-banking website after checking that the address displayed on your browser is the correct address AND has a relevant lock icon, indicating that an official digital encryption certificate has been issued.
- **Access through WiFi.** Make sure your WiFi connection is secure and also encrypted according to the latest specifications, such as WPA2 or WPA2-Enterprise if you are logging in through a corporate network. In any other case, a malicious user may intercept the communication by accessing sensitive information such as your secret security credentials. If you are not sure about the security specifications of a WiFi network, it is best to use the 4G/5G connection of your device for your banking transactions.
- **Keep checking your account.** It is good practice to regularly log in to your e-banking account and check your transaction history. In case you identify any suspicious transactions, notify us immediately.
- **Always watch your devices.** Since access to your email and mobile phone can be used as proof of your identity, you should be careful not to allow any third-party access to them. Please follow these steps in case you lose your mobile phone:
    - Contact your telecommunications provider in order to have your device disabled.
    - Immediately change your email password (especially if you have allowed access to your email through your mobile phone).

Log in to your e-banking website and change both your User ID and password. Alternatively, you may temporarily lock your security credentials by entering a wrong password 3 consecutive times (you can easily reset them online later, by selecting "Forgot your credentials).