FOR Xbase++ Developers

Google changed the way to log in to Gmail from external applications due to new security standards

As of May 30, 2022, Google has changed the way to sign in to its Gmail email application, but only from, as they call it, "less secure" applications.
This is a problem for users who until yesterday used access to Gmail from some of their applications, which Google allowed by using technology that allowed access to Gmail by "less secure apps" (Less secure apps sign-in). That is, Google allowed the user from one of its external (third-party) applications, which is not Google's, to log in to Gmail only with the user's existing username and password, and then receive or send e-mail within that application.

The option to access less secure apps has been automatically disabled by Google and can no longer be activated, so all apps that were able to access Gmail until now are prevented from doing so in the future.

Applications that are affected by this new rule are: Microsoft Outlook 2016 and all other older versions of Outlook, Mozilla Thunderbird versions older than 91.8.0, as well as numerous other third-party applications, including our accounting program, which does not support the new Google login technology named "Sign-in with Google" and therefore does not belong to the SAFE applications from Google's point of view. "Sign-in with Google" represents the integration of Google and their standards into other applications, and any application that has it is a secure application. Those applications that do not have this technology integrated are no longer secure, and some become totally unusable, such as old versions of Outlook, and some others, such as our bookkeeping program, can still be set up, but with additional settings of your Google account, which we will cover in more detail in the following text.

So what is the solution?

Regarding email clients, it is recommended that users start using the new Outlook 2019 or Office 365, or the new Thunderbird, or any other application that only supports the "Sign-in with Google" option (we said that such applications are considered safe applications google). For other less secure third-party applications, including the CSYSTEMS bookkeeping program that does not have integrated Google technology, you need to activate a new option on your Google account called "App Passwords" or translated "Passwords for Applications" (more precisely : special passwords for less secure applications). This option replaces the old option and was created exclusively for the purposes of signing in less secure applications to Gmail, but not like before in the old option where it was enough to enter only the existing username and password, but now we have to have this new special password, and in order to be able to create that new password, we must first activate two-factor authentication (2FA) on our Google account, which we have not used so far (those who have will have less work). So, the novelty is that new special password or "App Password" that we create exclusively for the application we use - one password for one application (we can use several different passwords for the same application, and I have not tested one password for several different applications, I assume that it can also that).

The "Sign-in with Google" technology is part of Google's new cross-platform technology that can be integrated into third-party software and is used for user authentication. It is based on OAuth 2.0 and similar user authentication technologies used by Google.
Therefore, this technology is based on the latest security standards that explicitly require that login to Google applications is done exclusively by two-factor authentication or the popular 2FA (implemented through the OAuth 2.0 system).

To make the text clearer, here are the definitions of the terms we use:

"OAuth 2.0" – protocol and technology for user authentication to Google services and applications

"2FA" - part of OAuth 2.0 technology, a secure way to login to Gmail

"Sign-in with Google" - an option in new email clients for secure access to Gmail with just a username and password. If some other external applications also have this option, then Google considers such applications safe, not less safe. So Google distinguishes between three types of applications: its own Google applications, third-party secure applications and third-party less secure applications.

"Less secure apps sign-in" - the old system for signing in less secure third-party apps to Gmail

"App Passwords" - a new system for logging in less secure third-party applications to Gmail

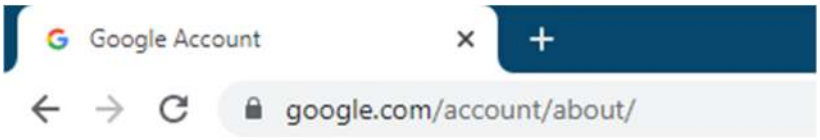
Furthermore, two-factor authentication (2FA) is a modern and secure way of logging into a website or web application that consists of "two factors". The first factor is the username and password that the user must enter in the application form as the first step in that application, followed by the second factor/step in the application, which is the VERIFICATION CODE that the user receives by SMS to the phone or through a specific application* on the phone and enters it in the provided field in the login dialog.
(*for example Google Authenticator or Microsoft Authenticator, applications that are installed on android or Iphone mobile phones).

Since our bookkeeping application does not support or integrate this Google login technology to their services, this means that in our program there is no option to log in via Google (Sign-in with Google) nor does the program support two-factor authentication because it is not a web application but a classic one desktop application, we provide the solution in the following text.

What does all this mean for a user of an accounting program or business program (application) who wants to send emails to users directly from the program, and how exactly does the user have to set up his Google account to enable sending emails from the program at all?

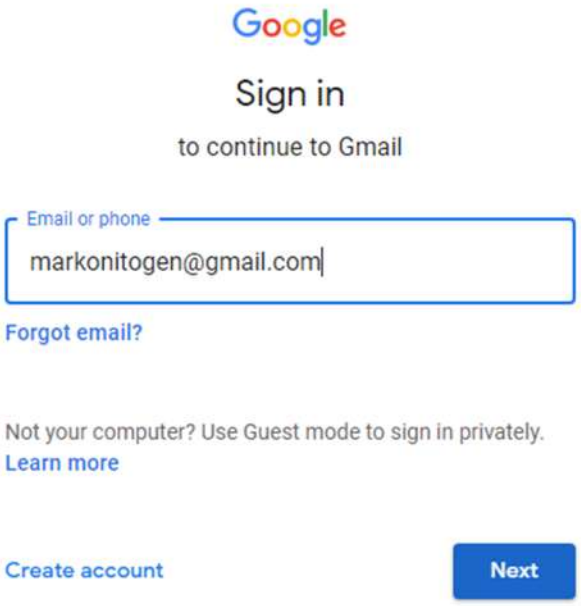
The first thing a user should do is to change the password for their Gmail account to a more complex and secure password with a combination of upper and lower case letters, numbers and at least one special character. This procedure is not mandatory, but we recommend it in any case if the password has not been changed in a long time.

To change the password, the user must first log in to their Google account at the address https://www.google.com/account/about/

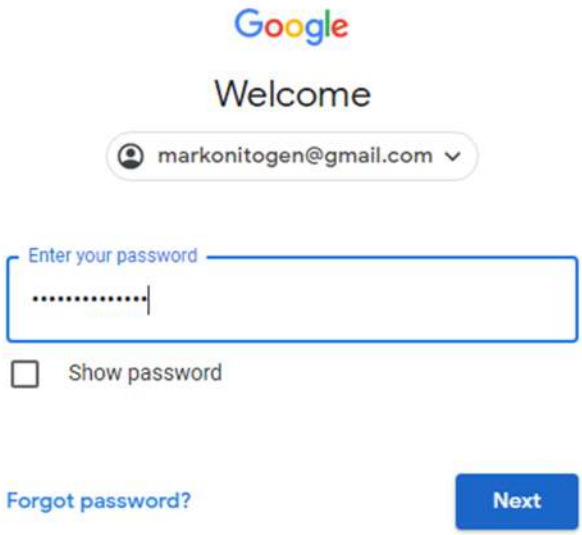


Then you need to click on the blue Go to Google Account button

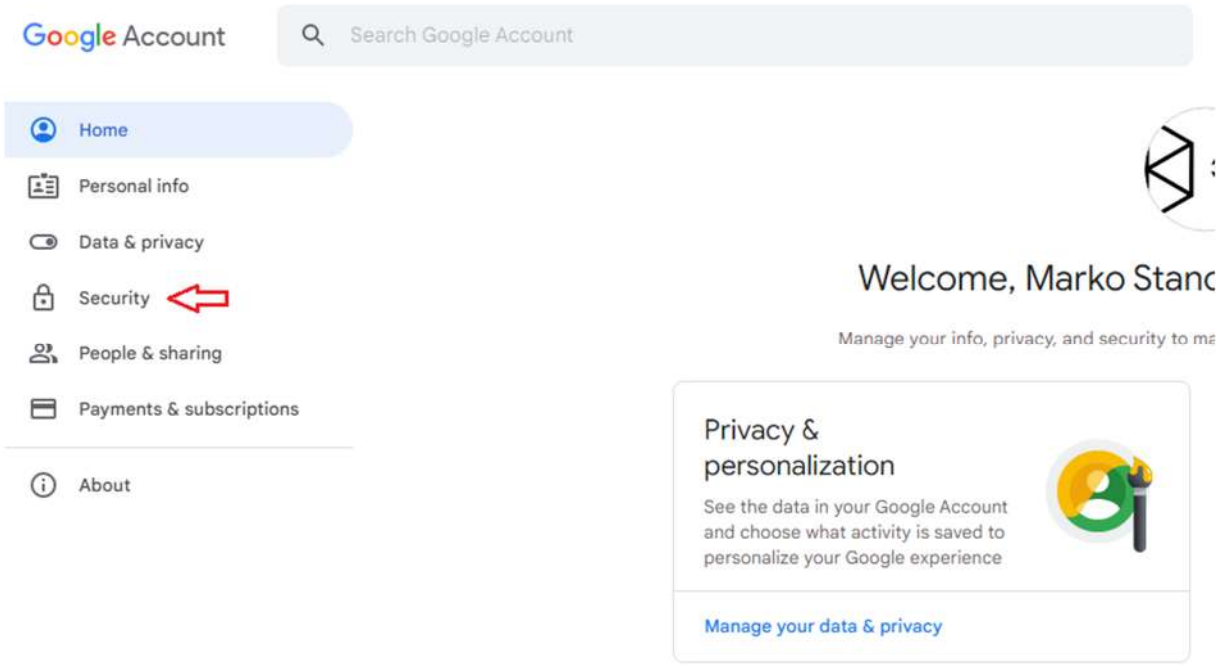
Then enter your username (email)



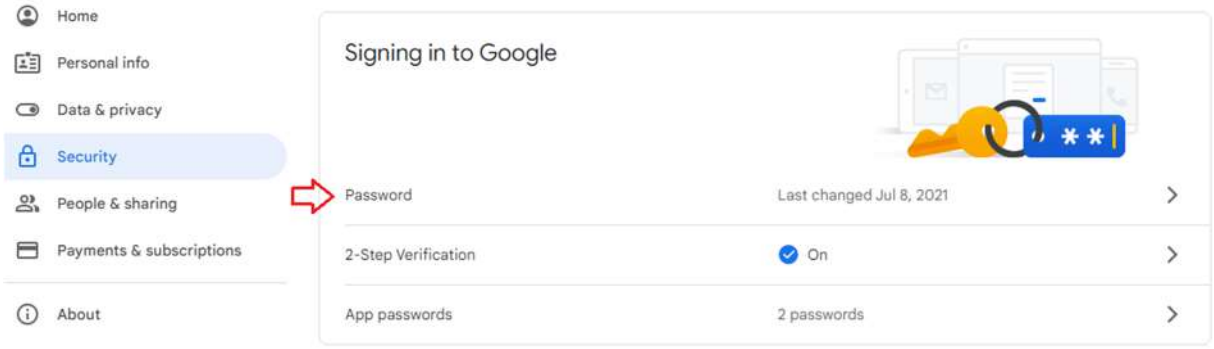
and then the password



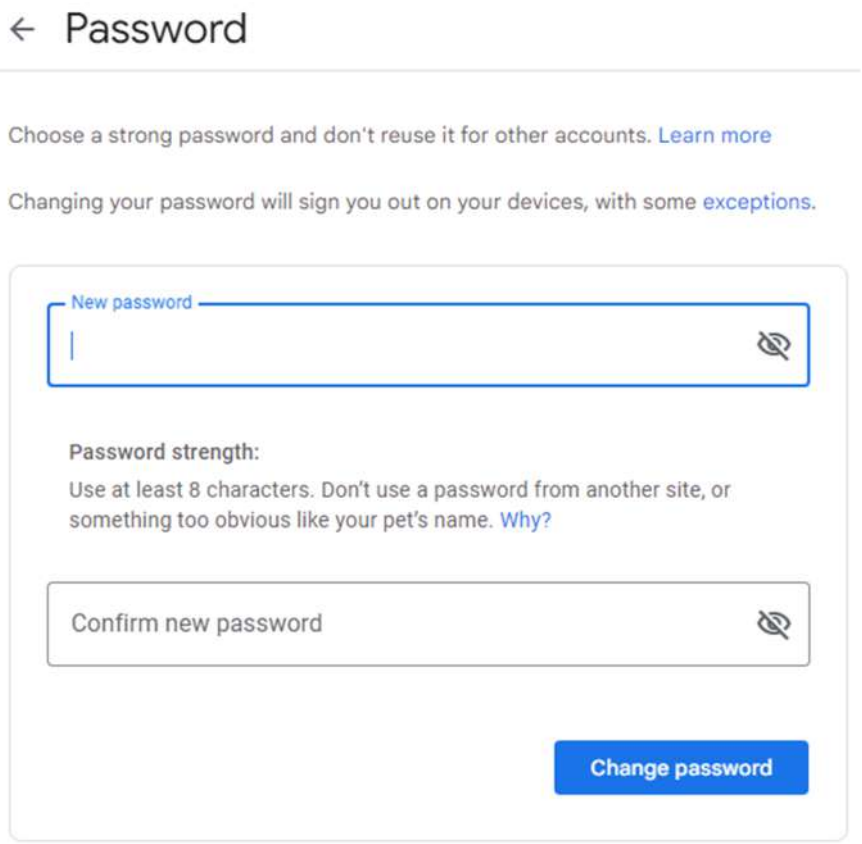
After that, a page will open with a selection of options for setting up your Google account, and for all subsequent steps, the most important option for us is Security (click on Security)



Under the Security menu, we now have several submenus, the most important of which is the one called Signing in to Google, and to change the password, select the Password option



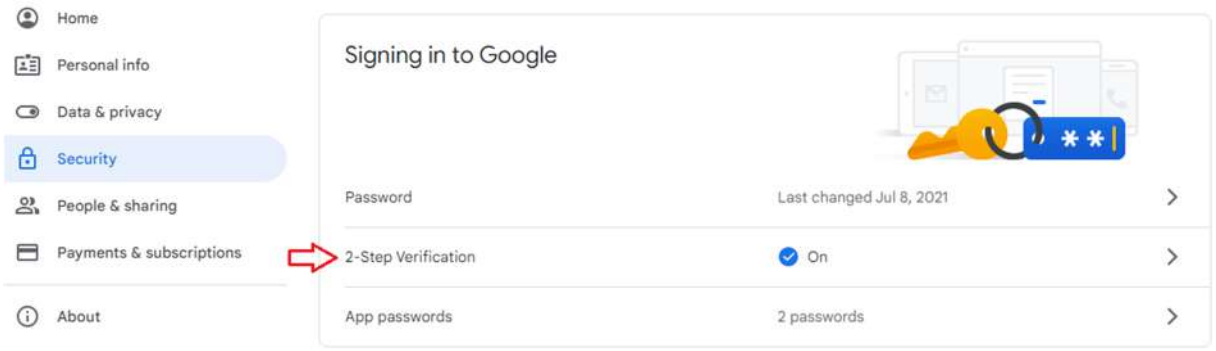
On this screen, we enter a new password



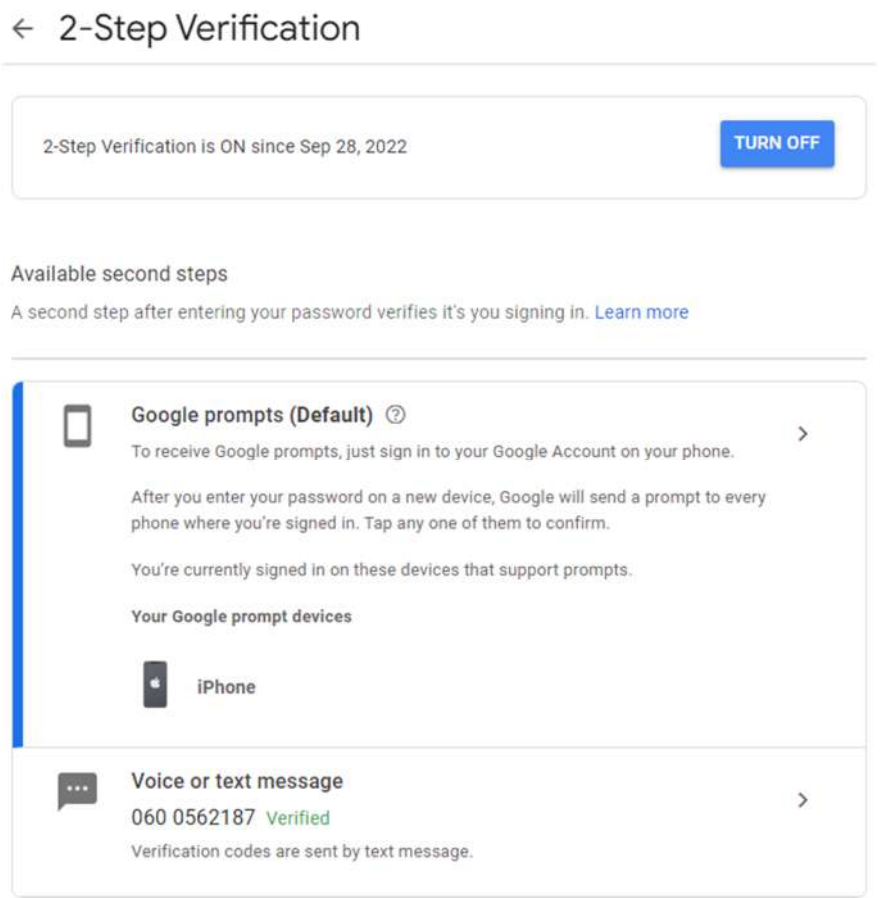
After entering the new password, we return to the previous menu and, as the next step, set up two-factor authentication.

The second thing a user needs to do is to activate 2FA authentication on their Google account. 2FA authentication must be active because "App Passwords" will not work without it, and "App Password" is what we need to be able to send emails from our application.

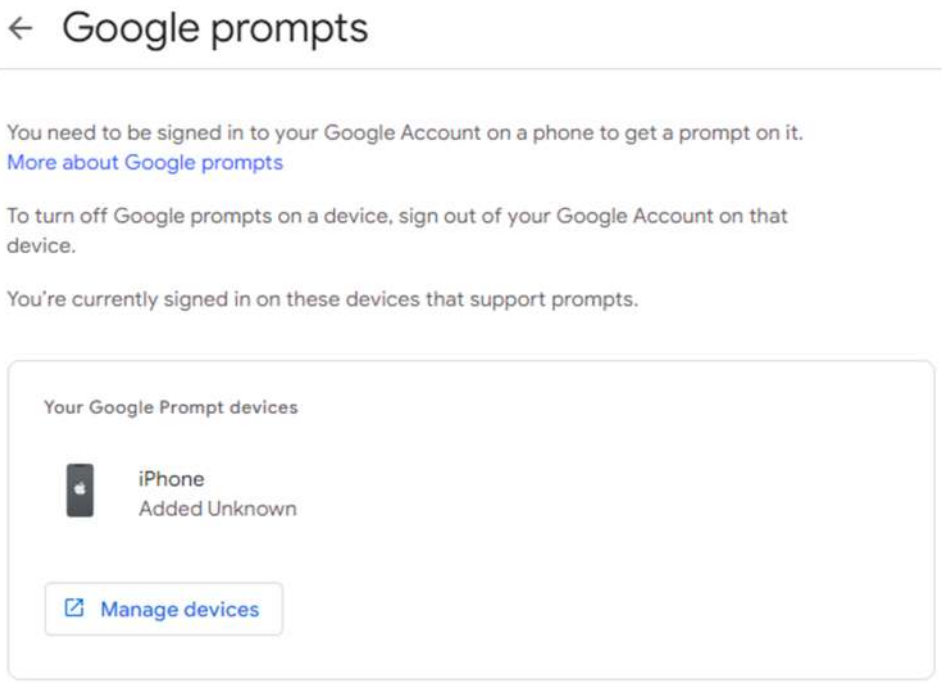
So, turning on 2FA authentication is done from the Security menu, and then, as in the previous step, we go to the Signing in to Google submenu, but now we choose the 2-Step Verification option



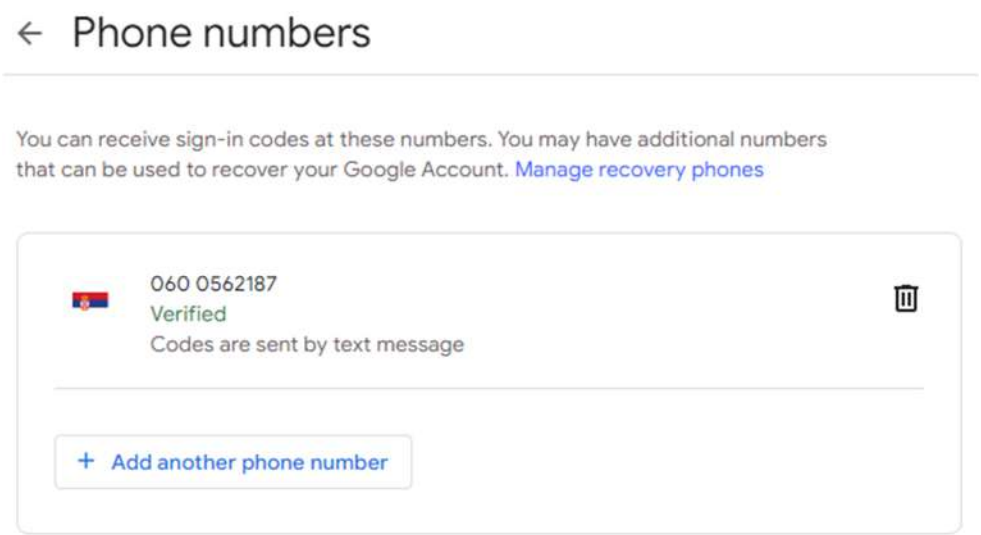
Here we enable 2FA authentication and set the way in which the "second factor" or step verification will arrive: in the form of a Google prompt, which is the default option, or via an SMS message to a mobile phone



Google prompt is the default solution, and if you already have a Google account set up on your mobile phone, your phone model will automatically appear here and the option will be active.



If you have a Google account set up on your phone, Google will automatically already know your phone number to which it will be able to send a verification code if by any chance Google prompt is not working

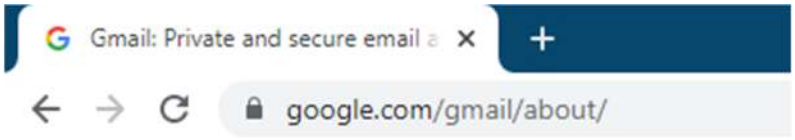


So, the second step or factor in the verification of the Google account login can be in the form of a Google prompt (only if we have a Google account set up on the mobile phone) or in the form of a classic verification code that arrives in the form of an SMS message. The good thing is that today the majority of users have Android phones on which a Google account has been set up for a long time - because it is a mandatory option on Android phones that is set up when the phone is first started. This option has also been around for a

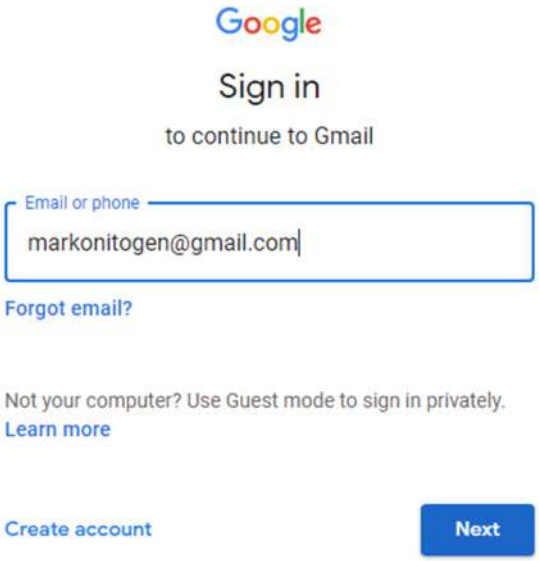
long time on Apple phones, so users won't have much to do with settings here. It is enough for them to enable 2FA authentication on their Google account and Google will set everything up for them.

What does it look like in practice to log into a Gmail or Google account from a classic computer at work or from home, but now with 2FA authentication enabled?

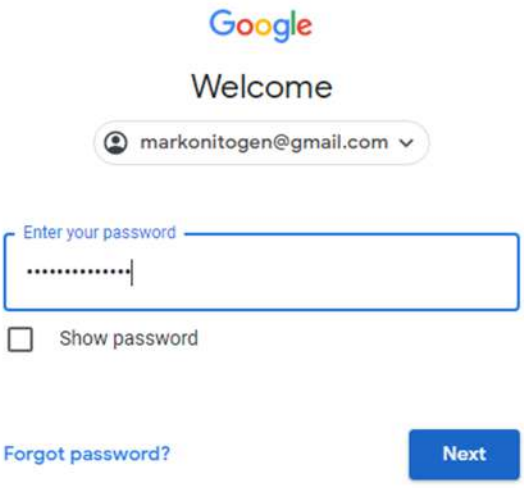
ON OUR COMPUTER, we enter the Gmail address in the browser



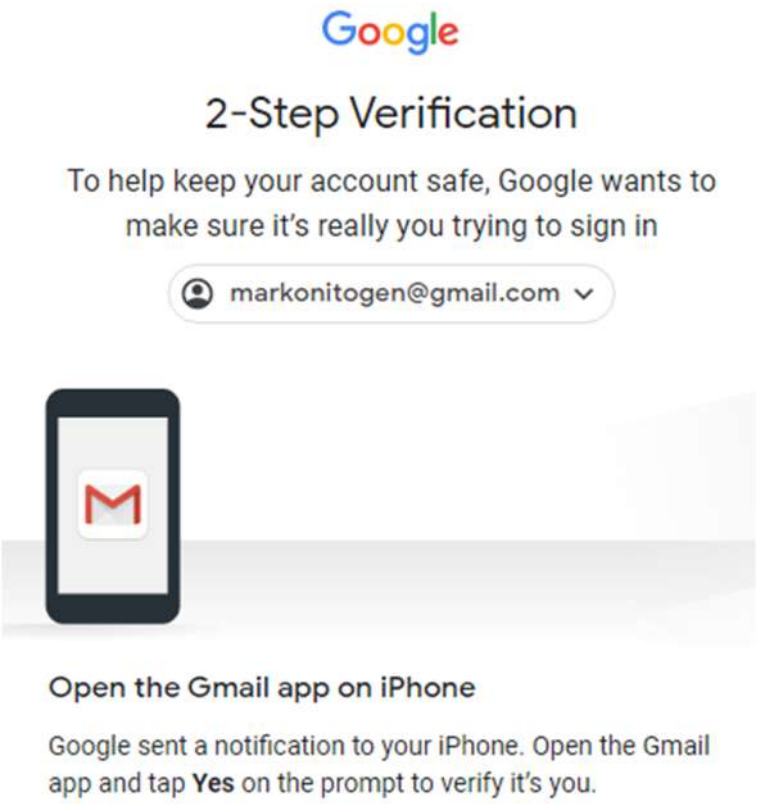
Then we enter the username (e-mail address)



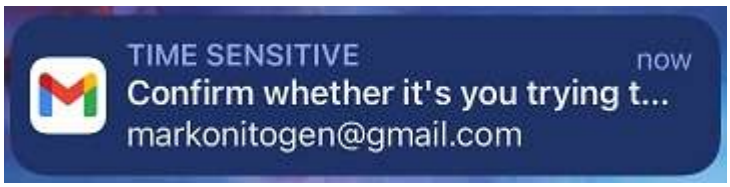
and then the password



After entering the username and password **IN THE BROWSER ON THE COMPUTER**, a new page will appear that will ask us to confirm the "second factor" or step in the application **(on this screen, Google specifically informs us to look at our phone now)**

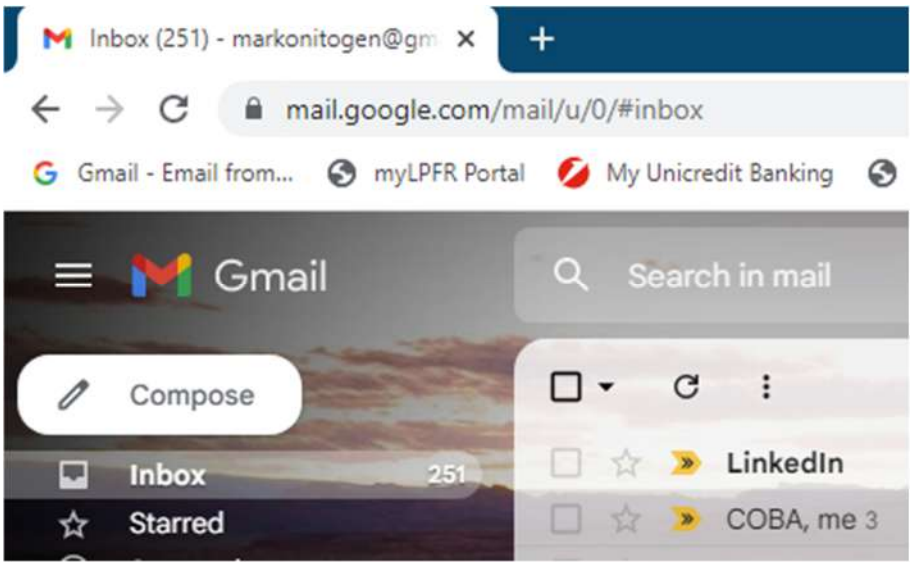


The next step is to first click on the authentication request notification **ON OUR PHONE (this is a Google prompt)**

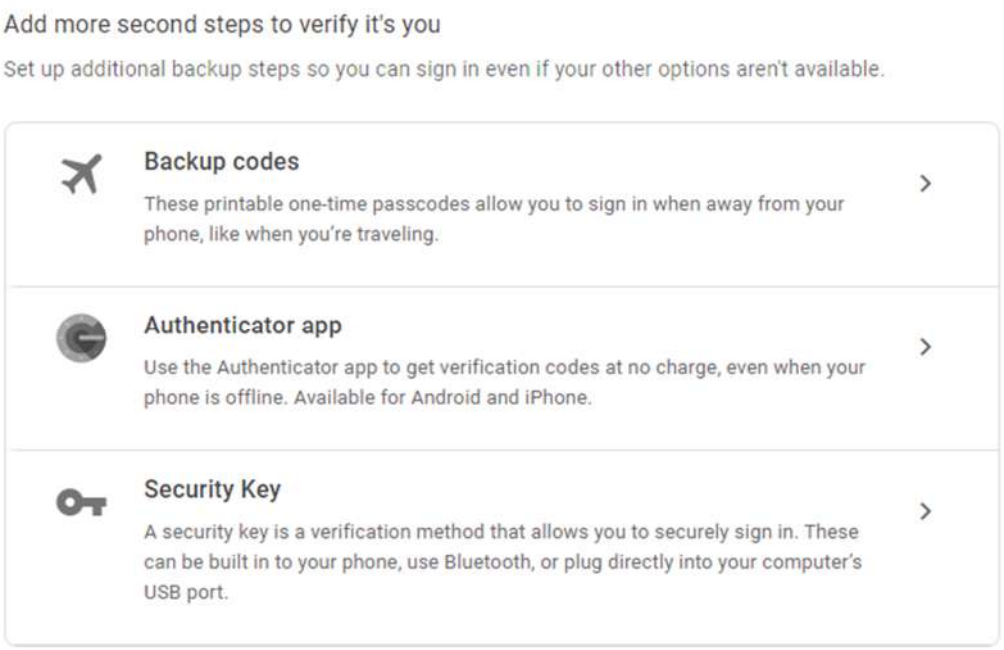


And then on the screen that opens next **ON THE PHONE**, click on **YES, it's me** and confirm the login **(and this is a Google prompt)**

After that, **ON THE COMPUTER** in the browser, our Gmail account will open



Here we have shown the login to a Gmail account with 2FA authentication enabled using the Google prompt option. Google prompt can be turned off and the user can set that the verification of the second step arrives via SMS message, and in addition there are several other ways that are not important for us at the moment, but the user can set them if he wants to experiment or protect his account even more strongly, as in example:

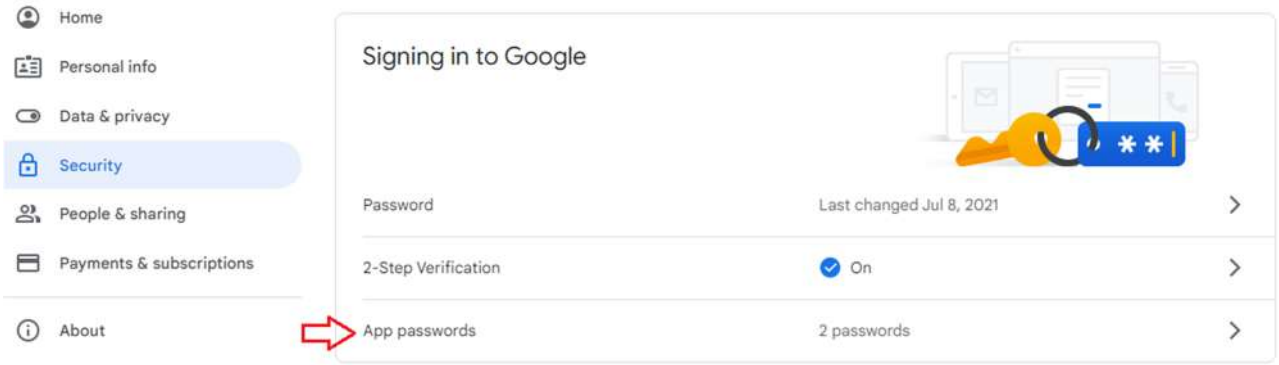


As we can see, now with 2FA authentication enabled, we will have to additionally use a mobile phone every time we log in to our Gmail account from a home or business computer. Until now, we haven't needed this way of logging in, mainly because of the unnecessary additional steps during logging in that take up our time, and it can also be a big problem because if our phone is not working at some point - we won't even be able to log in to our Gmail account on the computer. .

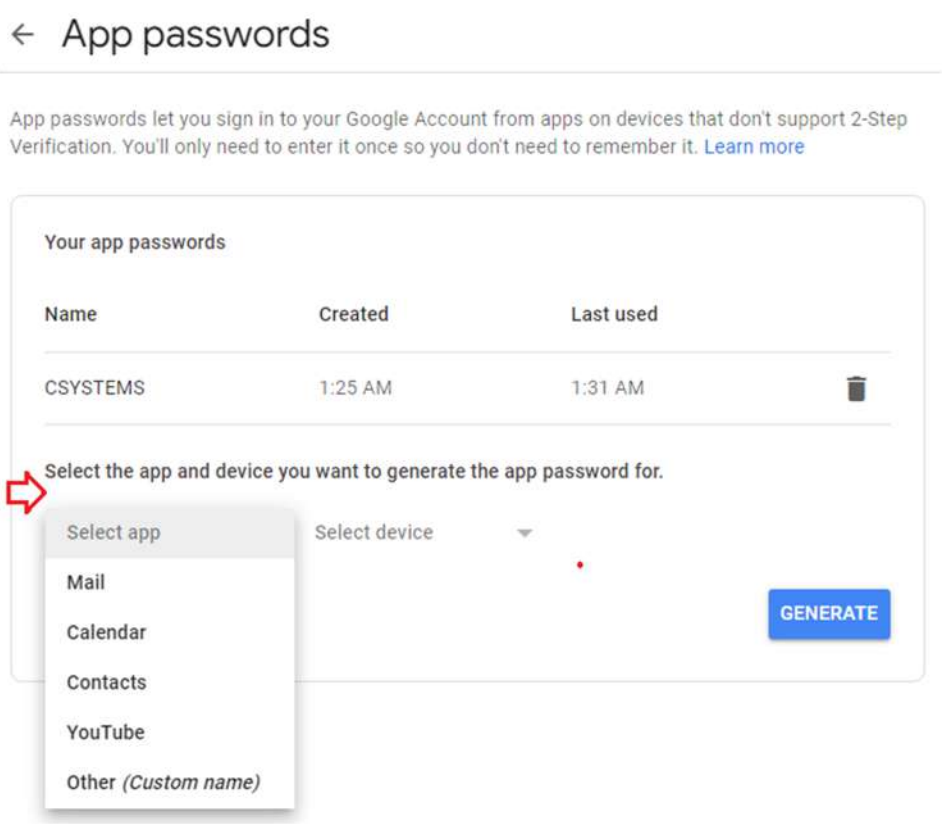
The third and most important thing the user has to do is to activate the option called "App Passwords". This option replaces the previous option that allowed a user from one of their external applications to log in to Gmail using only their standard username and password. This option now offers the user to create a special NEW password to be used with the already existing username.

App Passwords is a special password of 16 letters, which comes as a replacement for the older option Less secure apps Sign-in and can only work if two-factor authentication is active on the user's Google account.
(Google Article with detailed instructions on the function and use of this new option: https://support.google.com/accounts/answer/185833)

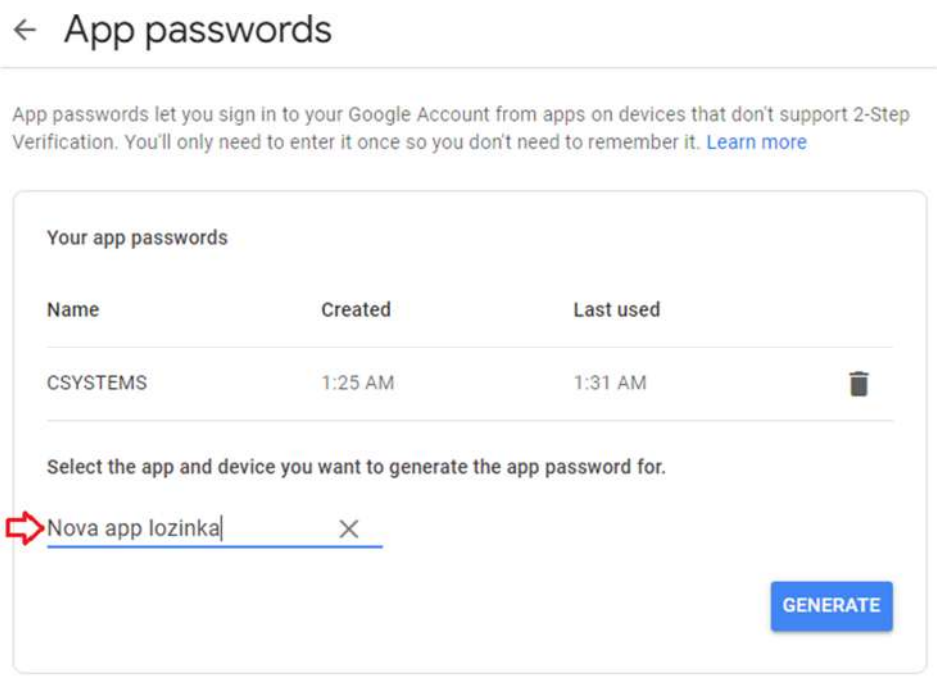
To activate this option, we return to the page of our Google account as in the first step, select the Security menu, then the Signing in to Google submenu, and now finally select the App passwords option



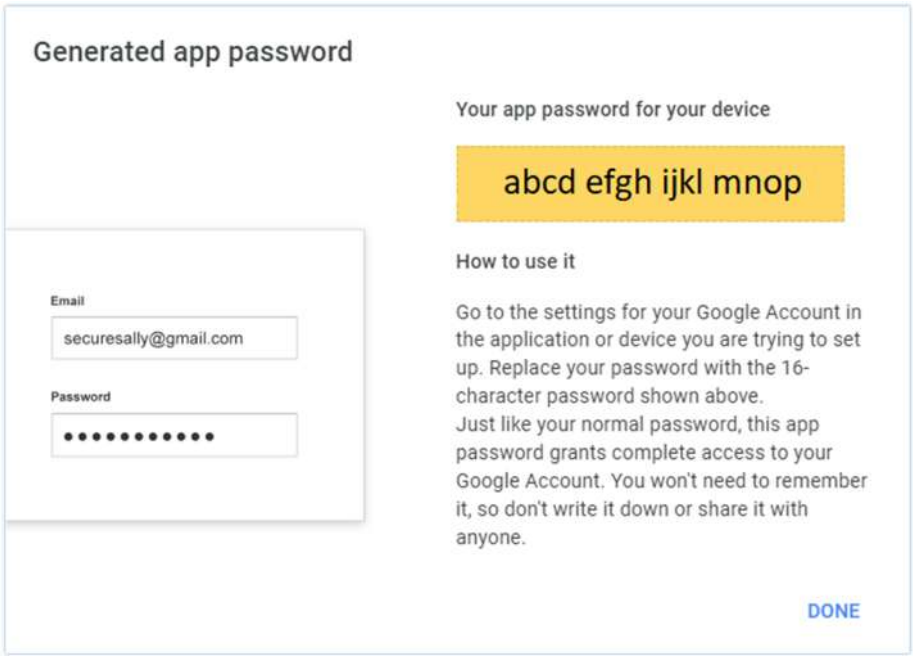
On the page for generating this special password, first select the application type (as the application type, select Other (Custom name) from the options offered)



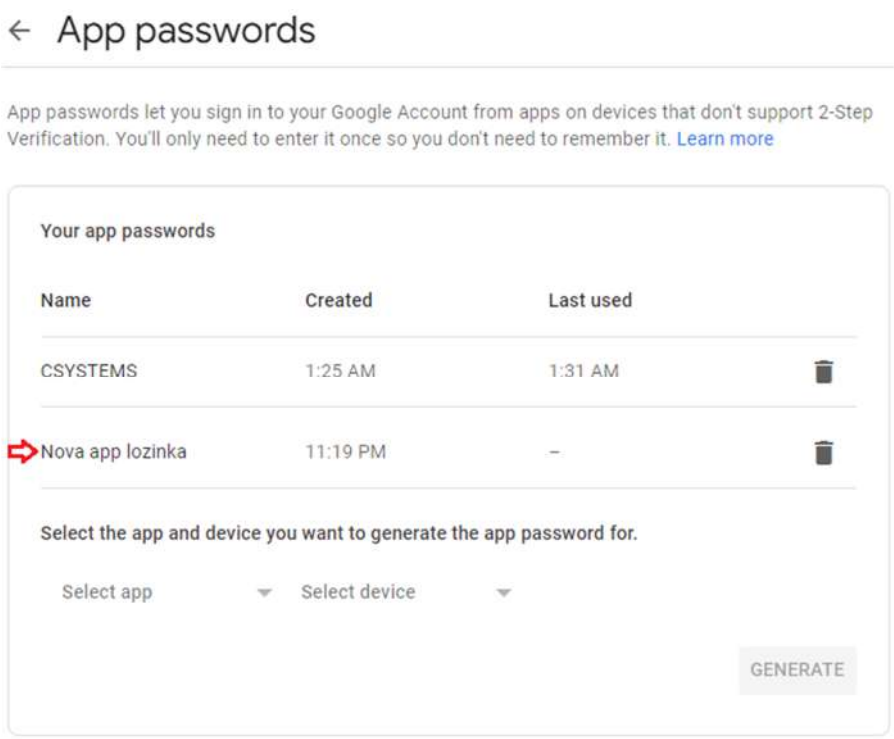
Then we enter a name of the application, for example **New app password** (Nova app lozinka) and then click on the blue GENERATE button



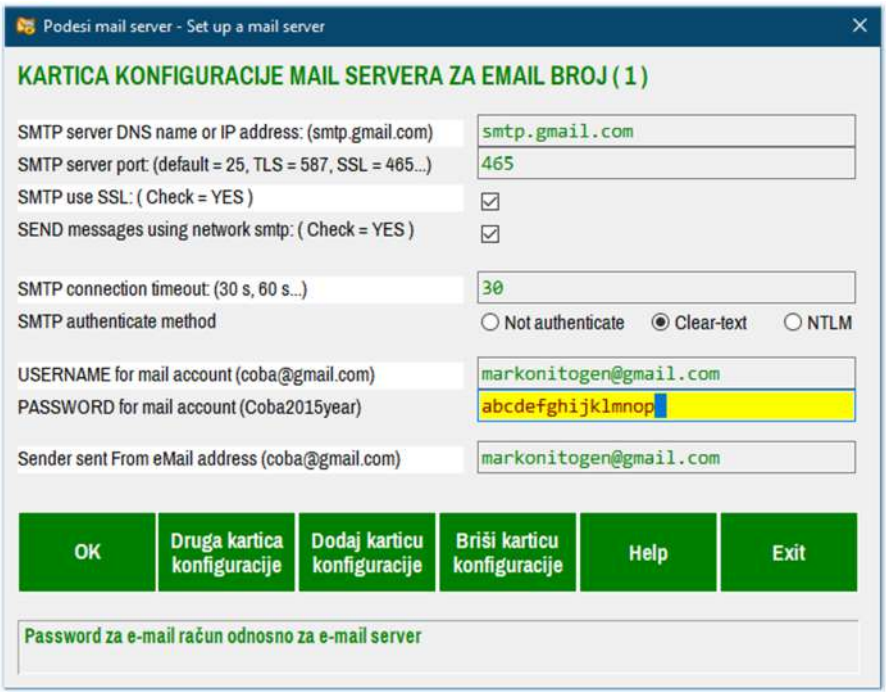
Next, a screen will appear with a new special password that should be copied into a TXT file and saved. After that, click on the DONE button in the lower right corner (the password is displayed in a yellow rectangle)



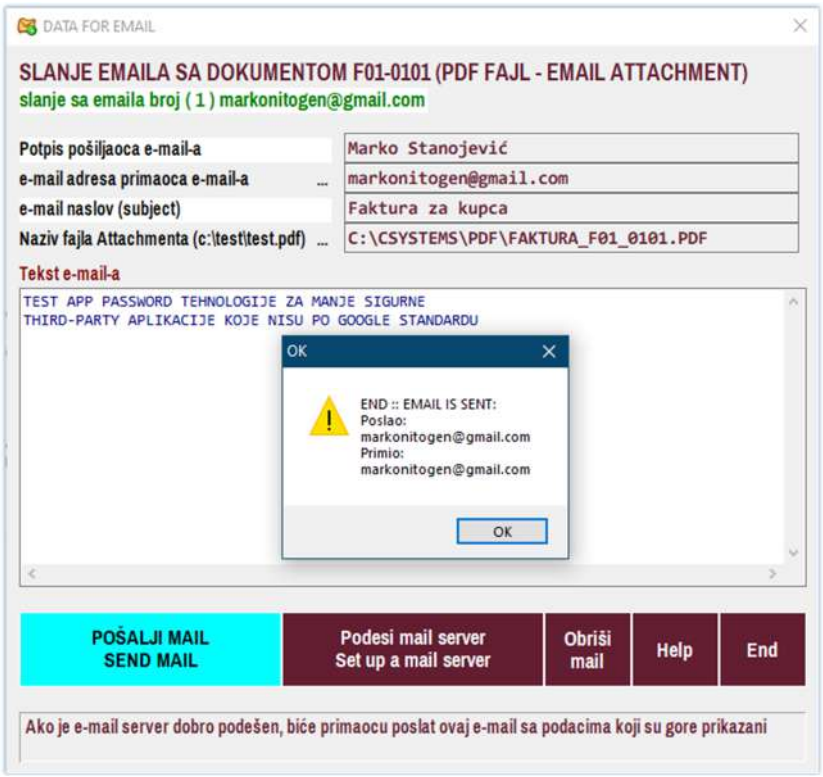
After that, we will be returned to the previous screen where we now see our password and information about it (application name, date of creation and date of last use). Here we actually see two passwords, one named CSYSTEMS that was created earlier and the one we created now, named **Nova app lozinka** (New app password).



Now that we have generated a new special password and previously set up everything so that it could be usable, all we have to do is simply replace the old password with this new one.
So, in our business application, it is necessary to REPLACE THE OLD PASSWORD WITH THIS NEW PASSWORD, and no other settings are needed in the program.



After changing the password, the program will be able to send emails without any problems (here is an example of sending one email and an accompanying invoice to one's own email address)



Especially important

The App Password option allows you to create an unlimited number of passwords and they have no expiration date.

I created those two (as in the instructions: Google App Passwords and Xbase++ developers.pdf) and I tried to send email from the program with both, and it worked with both.

Which means the following:

- Once created, the password has no expiration date

- Once the user enters such a password in his application (EXE program), it lasts and does not need to be changed, until the user himself wants to change it (first on the Google account, and then in the program)

- I tested sending emails with multiple passwords and it works, so there is no limit there either.

That App Password technology doesn't make much sense to me.

That password is the most common password that has no other purpose compared to the existing password except that Google knows that you had to protect your account a little better before that by forcing you to activate two-factor authentication.

And this password is proof that your 2FA is active.

And if you have 2FA active, then Google thinks you are safe and gives you this password so that you can access Gmail from one of your applications.

As you have seen, all other parameters for the Google mail server remain the same, the SMTP server and ports, and even your regular username, which is also your email address.

Marko Stanojević 29.09.2022

COBA
SYSTEMS SOFTWARE
www.cobasystems.com