


I'm not robot  reCAPTCHA

**Continue**

## Filetype xls username password gmail

Need to change your Gmail password? Or have you forgotten your login details? Whether you have access to email on your desktop, Android device, or iOS device, we have everything you need to know about changing or resetting your Gmail password. Google Gmail is one of the best email providers in the world, with over one billion users regularly checking their accounts. You can use Gmail either as a personal account or as part of a G Suite account that comes with Hangouts, Google Tasks, Google Keep, and Google Calendar — if you use Gmail for business as part of a team, you probably have the other one. However, using Gmail, losing access after forgetting your credentials – or being hacked due to a weak password – could have major implications for you personally and as a business. A secure password is the first step to protecting your account and data, and it's important that you update it regularly to ensure it's difficult to guess and is no longer used for all your other apps or accounts. Here are the best ways to change your Gmail password on p Computers, Android, and iOS devices. How to change gmail password on your computerFirst, open your Google Account in your internet browser - this will take you to the overview of your account. Then select Security from the menu on the left side of the screen. Under Sign in to Google, select Password and enter a new password (you may need to sign in again at this stage). Finally, select Change Password. (Image credit: TechRadar) It's also a good idea to add a recovery phone or email address if you lose access to your account in the future, so Google can contact you if it notices unusual activity associated with your account. To do this, go back to safety and scroll down to Ways we can verify that it's you. Select a recovery phone or recovery email, and then follow the instructions. Once you change your password, you'll be signed out of everyone except the following:Devices you use to verify that it's you when you sign in Some third-party apps that you've given access to your accountSmart home devices that you've granted access to your Gmail account On Android If you have an Android device, you can change your credentials through your device settings. First, open the Settings app, and then select Google &t; Manage Your Google Account. You can browse different sections at the top of your account report. Go to safety and scroll down to Sign in to Google. Select Password (you may need to sign in again here) and follow the instructions to change your password. (Image credit: TechRadar) Change your Gmail password on iOS If you're using Gmail with your iPhone or iPad, you'll need to open the Gmail app to change your password. In the upper-right corner of the app, tap your profile picture (or the first if you haven't set up a profile picture), and select Manage Google Account. At the top of the screen, tap Personal Information, and then under Profile, tap Password. Enter a new password and select Change Password. How to reset gmail passwordBorn Gmail password? Go to the Google Account Recovery page, where you'll be prompted to enter the email address and last password you remember for your account. If you don't remember a password, select Try another way and Google will send you a notification on your phone— that is, if you've added a recovery number to your account. If you haven't set up a recovery number, select Try another path again and Google will send you a notification to your recovery email address. I still can't get in there? Press Try another way again and you'll be prompted to answer the security question you selected when you opened your Gmail account. If all else fails and you don't remember the answer to the security question, press Try another way again. You'll then be asked to check your email account after 12 hours — during which time Google will try to verify that the account belongs to you. If Google can do this, you'll receive a link to reset your password. If you can't find the email, check your Spam or Bulk Mail folders and add a message to noreply@google.com. Choosing a strong password You should never use the same password for different apps - after all, if one account becomes compromised, you don't want a hacker to have access to all your other accounts because the credentials are exactly the same. If you're worried about remembering a lot of different credentials, the best password managers will do it for you – and many come with password generators that come for you with a strong password. If you're using Gmail for work, it's worth a look at the best business password manager. If you decide to choose your own password, be sure to use a combination of numbers, upper case, and lowercase letters to make it difficult to guess. Symbols like '!' or '%' are worth including, too, because they make your password even harder to guess. Enabling two-step verificationGoogle offers two-step verification for Gmail, which adds an extra layer of security to your account. Combining your email address and password is the first step to gaining access to your account — enabling two-step verification means adding a second step, making it harder for violators to access your account. This means that every time you sign in to Gmail, a code will be sent to your phone via text message, voice call, or Google Authenticator app. If you have a security key, you can insert it into your computer's USB port. (Image credit: TechRadar) To turn on this feature, follow the same steps as if you changed your password — but instead of selecting a password When you sign in to Google, select 2-Step Verification. Select how to receive the code and select Try Now. A prompt will be sent to your device, after which you will need to enter a backup option if you lose your phone or the desired second step is not available. Answer the prompt, and then you'll be able to turn on two-step verification. Two-factor authentication vs. Two-step verification: What's the difference? There is a security best practice where logins do not say the password is incorrect. Instead, you should say the username or password is incorrect. This best practice is. Stripe and GitHub logins, for example, follow this practice. The idea is if an attacker knows the username, he or she could focus on this account using SQL injections, crudely forcing password, phishing, and so on. Here's the problem. Stripe is a register page. Hell, you all know my username... I guess I'm fucked. Not to mention that you could just go to hacker must do is sign up to know if the username is valid or not. Why then bother with obfuscation signs in? Only the dumbest, most edging hacker is stopped username or password is incorrect login. You won't get any security, but your customers are losing clarity. Stripe has its submission form behind reCAPTCHA to prevent naïve scripts attacking their register. However this has been broken several times (1, 2) and will probably never be perfect. Even if reCAPTCHA was perfect, a hacker could manually verify their usernames of interest by trying to register, then automate the attack on the login page. To prevent attackers from knowing whether an account exists or not, they must have only an email address and provide no feedback in the User Interface if the registration was successful or not. Instead, the user would receive an email with information that they are logged on. An attacker might know if an account exists only if they have access to the target's email. In addition, that username or password incorrect is just bullshit. -Please say hello to @travisjeffery. Hit 📧 and share if you found it useful. Thanks for reading. Join Hacker Noon Create a free account and unlock your own reading experience. There is no need to panic about the nearly five million compromised Gmail passwords that appeared on the Russian bitcoin security forum this week, according to Google. Less than 2% of compromised username and password combinations work, Google's spam and abuse team said in a blog post late last night. They also say gmail automated anti-hijacking systems would block many potential login attempts. We protected affected accounts and required these users to reset their passwords, team members wrote in a blog post. phenomenon known in security circles as credential dumps - publication of lists of usernames and passwords on the web. We constantly monitor these landfills so that we can respond quickly to protect our users. Gmail is Google's free cloud-based email service that's integrated with Google Docs. Google responded this week to reports that hackers had gained access to the credentials of five million Gmail users. A combination of usernames and passwords appeared on Russian cybercrime forums. Peter Kruse, head of the eCrime unit at CSIS Security Group in Copenhagen, said Wednesday that most of the nearly five million stolen Gmail passwords are about three years old, although many are still legitimate and functional. He said CSIS experts suspect several hackers were collaborating, possibly using a compromise at the end point. Google was quick to note that its systems were not hacked. It is important to note that in this case and in other cases leaked usernames and passwords were not the result of google systems violations, Google's spam and abuse team wrote. Often, these credentials are obtained by combining other sources. John Shier, senior security adviser with British security company Sophos, said some Gmail users reported that their usernames and passwords were part of the dump and lent confidence when they claimed it was a legitimate Gmail credential. Doubts ensued after google's systems were hacked. Instead, the compromise probably stems from people being lax about using unique, powerful passwords. Let's say you want to create a new account on Reddit, he explained. It will ask you for a username and very often that username is your email address. And then you use the same password. Very often people use their Gmail address as their username for different sites – just to identify themselves. Google's team has the same theory. If you reus the same username and password across the website and one of those websites hacks, your login information could be used to log in to others, they noted. Or attackers can use malware or phishing schemes to intercept credentials. Shier pointed out that if hackers obtained usernames and passwords that people use in multiple locations, they could gain access to different aspects of a user's life. If you use the same password for Facebook and your bank account, it could lead to problems, he said. They could lock you out of your own account, or they could steal your identity. What should Gmail users do now? Security experts generally agree that this would be a good time for users to change their Gmail password and use strong passwords (that is, upper case, numbers, and punctuation marks). And don't use the same passwords for each web page and app. Two-stage if possible, it also adds an additional layer of security. Google also people update their recovery options so the company can reach you by phone or email if they are locked out of their accounts. Gmail users can access Google's list of security controls on this page. Don't panic, Shier said. If you change passwords and make sure your passwords are complex and you don't want to use them again, you should be in good shape. Copyright © 2014 IDG Communications, Inc.

