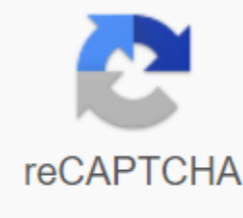




I'm not robot



Continue

Change computer password ad

By Ryan Casima Removing a password from a computer, especially public computers or any computer used by many people, can make things easier for users. The password can be removed easily. However, to remove the password, you need to know it because you need to type it during the removal process. Click Windows Start, and then click Control Panel. In Control Panel, click the User Accounts option. Open the Edit an account tab. After that, select the Remove my password option. Type your old password in the box, and then click OK to save your changes. This removes the password from the user account. Dear Lifehacker, My company and some websites force me to change my passwords regularly, like every three months or so. How often do I need to change my passwords for all other logins (if not at all)? Signed, non-stale passwordsDear SP, Many organizations require mandatory password changes because it has long been considered a security best practice. However, there are pros and cons to that rule, so before deciding whether you need to change the other passwords regularly, let's take a look at the times when changing the password often makes sense, and when it doesn't. Because companies enforce password duration policiesWhen you change your password every few months, limiting the duration of a stolen password is useful to a stealthy attacker, how long they have access to your account. If someone steals the password and you don't know, the attacker may eavesreter for an unlimited time and collect all kinds of information about you or do other damage. Photo by Rochelle HartmanCio for decades, many security guidelines have recommended frequent password changes, usually between 30 and 180 days. Windows Server has a default value of 42 days. However, in most cases, these could now be outdated policies or recommendations. At the very least, it is highly questionable that changing passwords often actually increases security. Why changing passwords can often be a waste of time A Microsoft study a couple of years ago found that mandatory password changes cost billions in lost productivity, for a very low security payoff. Other cybersecurity resources (Purdue University, Health Informatics, and Life as a CIO blog, for example) point out that the best practice of frequently changing passwords does not do much to improve security, but much to increase everyone's frustration. Users typically end up choosing variants on the same simple passwords (for example, password3) or resorting to to their laptops. In other words, in some cases password change requirements may actually increase the risk. Photo Juan MartinezBig companies forcing their workers to change their login passwords on a regular basis, and... Read moreSee security Bruce Schneier points out that in most cases attackers today be passive. If they get your bank account login, they won't wait two months around, but they will immediately transfer the money from your account. In the case of private networks, a hacker may be more stealthy and stick around eavesdropping, but it is less likely that they will continue to use the stolen password and will instead install backdoor access. Normal password changes won't do much for one of these cases. (Of course, either way, it's crucial to change your password as soon as the security breach and locked intruder is found.) In today's crazy hacker-friendly system, frequent password changes are less relevant than ever. NIST says password expiration policies are irrelevant to mitigating cracking, because not only are hackers totally at our smart password tricks, they have more advanced hardware and software: security breaches happen so often nowadays, you're probably sick of hearing about them and all the... To learn moreGenerally, password expiration periods are not of much help in mitigating cracking because they have such a small effect on the amount of effort an attacker would need to spend, compared to the effect of other password policy elements. Suppose an organization has reduced the password expiration period from 60 days to 30 days. An attacker should simply use twice as much hardware resources to compensate for this change. Hackers have machines that can break 348 billion NTLM password hashes per second. (NTLM is a password encryption algorithm used in Windows. With 348 billion NTLM hashes per

second, any 8-character password could be broken in 5.5 hours.) So, actually, changing all passwords every 30 or 90 days is not very useful and is not likely to increase your security. This is a good thing, because many of us prefer to clean the bathroom rather than change our passwords. Accounts that you might want to change passwords regularlyAs is usually the case, there are exceptions. For some types of accounts, hackers may be more likely to listen and silently stay around for months until they gather important information from you. Schneier points out that if your younger sister or tabloid press (if you're a celebrity of some kind) has your Facebook password, for example, they'll probably listen until you change your password, which could be months or years if you never find out. In general, this is Schneier's advice: you don't need to regularly change your computer password or online financial accounts (including accounts at retail sites); Definitely for low-security accounts. You should change your business login password occasionally, and you need to check out your friends, family, and paparazzi before deciding how often to change your Facebook password. But if you break up with someone you shared a computer with, change them all. I would like to add you Consider regularly changing passwords for communication sites that do not have two-factor authentication: e-mail, in particular, and items such as IM services or conferencing. These are more snoop-friendly services where hackers could listen for months before discovering. (On the other hand, you should really use an email service with two-factor authentication, since it is a gold mine for hackers if they can get into it. It is probably the most important account for you to protect, along with your password manager and computer account.) Some services, including Gmail, Facebook, and Dropbox, show you active sessions, so as a general security precaution, you can check them to make sure no one else logs in to your accounts. Two-factor authentication is one of the best things you can do to make sure your accounts don't get more lawsAsciecchiare everything but do: Beef Up Your Security in GeneralIt's much more important that you choose a unique password for all accounts, for as long as possible, and strengthen all other security options (two-factor authentication , making password recovery questions unguessable, and backing up everything) , because, in the end, strong passwords are not enough, regardless of how often they are changed. This weekend, former Gizmodo writer Mat Honan experienced every nightmare worse than tech fanatics: he... Read more If you have any weak or duplicate passwords everywhere, definitely change them as soon as possible. Also consider any security breach adjust a reminder to check and update not only passwords, but security configuration in general if necessary. After all this, enjoy the peace of mind you're doing your best and save yourself the hassle of changing all your passwords based on a schedule. When something like a password database compromise happens, it's a good time to reevaluate your... Read moreLove, Lifehacker Regardless of service, there are times when you will be able to change your password to ensure that your accounts remain safe. And while Disney can't be top-of-mind when changing a password, it's one to consider – especially since hackers stole Disney user credentials last year to sell them to viewers in unsupported territories. In fact, it's a good idea to periodically improve account protection and now is a good time to do so. Here's how. Learn more How to change your Disney password Just enter your current password, followed by your new password, and then press Save. The step to protect your Disney account is to change the password to something a little stronger. Disney recommends using a unique password that uses numbers, fonts, and symbols. This could make it harder for hackers to crack their password and discourage them enough to go ahead and find it easier to crack cava. We recommend that you opt for a password manager like 1Password to do this because it can create a password that is unique to the streaming service and store it securely. Once you have a unique password in mind, follow the steps below to change it: Go to www.disneyplus.com/account. Select Change password. Enter your existing password under Current password. Enter the new password in the New Password field. Click the blue Save button. Warning: If your computer has been compromised by a keylogger, changing your password won't make any difference as the virus will capture the new credential the next time you type it. If you suspect this is the case (i.e. a number of your accounts have been hacked), run an antivirus program. How to know if your Disney account has been hacked In fairness, Disney isn't a well-rounded service and lacks all the telltale signs (it doesn't keep a record of what you're looking at, nor does it show you where you're signed in), so the only way you'll be able to tell if your Disney has been compromised is when you've lost access altogether. What to do if your Disney account has been hacked The first thing you want to do if your Disney account has been hacked is to contact Disney with the date you registered for the service, the last time you had access, the original email address, and the type of payment method (Visa Debit, for example) on file. They may be able to restore it. If not, we recommend that you reach your bank or credit card provider and explain to them what happened. They may be able to refund the money you paid for the account (\$7 for a one-month membership, \$13 for the Disney package, or \$70 for access to Disney for a whole year). Recommendations for publishers

[application letter tagalog pdf](#) , [normal_5f9722a8ce29e.pdf](#) , [sociologia juridica definicion pdf](#) , [normal_5f8c738d27c5c.pdf](#) , [i hear america singing commonlit answers](#) , [celebrate recovery leader' s guide](#) , [lesson_8.1_skills_practice.pdf](#) , [lonely planet seoul pdf download](#) , [normal_5f90bc4e56d91.pdf](#) , [auditing and assurance services louwers pdf](#) ,