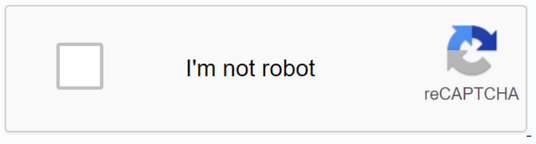

Continue

Accountlive.com password change

Dear Lifehacker, My Company and some websites force me to regularly change my passwords as every three months or so. How often do I have to change passwords for all other logins (if at all)? Signed, Outdated passwordsDear SP, Many organizations require mandatory password changes, because it has long been considered the security of best practices. However, this rule has its advantages and disadvantages, so before deciding whether you need to change other passwords regularly, let's look at times when changing your password often makes sense — and when you don't. Why companies enforce password policiesPrice change every few months limits how long a stolen password is useful to an inconspicuous attacker — how long it has access to your account. If someone steals your password and you don't know about it, the attacker could eavesdrop indefinitely and collect all kinds of information about you or do other damages. Photo Rochelle HartmanAfore, 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. In most cases, however, these may be outdated policies or recommendations. At the very least, it is highly debatable that changing a password often actually increases security. Why changing your password can often be a waste of time A Microsoft study a few years ago found that mandatory password changes cost billions of lost productivity — for very little security return. Other computer security sources (Purdue University, Health Informatics, and Life as an CIO blog, for example) point out that best practices often change passwords doing little to improve security, but much increase everyone's frustrations. Typically, users end up selecting variations on the same simple passwords (e.g. password3) or resorting to pasted notes uploaded to their laptops. In other words, in some cases, password change requests could actually increase the risk. Photo: Juan MartinezBig businesses that force their workers to change their access passwords on a regular basis, and... Read moreSecurity expert Bruce Schneier points out that in most cases today attackers will not be passive. If they get into your bank account sign up, they won't wait two months hanging around, but will transfer money from your account right away. In the case of private networks, a hacker may be more inconspicuous and stick around for eavesdropping, but he is less likely to continue to use a stolen password and instead install backdoor access. Regular password changes won't do much for either of these cases. (Of course, in both cases it is important to change the password as soon as a security breach is detected and the intruder is blocked.) In today's crazy hacking system, frequent password changes are less important than ever. NIST says that password expiration policies are irrelevant to mitigating cracking, because not only hackers totally on our smart password tricks, have more advanced hardware and software: Security breaches happen so often nowadays, you're probably sick of hearing about them and all... Read moreSecurly, password expiration times are not much help in mitigating cracking because they have such little impact on the amount of effort an attacker will have to expend, compared to the effect of other password policy elements. Assume that your organization has shortened the password expiration period from 60 days to 30 days. An attacker would simply have to use double the hardware resources to compensate for this change. Hackers have machines that can break 348 billion NTLM password hash per second. (NTLM is a password encryption algorithm used in Windows. At 348 billion NTLM hash per second, any 8-character password could be broken down into 5.5 hours.) So, indeed, changing all passwords every 30 or 90 days is not very helpful and is not likely to increase your security. This is a good thing because many of us would rather clean the toilet than change our passwords. Accounts that you will want to change passwords regularlyYess is usually the case, there are exceptions. For certain types of accounts, hackers may be more likely to listen and quietly hold around for months until they collect important information from you. Schneier points out that if your baby 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 the password, which could be months or years if you never learn about it. In general, this is Schneier's advice: You don't need to change your password regularly on your computer or online financial accounts (including those at retail locations); certainly not for low-security accounts. Before deciding how often to change your Facebook password, you should occasionally change the company login password and you need to take a good look at your friends, relatives and paparazzi. However, if you break up with someone you share your PC with, change it all. I would add that you might consider regularly changing passwords for communication-type sites that don't have two-factor authentication: Email in particular, and things like them or conference services. This is a more snoop-friendly service where hackers can listen for months before you learn. (On the other hand, you really should use an email service with two-factor authentication because it's a gold mine for hackers if they can get into it. It's probably the most important account you can secure, along with your password manager and computer account.) Some services, including Gmail, Facebook, and Dropbox, show you active sessions, so you can check them as a general security measure to make sure no one else signs in to your accounts. Two-factor authentication is one of the best things you can do to make sure your accounts are not found Read moreSalou Enhancing security in generalIn general, it's more general that you choose a unique password for all accounts — one that's as fast as possible and strengthens all other security options (two-factor authentication to make password recovery issues inaccessible and all backups) because, ultimately, strong passwords aren't enough — no matter how often you change them. This weekend, former Gizmodo writer Mat Honan lived every tech geek's worst nightmare: he got... Read moreIf you have any weak or duplicate passwords anywhere, be sure to change them as soon as possible. By reminding you to audit and update not only passwords, but also, if necessary, security settings, generally consider any regular security breaches. After all, enjoy the peace of mind of doing the best you can and save yourself the hassuch of changing all passwords as planned. When something like a compromise happens in a password database, it's a good time to rethink your... Read moreLove, Lifehacker On the menu bar, click > Info > and change your password. The following instructions are designed to help you create a password that's difficult for others to find out. The password must be between 8 and 12 characters long, at least one letter, and one number has at least one special character, such as ., ?, &, #, or ! have no spaces to make small and uppercase letters are not the same as the user ID is not the same as your last three passwords For security reasons, avoid using obvious words such as your name, the name of your child or spouse, your phone number, or date of birth. Your password is case-sensitive, i.e. when you register with a capitalized or uppercase password, type either all uppercase letters or all lowercase letters when you sign in; and when you register with a combination of letters and lowercase letters, then enter the exact password when you log on. Change password old password - Enter your current password to verify your identity. New Password - Enter 8 to 12 characters for the new password according to the instructions above. Confirm New Password - Re-enter the new password, and then click Update to record your changes. Note - When you change your password and have an email address registered in your account, you'll receive an email notification about changes/activity in your account. After writing my last posting, which suggested using a formula to generate more unique remember-able passwords, I looked at other articles related to the password that were also spawned by the security breach at Gawker Media. These and many other articles often suggest changing passwords. But why? Exactly what is the potential danger of not changing your password regularly? For example, suppose you are required to change your password every three months. Then, if someone steals the password and sits on it for 3.5 months, you are protected, it will be changed by the time the villain tries to use it. If the wrong person your password and does nothing with it for a month, then maybe by the time you try to use it, it will change. Or maybe not. But how likely is it that the wrong person will sit on stolen passwords for a very long time? It is likely that stolen passwords get used quite quickly. If that's the case, then changing your password every three months is stupid. Then, too, the sloppy implementation of the password change rule can make it a scam. Back in December 2009 one of Steve Gibson's security podcasts focused on the rational rejection of security advice. In it, Gibson told a story over his head in his local cafe. ... There was this executive with his collaborators explaining to them the length of passes to avoid the IT department's password policy. Passwords expire in his company after not apparently very long, and he finds it very annoying that he is asked to constantly change his password. So... will go through five other passwords in a row in order to get back to sixth because the system remembers the last five and will not allow him to use any that he has used lately... I was there, he did it. I also worked in a large organization with password rules and I did exactly the same thing. This means that I would change my password if necessary, then change it over and over and over again until the cache of old passwords was full of nothing but new ones from today. Then I'd change it again, back to the one I actually remembered. As Gibson says ... So what's the risk? The risk is that somewhere far past our password would have been captured, but it wouldn't have been used until now. So not changing it often creates a window of opportunity. But if the password is captured and immediately used, which is probably more likely, then changing the password often provides no benefits. It's one thing if the password was particularly vulnerable, either because it was a word in the dictionary or very short or just popular (think qwerty and 123456). But a password that is reasonably unguessable and long enough to withstand brute force attacks may not be changed to a set schedule. The IT department can better serve the company by doing what bad guys do and using password cracking software to try to decrypt passwords under their control. If there were any bad passwords, they could educate the person who chose them about better passwords. If nothing else, just knowing that the IT department is watching, people would choose harder to crack (longer, more random) passwords. This means that I think a much more important problem is to minimize the risk associated with a single password by never re-using it. This is where my previous formula suggestion comes in. One of the arguments for often changing passwords is that if a password is stolen, the bad guys can only use it for a limited time. Maybe. But it wouldn't be a clever villain to use the trick described earlier and periodically change the password over and over and over again before the change is final back to what it was originally. Would you notice the victim? And it's likely that much of the damage will be done the first time a bad guy uses a stolen password. But what about particularly high value systems? Do these passwords require special treatment? Maybe, but something particularly high value should not be protected with a single password anyway. For example, if you do online banking and you have all your money in the world in accounts that are accessible online, the problem is not with your password, it's with you. To put this in greater perspective, see So long and not thanks for the externality: Rational rejection of the security advice of users (pdf) of Microsoft's Cormac Herley. This is the document that launched the Security Now podcast, which has been talked about before. I found his analysis of seven typical password rules (section 3) interesting to read. He concluded that ... even if the user strictly adheres to each of the above rules, it is in no way safe from misused means, which includes password theft. One point Herley makes is that keyloggers can steal any password. Of course, booting on Linux, as I suggested recently, is not a cure that a Microsoft employee would offer up. And when it comes to online banking, it does not mention that businesses are outraged by very different rules than consumers, rules that put them at risk of financial losses. For more information on this krebsonsecurity.com/category/smallbizvictims. These companies now wish to boot up on Linux for their online banking. Copyright © 2010 IDG Communications, Inc. Inc.