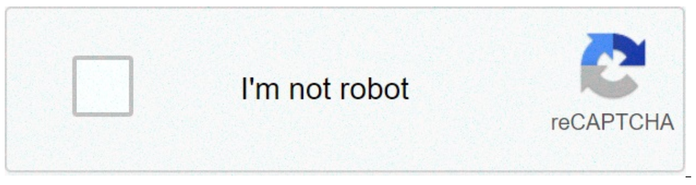

Continue

Breaking pdf password

Interested in Infosec & Biohacking. Security Architect by profession. Love reading and running.“Treat your password like your toothbrush. Don’t let anybody else use it, and get a new one every six months.” — Clifford StollWe use keys to unlock doors and use locks to protect our private properties. In the digital world, we do the same. While keys have many “forms,” the most common one is still the password.Passwords have been used as the foundation of authentication for years. While passwords are still a large portion of our cyber landscape, they have been on the decline for more than a decade. But eventually, we will face a time when the password is no longer proof of our digital self.Principally, using a password to get access to a system is a method of authentication. According to (ISC)² CBK | Common Body of Knowledge — ISC2, authentication is when the user provides a credential to the system to prove the identity. Authentication factor can be of the following types:Something you AARESomething you HAVESomething you KNOWUsing a password is an example of Something you KNOW. It is a mechanism of having one factor of authentication. A system relies on a secret that the login users must memorize and exhibit to prove their identity. This case may seem straightforward enough, but it has profound implications.The Problem with PasswordsSimple authentication methods that solely require username and password are intrinsically vulnerable. Attackers could guess or steal credentials and gain unauthorized access to sensitive information and systems using various techniques, including:Brute force attacks — using programs to generate random username/password combinations or exploit weak passwords like “123456.”Phishing — using fake emails or text messages to trick a victim into replying with their credentialsMan-in-the-middle attacks — intercepting communications traffic (over public WiFi, for example) and replaying credentialsCredential stuffing — injecting stolen or leaked credentials from an account to log in to other accounts that belong to the same user (people often use the same username/password combination for multiple accounts)Keylogging — installing malware/ hardware on a computer to capture username/password keystrokesPassword FatigueToday, we all rely on various apps to perform our jobs. By that, we are forced to memorize and track all the login credentials for each one of them. Moreover, changing passwords frequently is tiring for us in front of a computer.Flooded by password sprawl, users take risky alternatives like applying the same password weak passwords, repeating passwords, or posting passwords on sticky notes.Bad actors can take advantage of the loose cyber hygiene practices in password management to install cyber-attacks and data theft. Compromised credentials to get unauthorized access is a major cause (80%) of data breaches.Why Passwords Die HardFor years, the security industry has been producing multiple authentication alternatives to substitute passwords as the norm. These solutions span the technological spectrum:Something you HAVE:Proximity badges, physical tokens, or USB devices (FIDO2-compliant)Software tokens or certificatesA mobile phone application (SMS, One-Time-Code (OTC))Something you ARE:Biometrics — Fingerprint, palm, voice or facial recognition, or retina scanningBut the question is, with so diverse, considerably more secure choices available, why are passwords still around? Three drivers are retaining passwords from exiting the stage.1# Cost — Password is CheapMost applications and online tools now come preset with password-based authentication by default. Companies let their networks and IT departments set up to support this system of identity management.Renovating authentication protocols often need time and a substantial initial investment. For example, using security tokens as an alternative requires purchasing and distributing physical/ software devices to all users.2# UX — User Likes RoutinesUsers get used to the way password authentication works and made passwords part of their routines. Putting a new form of securing digital identities is often met with resistance. Training or education program is required to deploy the alternatives for password successfully.3# Not Everything Can Start Over or RebootIf your password is stolen, you can reset it immediately to prevent further damage. But for the others, it may not be the case. Say your fingerprint data was stolen online. You can only use another finger for authentication in the future if you revoke the first one.The physical token also needs to return it and map a new one to resume your authentication. That is why, ultimately, the password is the fallback plan for most of the applications.The Future-ready AuthenticationA password-free authentication that would become the replacement should be ready to tackle the three drivers. To simply put, it should be cost-effective and easy to use.Passwordless AuthenticationFirst, with passwordless authentication, there are no passwords to memorize or security question answers to remember. As a result, users would not have password fatigue. Unlocking your phone with your fingerprint is faster and easier than type-in the password. Besides, the complexity of your fingerprint data is natively higher than the 8-digits password.Moreover, to enhance security further, multi-factor authentication (MFA) is often deployed in conjunction with passwordless authentication. For example, when you log in to a web application online and prove your identity using a biometric method on your phone, you are using MFA at once:Something you ARE — fingerprint or facial recognitionSomething you HAVE — your mobile phonePush-based AuthenticationThis password-free, mobile-based system, ordinarily in downloadable apps, does the authentication automatically, only requiring the user to respond to a secured push notification.Also, push harnesses the user’s mobile phone as an authenticator, meaning that no secondary devices are required. You’ve probably seen that Google provides push-based authentication for Gmail.Adaptive AuthenticationThe latest MFA solutions support adaptive authentication methods. That is the one using contextual information, including location, time-of-day, IP address, device type, and business logic, to decide which authentication factors to apply to a particular user in a specific situation.Adaptive authentication balances practicality with security. Let say an employee is allowed to work from home for a period. And he accesses the company network from one external location consistently from his home address. The first-time login could be a combination of multifactor authentication and activity monitoring for IAAA purposes.But later on, the authentication process could “step down” to simplify his/ her daily workflow. That user would be under supervision, but he can focus on his work instead of remembering various login secrets.In another scenario, an employee accessing an enterprise application from a trusted machine might be required to provide only one authentication method. However, to access a foreign country's application over an untrusted WiFi connection, the user might also enter a token code as supplementary (step-up).Final WordsPasswordless Authentication provides a variety of practical and business benefits.Improve user experiences — by eliminating password and password fatigue.Strengthen security — by eliminating bad cyber hygiene of password management and reducing the risk of credential theft and impersonation.Today, with the risk of a data breach and identity theft firmly in public awareness, organizations and individuals alike will have to start thinking more seriously about supporting their authentication.Companies and users need to understand that while passwords are becoming more obsolete by the day, there are robust, user-friendly options for replacing this outdated method.Before that day comes, you can learn more about how to create a strong but memorable password from my previous HackerNoon post.Thank you for reading. May InfoSec be with you🖖.Also published here.Join Hacker Noon Create your free account to unlock your custom reading experience. Photo Illustration by Elena Scotti/Lifehacker, photos via Shutterstock The U.S. government recently revamped its password recommendations, abandoning its endorsement of picking a favorite phrase and replacing a couple characters with symbols, like c4tlo^eR. These short, hard-to-read passwords look complicated to humans but very very simple to computers.Instead, you want long, weird strings that neither computers nor people can guess. Humans are bad at coming up with these—we all pick the same “random” words, and we’re bad at remembering actually random strings. Follow this guide to make good passwords, or better yet, let an app make and remember them for you.Make your passwords very longYour enemy isn’t some guy in a ski mask trying to guess your password one try at a time. It’s a program that automatically runs through massive databases of common passwords or random combinations of characters.The best answer to that is a very long string of words. As the webcomic xkcd famously pointed out, a bunch of plain words is pretty good. But as many hackers use “dictionary attacks” to guess regular words, it’s best to add some capital letters, special characters, or numbers.Don’t use a common phraseBut don’t use the same bunch of plain words as everyone else. If your password consisted of the entire script of Hamlet, it would still be unsafe if everyone else had the same password. “When in the course of human events” is a shitty password. So is a famous movie line, or a Bible verse, or even an acronym of a Bible verse.As we’ve established time and again, your clever tricks aren’t protecting your password. If you or…Read moreAnd don’t get clever with thematic or personally meaningful passwords. Sometimes humans do try to crack passwords, so don’t help them out by using your son’s birthday or the phrase printed on your favorite coffee mug.Test your passwordIf you use a password manager, it’ll test your password in real time, on the safety of your computer. The sites How Secure Is My Password?, How Big Is Your Password?, and How Strong Is Your Password? test if your password is long enough. But they won’t warn you about common guessable phrases, like those Bible verses.Of course, typing your passwords into unfamiliar sites is a bad habit. These sites are safe, as they’re all publicly run by trusted developers who promise that your entered text never leaves your computer. Still, to be safe, just use these sites to get the gist before you make your real password.Don’t reuse your passwordWhen your password on some web service gets hacked (and it will), you’d better hope you didn’t use the same password on three other services. Don’t use a weak password for services that “don’t matter,” because some day you might give one of those services your credit card info, or use it to authorize more important services, and you won’t think to beef up your password.Yahoo has confirmed that information from at least 500 million user accounts was stolen in 2014….Read moreUse a password managerUntil you do this, no matter how hard you try all the rules above, you will keep picking bad passwords. Here’s how:Your “random” string of words will be something like “monkey dragon baseball princess,” four extremely common password words, and a computer will guess it.You’ll pick something memorable, which will limit your options, and a computer will guess it.You’ll manage to make a password a computer can’t guess, and you’ll forget it, and you’ll have to replace it with a weaker password, and a computer will guess it.You’ll pick something identifiable to anyone who follows you on Twitter or Facebook—like your dog’s name—and a human will guess it.Internet standards expert, CEO of web company iFusion Labs, and blogger John Pozadzides knows a…Read moreInstead, get your computer to make and remember your passwords for you. This is the only reliable but convenient way to manage the vast quantity of passwords that modern life requires.The current best in class is 1Password. If you don’t care about the detailed differences between managers, just grab this one and follow Lifehacker’s setup guide.Using a password manager is basically internet security 101 these days, but that doesn’t make them…Read moreThere are several other fantastic, full-featured password managers for Windows and OS X, beloved by Lifehacker staff and readers. All these apps will create and remember your passwords. And all of them tell you how secure each of your passwords are. Some even alert you when the services you use get hacked, whether or not you were personally exposed. You have a ton of options for password managers, but when it comes to your security, you want the…Read moreOf these top picks, the most distinctive is the open-source KeePass. It focuses on local storage rather than cloud solutions, and it even lets you use a file to unlock it, so you could turn a physical thumb drive into your “password.”Cloud-based services like 1Password and LastPass are more vulnerable to remote attacks. But because they heavily encrypt your data and don’t store your master password, you’re still safe even if those services are hacked—as long as your master password is too hard to crack. (You can also sync your encrypted password file with Dropbox or Google Drive; a hacker would still need your master password to unlock it.)You know you’re supposed to use a password manager. In fact, you’ve been meaning to set one up for…Read moreYou just need to remember one password: The one that locks your password manager. Follow all the rules above to create a strong master password, especially if you sync your data. Otherwise, if your password service ever gets hacked, the hackers will also guess your weak master password, and they will swim around in all your accounts as in a silo of Scrooge McDuck money.Now if you just have to write that master password down, do it on paper, and keep it somewhere safe like your wallet. Don’t write “MASTER PASSWORD” on it. Rip it up as soon as you’ve memorized it (which will take just a day or two, thanks to the muscle memory of typing it in every time you log into anything).Don’t forget your master password, or you could be completely and utterly screwed.Using a password manager is smart security. That’s nothing new. However, the best password managers Read moreDon’t store passwords in your browserThose can get hacked, too. Some of Opera’s saved passwords were partially hacked last year. Even Google accounts are vulnerable. A hacker doesn’t have to defeat Google’s security—they just have to trick you, and it’s a lot easier for hackers to pose as Google and request your login than it is for them to pretend to be your chosen password management app. If your Google account gets hacked, you’ll be in enough trouble without also worrying about all your saved passwords.Follow the rules every timeOf course, your bank, your doctor’s portal, and your library are still following the outdated security recommendations, so they’ll still force you to follow weirdly specific rules for password creation, like making you start with a letter or include one symbol. (Ironically, by lowering the number of possible passwords, these rules make them easier to crack.)First generate a random, secure password with your password manager. Then amend that password as minimally as possible to comply with the service’s specific rules. Do your password editing inside your password manager, so it can alert you if you’re turning a strong password into a weak one.We’ve covered how to create a memorable password if you absolutely have to. But since all our recommended password managers offer mobile apps (KeePass recommends certain third-party mobile ports), you can save your password anywhere you go. There’s just no reason to make up your own password.Use two-factor authenticationWhile it isn’t foolproof, two-factor provides a layer of security for only a minimal loss of convenience. But not all two-factor is equally secure. Dedicated authentication apps are a lot safer than just getting a code over SMS. But both are safer than a password alone.Two-factor authentication is one of the most important ways to protect your accounts. However,…Read moreDon’t ruin all this by using security questionsSecurity questions? More like insecurity questions! I’m fun at parties. Point is, the concept of security questions made some sense when they were used in 1906 and answered face-to-face, but they’re ludicrous now that anyone can Google up your mother’s maiden name, where you went to high school, or your favorite ice cream flavor, then call Amazon tech support and pose as you.A few security-conscious web sites allows users to write their own security questions, and web…Read moreTreat security questions basically the same way you treat your passwords: Make up fake answers, and save them in your password manager. Security questions are for talking to humans, not computers, so you don’t have to add weird characters to your answers. Instead, you want to pick wrong and uncommon answers. What high school did you go to? Scoobert Doobert High. What’s your mother’s maiden name? Blempgorf. This is where you can put all that clever energy that you’re not allowed to put into your passwords. (It’s also a decent strategy for picking that one master password that you have to memorize.)Remember, everything is brokenPasswords are bad and dumb. But so is everything else. Fingerprints can be stolen, two-factor texts can be rerouted, keys can be copied. As tech reporter Quinn Norton put it, everything is broken, and as writer/programmer Dan Nguyen put it, everything is (even more) broken. Security technology is a race between the good guys and the bad guys, and it’s just impossible to have perfectly secure technology without sacrificing many of that technology’s benefits.So once you’ve set up your password manager, replaced all your passwords, and enabled two-factor authentication, don’t think your work is done. Some day everything will move onto a new security system, and you’ll have to adapt. That’s the price we pay for putting our lives online.