Dear Readers,

**Welcome to the 21st Century and the Curse of Passwords.**

**Anyone who uses a computer, be it a desktop, laptop, iPad or cell phone is living a life of misery. We must all use passwords to provide some protection from outsiders accessing our emails, files and financial accounts. They need to be unusual, so that others cannot guess our chosen passwords, and since we all must use at least a half dozen different passwords for different applications, the human mind cannot devise strings of characters that are possible to be recalled, but not easy for others to discover.**

**Unfortunately, we must make passwords others cannot guess, but because we all need to use a dozen or more passwords for different applications, it is extremely difficult to not use certain patterns that we can recall so that we can continue to access different applications we must use.**

**Our worlds get seriously upsetting when we must regularly change passwords, and make them sufficiently different so that others who know you, or can access your use of passwords, will be able to figure out your repeated strings of symbols that help you recall your new passwords that are changed periodically for security reasons.**

**For many of us seniors who have problems with memory, passwords and changing passwords that are secure (that we can remember) poses anger and anxiety for most of us. We should note that it will also be a pain and headache for everyone who survives to be a senior who continues to use a cell phone, or iPad, or any type of computer.**

**The use of a convenient notebook to record all your passwords and changes made, can make life less stressful and positive for everyone's life. Do it, if you know what's good for you.**

===========================================================

**SOURCE:**

**Password Policies Make Us Less Secure**

**Mandating frequent password changes and requiring special characters reflect outdated thinking**

**Does your company network or a website you frequently visit force you to come up with a new password because it has declared your old one is past its expiration date?**

**If you find that annoying, you’re not alone. What’s worse: It’s actually bad for cybersecurity, say researchers.**

**The scheduled-replacement policy is one of a number of poor password practices that make logging into sites, apps and services more of a pain than ever.**

**We’re not just talking about issues with government and corporate IT systems. Companies and services including Apple, Microsoft, Instagram and LinkedIn, among others, all have less-than-optimal password policies, according to a recent paper by researchers at Princeton University.**

**These password policies can increase the chance that individuals’ accounts can be breached, especially if the users aren’t using additional means of securing their accounts, such as two-factor authentication, says Arvind Narayanan, a professor of computer science at Princeton and one of the authors of the paper on bad password policies.**

**Compelling routine password changes, for example, actually tends to make people more likely to choose weak passwords in the first place, according to numerous studies. Another flawed practice is to limit the combinations of characters one can use in a password, or compel users to include special characters in their passwords. It turns out those rules don’t generally lead to more secure passwords, either.**

**Human nature**

**Lorrie Cranor, a professor of security and privacy technologies at Carnegie Mellon University, is somewhat unusual in the cybersecurity field, in that her research is as much about human behavior as it is about the tech we build and use. By looking at how regular people actually respond to the cybersecurity policies—including password rules—set by organizations, she’s discovered a few basic facts about most of us.**

**At the risk of oversimplifying, they are: When it comes to cybersecurity, people are smart, but lazy. We are also, it turns out, remarkably predictable.**

**Mix all of these traits with cybersecurity policies that are well-intentioned, but focused on rules rather than outcomes, and the result is a potential bonanza for hackers, who can exploit the weak passwords and other bad security habits that result.**

**The widespread policy requiring regular password changes goes back decades. The original idea was that if a password were breached, a periodic reset would shut an attacker out of a system.**

**But when forced to update their account passwords regularly, people tend to choose the simplest possible password the system will accept. They will also do things like modify their existing password in some entirely predictable way, such as incrementally increasing a number on the end of it, says Dr. Cranor.**

**Hackers know all these tricks, in part because the web is full of databases of stolen passwords.**

**Dr. Cranor began urging companies to stop asking users for regular password changes in 2016, when she was the chief technologist at the U.S. Federal Trade Commission. And in 2019, Microsoft stopped recommending that IT administrators mandate periodic password resets, calling the practice “ancient and obsolete.”**

**And yet this policy persists. One reason is that if you’re in charge of security at a company, adding more rules and restrictions looks good to bosses. If you take away such rules, company leaders may question whether that’s wise, says Dr. Cranor. Another issue is that official guidelines from the National Institute of Standards and Technology, which are treated by many as the gold standard for cybersecurity policies, didn’t stop recommending regular password resets until 2019.**

**Passwords vs. AI**

**Recently published work from researchers at several Chinese universities and the University of New South Wales in Australia has shown that new generative artificial intelligence is now so good at guessing what tweaked passwords we’ll come up with that our habit of using slightly modified passwords could become nearly as big a threat to our cybersecurity as reusing passwords.**

**By now almost all of us have passwords that have been made public in a breach, so determined hackers already have a good idea that your favorite password to reuse with slight modifications is, say, your pet’s name.**

**Stop using these passwords**

**Another common sin of corporate password policies—including those set for consumers by companies such as Amazon, Netflix and Zoom—is allowing users to use common, easily guessed passwords, says Dr. Narayanan.**

**Want to make your Amazon password “12345678”? You can, says Kevin Lee, a research scientist and one of the co-authors of the paper with Dr. Narayanan. But hackers and identity thieves may thank you.**

**Data gathered by Dr. Narayanan and his co-authors found that of 120 of the most prominent sites and services on the internet, 71 didn’t block any of the most frequently used and easily guessed passwords.**

**Another bad password policy that is also a chronic annoyance to many of us is the rule that you have to include special characters in your password. In days of yore, the rationale behind this rule was that special characters could foil attackers by making passwords more complicated, and therefore harder to guess, says Sten Sjöberg, the third co-author on the Princeton paper.**

**But in the real world, this turns out to be just another incentive for people to make short, guessable passwords and then, say, add an exclamation mark to the end, says Dr. Cranor.**

**Availability isn’t enough**

**Cybersecurity-savvy readers may, by now, be throwing up their hands in exasperation. Of course these are all bad password policies! But do they matter, if a person uses two-factor authentication on their most important accounts, and they’re using a password manager to generate a unique and complicated password? (A password manager, which everyone should adopt, generates strong passwords, stores them and automatically enters them into apps and sites.)**

**Perhaps not—if people are actually using those tools. The problem, as years of surveys have uncovered, is that just because people have the option to better secure their accounts, it doesn’t mean they will. Indeed, surveys suggest that 10% to 34% of people use password managers.**

**Statistics on two-factor authentication, which verifies a user’s identity by asking them to provide a second secret, such as a code sent by text message, are harder to come by.**

**Microsoft has since 2014 required that every consumer Micro-soft account use some form of two-factor authentication. And since 2021, the company has allowed all users to go completely password-less and log in with a new technology called a “passkey,” which uses techniques such as facial recognition to verify users’ identities.**

**“Our point of view is that passwords are fundamentally flawed, and rather than trying to fix them, we are trying to think of them as one small part of that overall ceremony to figure out, ‘are you who you say you are?’ ” says Alex Simons, a corporate vice president in Microsoft’s identity and network-access division. That “ceremony” to identify users includes whether they’re logging in from a new device, whether Microsoft’s machine-learning systems have recognized unusual behavior in their account, and where they’re attempting to log in from.**

**Send this to IT**

**So, what exactly are some of the best practices for password and cybersecurity policies?**

**First, companies need to stop forcing users to regularly reset their passwords. Second, don’t allow people to use any passwords that appear on publicly available lists of leaked and easily guessed passwords. Third, provide real-time password-strength estimates, as someone is typing out their password— and make sure this tool is informed by up-to-date research. Fourth, don’t require special characters in a password. Fifth, it is OK to encourage people to use longer passwords than they typically might.**

**In addition, mandating that users adopt device-based two-factor authentication can radically increase the security of any given account. Likewise, encouraging users to use password managers can help. (Hey, companies, why not let employees expense them?) Finally, the move to passwordless login, via passkeys, is an opportunity to leapfrog current security standards, to a kind that is both more convenient and new enough that there are fewer known ways to hack it.**

**The key to making individuals and organizations more secure is to create cybersecurity policies that respect how people actually behave in the real world.**

**“I think security has always been everybody’s problem, but now we are realizing it,” says Dr. Cranor. “And I think a well-designed security system can help reduce the burden on the non-security experts on the team.”**