Passwords Redux Deluxe

New Password Rules for the 2020s

STEPHEN HUSTON

Why Would Anybody Want to Hack *Me?*

I'm not a likely target.

Yes, **you are the target**… *and so is everybody else!*

Numerous *nation states* have professional teams and military units hacking into financial accounts all around the world as a means of financing their clandestine activities. There are other criminal groups operating as international businesses which do nothing but steal money from foreign citizens. Hacking crimes in one country can't usually be prosecuted in another. If you have funds in any bank or account system that uses computers in its business, your account is hackable. Banks rarely recover hacked funds, and they seldom restore funds if an individual's account is emptied using that customer's own login and password.

It's All About the Passwords

There is one undeniable fact about Passwords — *given enough time, they can all be hacked*. My goal is to help you ensure that hacking your passwords will take so long that no hacker will bother to crack them. Then you can quit worrying about it.

Before getting to my updated password guidelines, I'm going to explain how computer password systems and hacking techniques have changed in recent decades. I won't get technical, but seeing how we got to where we are now will clarify why we need to improve our password craft to cope with today's risks.

Early Computer Passwords

The first significant use of passwords on computers came in the 1960s, to implement time-sharing on mainframe computers. Multi-user account systems became necessary to segregate users' files and to restrict each user's time on a mainframe system. Because terminals for mainframe computers were few and computing power was limited, users' time on those systems had to be restricted.

That first password system was soon hacked. Someone simply figured out where the Passwords file was stored, and printed it out. Then he could login as any authorized user so his time in the system was no longer limited to his own allotment. It didn't matter how strong or weak those early passwords were because he didn't have to hack them. He simply printed them all, and then he could impersonate anyone in the system. (Stealing a copy of a system's entire password list is now known as a *Data Breach*.)

Multi-user password systems gradually moved to desktop computers and laptops, mainly to segregate each user's files in shared environments. However, it's still common for personal computers and smart phones to be set to auto-login without requiring a password, giving anyone who can power it up access to all of the email accounts and stored logins in the system. (This is *No Security At All*.)

Passwords in the Internet Age

Since the mid-1990s, internet services and computer systems have implemented Account Name and Password *credential systems* to restrict access to files, email, banking, and retirement accounts, as well as other online services.

When setting up a new online account, users are prompted for an Account Name (often their email address) and a password. Passwords of any length were once allowed, so most people picked simple words that would be easy to remember but hard for their friends and family to guess. Most people chose passwords such as *123456*, *password*, *monkey*, *iluvyou*, or a simple *hello*. Occasionally, some rebel would pick *I am the Walrus!* — which is actually pretty strong. (It's not particularly *good*, but it is *stronger* than most passwords currently in use.)

Online Systems Administrators assigned short passwords such as **M/sXP#** to manage web servers and email systems because they were *hard to guess*. I still remember being pleased when my web-hosting company assigned me a 6-character password nobody would *guess*, while also being a bit irritated that it was nearly impossible to recall when I needed it because it wasn't memorable and I didn't need it often. That little password provided full access to my website and email server back in 1999, but 6 characters wasn't much protection against intrusion by others. Its only strength was that *it was not easy to guess*.

The Birth of Password Policies

In 2003, to improve security standards as Internet use expanded, the National Institute of Standards and Technology (NIST) commissioned a report by William Burr which became the go-to reference for both business and government in setting new password policies. Burr's guidance was well thought out, though most of it was entirely speculative — there being no actual data on password usage available for him to study. His report of over 100 pages was reduced to a small set of rules which could be easily implemented.

2003 Password Rules

The complex NIST report was reduced to a few basic rules:

1. Passwords must have a minimum length of **x** characters. (**x** = 6 or 8)
2. Passwords must include multiple character types, not just lowercase letters.
3. Passwords must be changed at regular intervals.
4. Passwords must not be reused when changing a password.
5. Passwords must not be written down; they should be memorized.

These rules had an unexpected impact on real-world password choices as people struggled to memorize passwords for their growing list of online accounts.

- Passwords were kept to the minimum length allowed, or very close to it. (Curiously, nobody's rules ever required "at least 7" instead of either 6 or 8.)
- Passwords were usually *readable* and *pronounceable* as words, but with a capital letter and/or some character substitutions to satisfy rule 2.
- Having devised a memorable password which passed all of the required tests, computer users frequently reused their favorite passwords across multiple accounts rather than creating and memorizing a new one for each account as their online registrations multiplied. Because each online system sees only its own password data, it can't stop you from reusing a password you've used elsewhere — it doesn't even know you've reused it. Password rules are only enforced at each website, not across your entire online systems of accounts.

Hacking Comes of Age

Meanwhile, hackers were learning new skills. Those good old days when most people's biggest security concern was that someone would try to piggyback on their broadband connection were fading fast. Before long, international criminals began emptying online bank accounts. Password systems were facing new and more costly risks, but those password rules didn't evolve, and online security systems didn't keep pace. The real-world results of the 2003 password rules ended up being so unfortunate that, 15 years later, NIST's author, Bill Burr, publicly apologized, saying: *Much of what I did I now regret*.

If that first hacker in the early 1960s hadn't located the password file, he might have tried *guessing* passwords, as so many amateur hackers did when sniffing for neighborhood broadband connections. Even now, *Password Guessing* is the main threat most people expect — so picking a password no one will *guess* feels safe.

Hackers changed all that as they harnessed computing power itself to automate their hacking process. It became faster and easier to have a computer run millions or even billions of possible passwords in less time than a person could enter one password guess via a keyboard. Suddenly the very concept of what made for a strong or weak password had nothing to do with it being *guessed*.

The new question has become: *is it hackable?*

Every Password is Hackable

All passwords can be hacked — given enough time. So hackers have devised several strategies to improve their chance of finding correct passwords more quickly, based largely on how people choose passwords under the 2003 rules.

Without getting technical, here's a basic list of common password attacks:

1. Credential Stuffing
2. Breached Passwords
3. Dictionary Attack
4. Brute Force Attack

Let's take a look at each of these just to understand what it accomplishes for the hacker and what its risks are for your password security.

CREDENTIAL STUFFING

According to security specialists, Credential Stuffing accounts for more internet traffic than all other internet uses combined, including billions of daily emails, internet searches, and website viewings. A server is targeted rather than any specific user's account. For instance, a hacker may decide your bank is a good target — that's where the money is — without caring whether you personally bank there. Credential Stuffing takes billions of Account Names and Passwords known to be used together from past data breaches, and digitally stuffs them all at that bank's server to see which Account and Password pairs work at that bank. The hacker's system reports which ones succeeded. The hacker can then take funds from the accounts, sell the account info to other hackers and criminals, or both.

The tendency of most computer users to reuse passwords across multiple accounts guarantees that there are always enough successes with Credential Stuffing to justify the effort of these automated attacks. If you reuse a password, you will eventually be hacked via Credential Stuffing, even if you follow all the other rules.

BREACHED PASSWORDS

The number of accounts exposed in Data Breaches has now passed *13 billion*. Hackers have lists of those passwords and use them to automate attacks against lists of accounts. A hacker takes a list of email addresses or account names, then automates running those billions of passwords against the accounts. Using modern computer systems, this attack may take less than one second per account — yes, just one second for a billion password attempts. (Ain't computers great?)

If any of those passwords match an account's password, that account can now be used by the hacker, whether its your email account or your retirement savings. Some hackers just sell this information to a criminal gang or other hackers. Selling your credentials generates income for the hacker without risking the criminal liability of personally stealing your money. It's safer for hackers to let criminals do the real dirty work of theft, often from the safe distance of a foreign country.

DICTIONARY ATTACK

This attack is very similar to the previous data breach attack, but instead of using lists of known passwords, it compiles all of the words in the World's dictionaries, including common character substitutions. While there are hundreds of languages, the total number of different letter combinations that spell real words is only about 6 billion. These custom *hacker dictionaries* are sold and traded among hackers. Unlike a Breached Password attack, these dictionaries even include words and substitutions that nobody has yet been caught using as passwords.

BRUTE FORCE ATTACK

The Brute Force Attack is usually a hacker's last resort, though it is fully capable of cracking *every possible password*. The hacker automates running all combinations of characters starting with the shortest length allowed by the target site's password rules, up to longer and longer combinations until it eventually finds the exact sequence that matches your password. Brute Force Attacks *do eventually find it*, but they have one limitation — *Time*. A computer's speed coupled with how long the hacker is willing to wait for that winning combination are the only reason this attack might be called off before your password is found, *so length matters*. You need to survive all of the other attack types and also have a password that is simply too long to find before any hacker will choose to move on to easier victims.

Time is Money

All of these attack types except the Brute Force Attack can be run against an account system in a matter of seconds. Contrary to the movies, no competent hacker will ever attempt to *guess* a password when they have the computing power to run passwords at millions or billions of times the speed of using a keyboard.

In our brave new world, you need passwords that won't be found in the first three attack methods, *and* are so long that a Brute Force Attack will be abandoned long before your passwords are reached.

The password rules of 2003 encouraged people to pick passwords that can be found quickly by these modern hacker attacks; after all, hackers devised these approaches based on how people responded to those old rules!

Our new rules still must meet the requirements of the earlier password rules, because those are the rules currently being enforced all around the world. However, we need *better* rules if our passwords are to hold up against modern hacking attacks.

New Password Rules for the 2020s

1. **Never reuse a password, ever**!
2. **Always include all 4 character types**.
3. **Password length — as long as possible**.
4. **Use only unique passwords**.

These may sound a bit like the old rules, but in fact they are quite different, so some explanations are in order.

NEVER REUSE A PASSWORD, EVER!

No matter how strong you think your password is, use a different password for each and every account. If you change a password, don't pick a password you've ever used elsewhere, even if you're no longer using it anywhere else. This reduces the risks from both Credential Stuffing and Breached Passwords attacks.

USE ALL 4 CHARACTER TYPES

Using all 4 character types ensures that a Brute Force Attack will take much longer with 95 possible characters instead of just 10 for numbers or 26 for lowercase letters. Basic math shows that the more available characters, the more combinations can be made, so it takes longer to try all the possibilities.

For example, hacking a 12 character passcode takes about 1 second if it's all numerals, and around 15 minutes if it's all lower case. However, if all 4 character types are included, that 12 character passcode could take years to crack!

Making the hacker's Brute Force Attack take way too long is the only defense against its eventual success, so the number of character types matters. This also contributes to the success our next rule… length.

PASSWORD LENGTH — AS LONG AS POSSIBLE

With current computer speeds, anything under 12 characters is already too short to be safe against a Brute Force Attack. If your bank won't let you use 16 characters, *change banks*. That is not a joke. Make your passwords as long as you can stand. In 2020, as this is being written, 12 characters is considered a bare minimum, and that minimum safe length keeps increasing as computers get faster.

For example, a Brute Force Attack can already crack every possible password of 8-characters-or-less within one minute. *Eight is not enough!*

As computers get faster, hacking times will keep getting shorter, so your passwords will need to keep getting longer. Future-proof your passwords now by making them significantly longer than seems necessary, then review your passwords annually to be sure they will remain safe for the foreseeable future.

USE ONLY UNIQUE PASSWORDS

This is an extension of the first rule — never reuse a password. However, this puts that first rule on steroids: Never use anyone else's passwords either! This new rule of being *unique* requires some explanation and practical ideas for implementation.

Death of Your Perfect Password

Let's imagine you've come up with a great 16-character password that you've never used. It has all 4 character types and doesn't even look like a dictionary word. Now suppose that just by chance that same string of characters was previously used by someone else — just once, anywhere in the world — and the server where they used it was hacked and its password list was stolen. So now *your perfect password* is part of a hackers' kit, just waiting to be used in a Breached Passwords attack, where it would open your account within seconds!

How can you avoid using a password that someone else might have used, including passwords others might pick in the future? (Data breaches continue to happen daily.) This requires a new level of cunning to create a password that is unique now, has never been used by anyone before, and is likely to stay unique while billions of people continue to create new passwords. That is what's required to stay safe from Breached Passwords attacks.

What Do We Mean by Unique?

1. Unique means *one of a kind, unlike any other*. It's an absolute quality. A thing is either *unique* or *not unique*. There is no third option or sliding scale.

2. *Beware of Entropy!* The more chaotic a thing is, the less likely it is to repeat. This is sometimes called *entropy*, but nobody agrees on how to measure it. When you encounter the word *entropy* in a password discussion, it's time to move on to the next paragraph… like right now.

3. The words *Unique* and *Random* are often used interchangeably in password discussions, though they are entirely different in meaning and have nothing to do with each other. Picking something randomly does not make it unique. For example, computer-generated *random numbers* tend to repeat with surprising frequency. They're numbers! Numbers have a predictable sequence, so a number cannot be unique no matter how randomly you chose it. Similarly, randomly generating a password does nothing to assure its uniqueness. While any system can be made to generate a value that is *unique within that system*, it cannot stop another system from generating that same exact value.

4. *Words* are not unique. Substituting numbers and symbols for some letters won't necessarily make the result unique either. Because the human mind works with patterns, many of us will pick similar substitutions, and those substitutions are predictable instead of unique. No amount of cleverness is going to create something unique using a dictionary word and letter substitutions.

5. *Phrases* are rarely unique. Phrases are, by definition, *recognizable word groups*. Remember the *phrase*, "great minds run in the same ruts." Any chance of coming up with a phrase that is unique is pretty small. You need something even less predictable and less likely to be repeated than a phrase if you want to avoid the risk of duplication on a world-wide scale.

While there is no guaranteed test for uniqueness, I do have some ideas that can get you well down the road toward crafting unique passwords.

Attempting Uniqueness

1. Pick two or three unrelated words — not a phrase, not song lyrics, not a quote or *saying* — but words that really are not related in such a way that they might be used together. Don't just *assume* that they are unrelated; usually you'll be wrong. After all, something made you think of them together. (We all rely on our brains' pattern recognition and associations without being conscious of it.)
2. Search for your words together on the internet to make sure they aren't found together. When you finally get a pair or triplet of words that returns no matches in a search engine, you're ready to go. (You will probably have to intentionally misspell one or more of your words to get this far. Test your misspellings too.)
3. Now slap them together with a symbol, punctuation, or number separating them, and stick another character type at either end of the whole thing. Capitalize one or more of the letters, but not at the beginning of any word.

You should now have a password containing all 4 character types, *more than* 12 characters long, that you've never used before (and know better than to ever use again), and very probably nobody else has or will either. You've given it your best shot, so quit worrying about it — unless you want to make it *looooonger*.

Longer is always a good afterthought. Heck, if your new password is still under 20 characters, add a repeating letter to the backend to make it longer.

You've Come a Long Way

We've now taken passwords from *monkey* to something more like

filBerg2bargain#sfff.

It takes a few minutes, but it's very satisfying to finally see a "No Results Found" result in your search engine just before you add those few refinements to satisfy both the old password rules and these new ones.

Can I promise that nobody else will ever come up with that same text string to use as a password?

No, but it's highly unlikely if you followed those three steps.

One Last Thought

Record your passwords safely, and not just on your main digital device.

That old rule about memorizing passwords and never writing them down made people do really stupid stuff like keeping their passwords as short as was allowed or reusing them because new ones were hard to remember. There are ways to record passwords securely and easily, and there are Password Managers to help.

Do your best.

It's your privacy and your financial security that's on the line.

Well-reviewed password management software products include:

- **1Password** from *AgileBits Inc*. at *1password.com*
- **BitWarden** from *BitWarden.com*
- **Dashlane** from *Dashlane Inc*. at *Dashlane.com*

The first two are the most mentioned by techies I know as their personal favorites, but most people tend to recommend whichever one they use.*

Review them all to see what each offers and what they charge for subscriptions. They are available online and on Apple's App Stores, and they work across multiple computer platforms and devices. This listing is neither exhaustive nor an endorsement of any product, but it's a good place to start.

* *LastPass* was removed at the beginning of 2023 due to a security breach of user Vaults, lack of encryption of user IDs & data, and lack of public transparency.

* *RememBear* was removed because it will be discontinued after 2023.
