Legal Tech: Passwords & Security

By Trey Peacock, Winning Cases Based On Science & Data For Over 25 Years
Originally published on LinkedIn.com

Hardly a month passes these days without a major global technology or web company regretfully announcing a breach of its users' most personal, private data. These hacks, or leaks, happen so often that it's easy for everyday users to brush them aside, justifying blissful ignorance with the unwarranted hope that their data isn't among that proliferating on the internet or the dark web, available for use by scammers and identity thieves. The hard-to-swallow truth is, nearly every person with an internet account of any kind has had at least some aspect of their personal online identity compromised by a hostile force. The most devastating leaks occur when hacks on companies such as MyFitnessPal, Wells Fargo, and others, net not only credit card data, but passwords, usernames, and email addresses as well. A system of strong, unique, and practical passwords guards your electronic assets and is one of the most potent lines of defense against the fallout from inevitable data breaches. In this article, I offer several rules and tips to help readers safeguard their data and devices using easily understood and implemented steps.

How Your Passwords Get Hijacked & Distributed

Some argue that if, for example, your Facebook username and password were accessed by a hacker, the maximum damage amounts to an embarrassing post or two, and maybe an annoying Account Reset process. This could not be more wrong. The true danger of a password hack such as the one that occurred at Facebook, arises when the tenacious hacker capitalizes on the reality of human user error. All too often, the password to your Facebook account isn't just for Facebook. It's also your Amazon password, and your Wells Fargo password, and it's just one letter or digit off from your work computer login. Now, what was just a breach of your Facebook account has allowed a clever hacker to access your address and credit card data stored in your Amazon account, your banking information, and potentially, your entire library of sensitive, confidential work files. Once the hacker has the information, he can use it in his own phishing or fraud scheme, or sell it on the dark web to other exploiters. The domino effect in cyber form.

Rule #1: Use Lengthy, Complex, Unique, Truly Random Passowords for Each Site

Creating **unique** passwords for each of your online accounts is essential to maintaining the integrity of your data. That way, if one domino goes, the others stand fast.

Several criteria factor into the creation of a strong, unique password. First and foremost, never repeat any password, in part or whole, across more than one account. This includes tacking on characters, numbers, or capital letters. Hackers know that trick too, so just start from scratch and get ahead of the curve. Second, not every account hack arises from a big tech company data breach. Sometimes, hackers employ a "brute force" attack on a user's account. This simply means that, through sophisticated computer work, they try dozens of possible password combinations every second until the correct one is reached. The only safeguard against this measure is making your password long enough and complex enough to render a brute force attack impractical. For example, the simple password "lawyer" would take a modern computer only 0.2 milliseconds to guess. That's literally faster than a blink of your eye. In contrast, the moderately more complicated password "Law&yer2" would hold up against a brute force attack for over ten years. The longer and more complex a password is, the harder it is to crack. Thus, a secure password ought to include at least ten to twelve characters, both lowercase and capital letters, and preferably a few numbers and symbols to boot. Including upper and lower case letters, numbers, and symbols increases the crack time of your password exponentially from a few milliseconds to a few millennia.

Rule #2: Use a Password Manager

The point at which I ask you to create long and seemingly impossible-to-remember passwords for each of your accounts, is where a lot of you abandon the cause. Most people own and operate dozens, and maybe even hundreds of online accounts. How are you supposed to create and remember a complicated, unpronounceable, twelve-character password for *every single one of those accounts?*

The answer is also the most useful tool in combating online security breaches: a high-performance password manager software such as DashLane, 1Password or Keeper.

These applications allow users to easily create, store, and retrieve lengthy, randomly-generated passwords for each of their online accounts. Utilizing a single program to store all of your passwords may feel irrational; if all my passwords are in one convenient place, doesn't that make it easier for hackers to get at my stuff? No. These companies used heightened encryption technologies combined with your unique Master Password (stored only on your computing device) to secure your password data.

With the help of a password manager, the savvy internet user need only remember THREE unique passwords: (1) the password for your work or office network; (2) the password for all of your mobile devices (more on that later); and (3) the master password for your password manager. If you use this method to secure your data, a hacker cannot use data gleaned in one breach, such as a social media company breach, to access other data like that for your bank account. Instead, the hacker would need physical access to your mobile device, your mobile device password, and then, would have to gain access to your password manager using your unique master password. All the more reason to keep that one as long, unique, and secure as possible.

Rule #3: Create Easy to Remember, Lengthy, Complex Passwords

But still, you've got to remember those three passwords. To do so, think of an easily-remembered song title, lyric, street name, or other tidbit, and use it as a base from where to start. For example, say you are a Jimmy Buffet fan. Then, you might start with the lyric "wasting away in Margaritaville." Compress that, add a few characters, and you've got "JBwaiM1946" Easy enough, right? Compare this complex password, which would take nearly 27 years to brute force, with the simple alternative: "buffet," which would fold under an attack in only 0.8 seconds. Utilize this approach for the handful of main passwords in your daily life and your data will be far more secure.

Rule #4: Change the Passcode on Your Phone and Tablet

Finally, you should implement these same password criteria on your mobile devices. Mobile phones and tablets carry a much greater risk of breach via physical theft than a network does. Yet, as all tech-savvy professionals know, the files contained within these devices are no less confidential or sensitive than the information on your network server. Many newer devices can be unlocked with fingerprint or facial recognition software. Users should take full advantage of these features, as they are far harder to beat than a standard passcode. However, users are still required to enter a passcode every 10-14 days, or whenever the device reboots. Thus, you should modify the passcode settings in on your mobile devices from the standard 6 digit passcodes to an 8-digit numeric code, or even better, a ten to twelve character alphanumeric password containing the criteria listed above. The following graphic illustrates just how effective these longer passcodes are at protecting your devices.

Password Length	Possible Combinations	Time To Crack (S = Seconds, M = Minutes, H = Hours, Y = Years)
4	45697	<1 S
5	11881376	<1 S
6	308915776	<1 S
7	8031810176	~4 S
8	208827064576	~1.5 M
9	5429503678976	~45 M
10	141167095653376	~19 H
11	3670344486987780	~.1 Y
*12	95428956661682200	~1.5 Y
13	2481152873203 74E4	~39.3 Y
14	64509974703 2972E5	~1,022.8 Y
15	16772593422 8573E7	~26,592.8 Y
16	43608742899 4289E8	~691,412.1 Y
17	11338273153 8515E10	~17,976,714 Y
18	29479510200 01390E10	~467,394,568 Y

Courtesy of Offensive Security Society. (https://oss.org/ios/set-a-complex-iphone-password/)

To modify the standard security settings on an iOS device, follow these steps:

1. Go to the Settings App
2. Scroll down to "Touch ID and Passcode"
3. Enter your current passcode
4. Tap "Change passcode"
5. Enter your current passcode again
6. When prompted to enter a new passcode, tap "Passcode Options" and select from the menu: a "custom alphanumeric code."
7. Enter your desired passcode
8. Enjoy your enhanced cyber security.

You may use all, some, or none of the precautions discussed in this article. Regardless of your current level of security-consciousness, there are myriad resources and programs available to help users secure and protect electronic information. Savvy users understand that ignoring cybersecurity precautions can have far-reaching and long-term consequences.

About the Author

Trey Peacock, a partner at Susman Godfrey, has been winning cases based on science and data for over 25 years. He has also chaired the firm's IT committee for over two decades. Learn more about Trey here.