Passwords: Your Greatest Vulnerability

A hack here. A hack there. A hack everywhere.

Monster, 2007—1.6 Million Accounts Compromised

Personal information was used to exploit account holders and extort them for money. Phishing emails that appeared to come directly from Monster contained specific account details and encouraged users to download a malicious program. For those that downloaded the program, their files were encrypted and held for ransom and the users were forced to pay the hackers for a decryption code.

LinkedIn, eHarmony & Last.FM, 2012—8 Million Passwords Stolen

Of this 8 million, a majority of them were cracked in less than 24 hours. Many of the passwords contained key phrases such as Harmony or eHarmony and even more of them were considered the most crackable and most popular passwords on the market.

AshleyMadison 2015—37 Million Accounts Placed Out in the Open

A group of security researchers by the name of CynoSure Prime splintered nearly 11 million of these passwords and are currently in the middle of 15 million more. They are not releasing the passwords to the public, but their research suggests a significant percentage of these passwords were less than eight characters long, with no special characters and no capitalization.

How do passwords get hacked?

Hacking occurs everywhere, to anyone, and sometimes for no better reason than to have a little fun. The first line of defense against any good hack is a good password. A nicely formatted password can withstand even the most brutal of attacks.

But before you build up your password, you must know how it can be broken down. Here are seven common ways a hacker plans to crack your code:

They Guess It.

Anyone who knows you personally, checks out your social media page or overhears your conversation can crack a simple password. Do you use the name of your child, your favorite football team or the make and model of your vehicle? What about your wedding anniversary, place of birth or favorite movie? If so, you've done been cracked.

They See It.

Have you ever logged into an account in public or written a password down on a piece of paper? Did the person standing behind you in line see you? Did you even know someone was standing behind you?

They Log It.

Has your PC, phone or tablet been infected by malware lately? If it has, you might be infected with a bad case of the Keyloggers. This tricky version of malware can see and track everything you type. If you don't use a password manager, it can log all your keystrokes, including when you signed into your bank account, your email, and your Facebook page.

They Automate It.

There are many types of software available—most of which are free—that hackers use to crack your passcodes. These include Brutus, RainbowCrack, and John the Ripper. These automate the code-cracking process and the only defense is a long, complex password and time. This malicious software creates algorithms to quickly run through every dictionary word and a list of the most popular passwords. It will then attempt other less common word combinations and begin attaching capitalizations, numbers, and symbols. If your password is complex enough, it may take weeks or months this tool to guess your code.

They Expose It.

Hackers can use a variety of means—phone, email, letters—to wrongfully expose your password. This type of password cracking would fall in line with the Monster example noted previously. The hackers stole personal information from Monster's account holders and used this information to moonlight as the company. While their intent was not to gain passwords, they easily could have done so.

They Phish It.

The intent here is to trick you into inputting your login information. A corrupt link will lead you to an illegitimate website that looks almost identical to the real thing—your email, a shopping website or your bank account. Once you type in your credentials, the site will record your information and use it to gain access to your true account.

They Steal It.

Ashley Madison's account passwords were stolen. Someone hacked into their database and kidnapped all the information it contained. These passwords were 'hashed', which transforms your data into another format much like encryption does. But with hashing, the data is stored differently and is not 'reversible', meaning it should be more secure for data like passwords; however, this did not stop a handful of security experts and groups from trying. It only took a few hours for most of these groups to crack millions of Ashley Madison passwords. And, once again, the only defense you have is a long, complex password and time.

What does a strong password look like?

Many companies, such as LastPass, utilize a password generator and a formula to spit out an unintelligible combination of letters, symbols, and numbers much like this one, “**19Qu^Tf3U55j**”. This is considered a quality password, but most of the public never have and never will employ a password like it.

A strong Password:

- Contains at least 8 characters, although many security firms believe a password is not acceptable until it has 14 characters.
- Uses random capitalizations and characters.
- Never contains complete words or names or coherent phrases.
- Won’t use a word that can be found in a dictionary.
- Employs ‘toothbrush’ logic, meaning it will change about every 2-3 months.
- Is unique and will not be used more than once or ever again.
- Won’t be stored on a computer or anywhere on the internet.

Why don’t people use strong passwords?

Time and time again, people fail to use strong passwords and what’s worse is that they do it knowingly. In fact, in 2013, 90% of all passwords were considered vulnerable to hacking. Internet users are still resorting to passcodes like ‘password’ (7% of users), ‘qwerty’ and ‘12345678.’ These passwords are on the list of the Top 500 Passwords, which means people everywhere use these passwords to store multiple accounts on a daily basis (79% of the public to be precise). These are also the passwords that are the first to be cracked, within minutes and with no software needed.

So why don’t people use strong passwords? Simple.

1. They’re hard to remember.
2. They’re in a hurry.
3. They have too many accounts.
4. They don’t care.
5. They don’t realize the risk.
6. They think they’re immune.

How do you remember a strong password?

In a blog written for the New York Times, the author interviews two cyber-security experts, Jeremiah Grossman, and Paul Kocher. The author goes on to explain how these security researchers protect and remember their super complex passwords.

Grossman copies and pastes his passwords directly into and out of an encrypted USB drive. He generates a long, intricate password and stores it in the USB. When he needs to log into an account, he copies and pastes the password from the USB. This accomplishes three things.

1. He never types out his account information, which means keyloggers cannot record his passwords.
2. He doesn't have to remember his passwords.
3. His passwords are never stored anywhere—on the internet, on his hard drive or on a piece of paper.

Most people would never go this far to maintain a strong password; therefore, Grossman follows up with the potential of a password manager like LastPass or SplashData. These programs create strong passwords for you that you never have to remember. The downfall of password managers is that your information is still stored on the internet. If someone gains physical access to your computer, they can potentially gain access to every single password. On top of this, password managers are just as prone, if not more, to hacks than any other company, website, or individual. In June of 2015, the LastPass database was hacked. This company, in particular, utilizes a combination of hashing and salting to secure data; therefore, cracking these passwords would take significantly more work than it took to crack Ashley Madison's passwords. But that still doesn't ensure every account is secure.

Aside from password managers, you are only left with your mind. So the trick is to come up with a complex password that you can actually remember, which can be difficult. Grossman and Koch say passphrases are helpful, but it's important to remember not to use the passphrase itself.

Example:

"May the force be with you." = "m11*t33&f55^B77%W99$Y##"

Use the first letter of each word. In between each letter, put a specific quantity of characters, additional letters or numbers. You can make this easier to remember by creating a pattern. For instance, this specific example uses odd numbers and goes up by two each time. The first three letters are not capitalized and the last three are. The characters go down the keyboard starting with '*' and ending with '#'.

You don't have to use a password this complex for every account you have. Your passwords should always be slightly difficult to crack, but save the most intricate ones for anything that ties back to your work, your finances or your inbox.

Where are passwords headed?

Passwords are a dying breed. Every company and security firm across the globe know it's only a matter of time before even the most complicated password is cracked. Because of this, the traditional password must be phased out. The public has already seen bits and pieces of this, such as two-factor authentication (push notifications) and biometric scanning (fingerprints), but here are a few of the ways the traditional password might be replaced in the future:

- **Embedded Chips:** PayPal would like the public to ‘wear’ chips underneath their skin or ‘eat’ sensors that would directly communicate with your heart and wireless antennae.
- **Handwriting Match:** A security firm based in Sweden has developed software that recognizes the way you type, much like the way you write.
- **Security Tokens:** Out of Alabama, a group is working on utilizing Bluetooth or “a short-range, wireless communication channel” to identify you as the proper user. Once identified, you will automatically be logged into your account.
- **Voice Biometrics:** The security firm, Nuance, is working on voiceprint technology. Like a fingerprint, your voice cannot be replicated and may add an extra layer of security to your ‘password.’
- **Face Recognition:** This type of technology is already being used in vehicles by Canberra to detect fatigue while driving and can potentially be used to secure accounts, homes and applications.

What should you remember?

Like mentioned previously, it’s only a matter of time before your password is cracked. But, ‘time’ is also your greatest ally. Secure your most important accounts with a complex password that takes time to crack. If it’s easy to remember and can be found in a dictionary, you’ll be one of the first to go.

Sources

http://www.securityweek.com/study-reveals-75-percent-individuals-use-same-password-social-networking-and-email

http://www.pcmag.com/article2/0,2817,2368484,00.asp

https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=strong+passwords&start=10

http://www.nytimes.com/2012/11/08/technology/personaltech/how-to-devise-passwords-that-drive-hackers-away.html?_r=0

https://lastpass.com/generatepassword.php

https://identitysafe.norton.com/password-generator/

http://www.slideshare.net/jcleblanc/kill-all-passwords

http://tiptopsecurity.com/password-cracking-101-how-hackers-get-your-passwords/

http://www.cnbc.com/2014/08/25/forget-passwords-this-is-the-future-of-logging-in.html

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

http://arstechnica.com/security/2012/06/8-million-leaked-passwords-connected-to-linkedin/

http://www.scmp.com/lifestyle/article/1805289/forget-passwords-future-digital-security-lies-biometrics

http://www.theinquirer.net/inquirer/news/2418367/hackers-breach-cheaters-website-ashleymadison-in-data-debrief-encounter

https://www.yahoo.com/tech/in-the-future-your-veins-could-replace-your-116644086459.html

http://resources.infosecinstitute.com/10-popular-password-cracking-tools/

https://danielmiessler.com/study/encoding_encryption_hashing/

http://www.businessinsider.com/90-percent-of-passwords-vulnerable-to-hacking-2013-1

http://www.informationisbeautiful.net/visualizations/top-500-passwords-visualized/

http://www.hongkiat.com/blog/passwordless-future/