THE 2022 WEAK PASSWORD REPORT

An annual investigative look at the state of passwords

Passwords are easy to attack because people use easy-to-guess passwords. These passwords are guessable because people reuse passwords and follow common patterns and themes. These passwords then end up on breached lists and can be attacked via brute force and password spraying.

Understanding common password patterns and user behaviors is the first step in securing passwords and the critical business data they protect.

ABOUT SPECOPS Specops Software, an Outpost24 Group company, is the leading provider of password management and authentication solutions. Specops protects your business data by blocking weak passwords and securing user authentication. Every day thousands of organizations use Specops Software to protect business data. For more information, please visit specopssoft.com

Executive Summary

Password attacks are on the rise because passwords themselves are very vulnerable to attack. What specifically makes them vulnerable? This year's Weak Password Report takes a look at both the human side and the tech side of why passwords are the weakest link in an organization's network.

From real world attack data to passwords inspired by pop culture, the 2022 Weak Password Report has insights into just how vulnerable passwords truly are.

Some highlights:

- 93% of the passwords used in brute force attacks include 8 or more characters
- 54% of organizations do not have a tool to manage work passwords
- The Cincinnati Reds top the list of most popular baseball teams found in compromised password lists
- 48% of organizations do not have user verification in place for calls to the IT service desk
- 41% of passwords used in real attacks are 12 characters or longer
- 42% of seasonal passwords contained the word "summer"
- 68% of passwords used in real attacks include at least two character types

The research in this report has been compiled through proprietary surveys and data analysis of 800 million breached passwords, a subset of the more than 2 billion breached passwords within Specops Breached Password Protection list. The data analysis looked at any password containing words within a particular theme. While it is impossible to say that using the word "angels" in a password is related to the baseball team in Los Angeles, the prevalence of words related to the themes demonstrates the problems of password reuse and compromised passwords.

The data in this report should bring awareness to this all-too common problem. The next step is to take action, which means blocking weak and compromised passwords, enforcing password length requirements, enforcing user verification at the service desk and auditing the enterprise environment to highlight password-related vulnerabilities. For this reason, Specops Password Auditor was developed to help organizations identify multiple vulnerabilities, exportable in report format all in a matter of minutes.

The weakest link: Passwords

Passwords are easy to attack because people often use vulnerable passwords that are easily guessed or already compromised. In the Online Security Survey, Google reported that 65 percent of people reuse their passwords. These passwords are vulnerable because people reuse them across various personal and professional platforms. This makes it more likely that they end up on breached lists which are then used repeatedly in password attacks.

Historically, the best practice for creating stronger passwords was to require minimum character length and added complexity, in the form of different character types. This advice has proven to create passwords that are difficult for people to remember, and easy for hackers to exploit. As long as people reuse passwords, making these more secure comes down to disallowing all known compromised passwords.

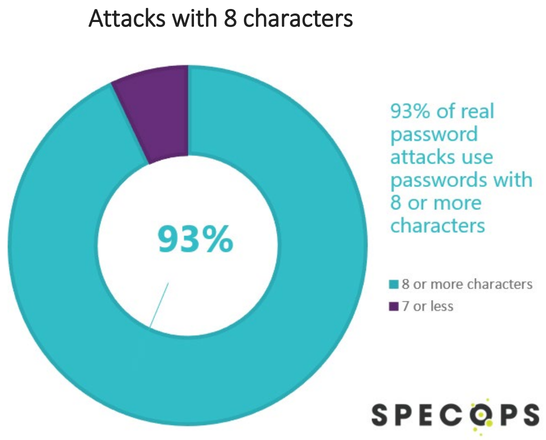
Reusing passwords is the understandable result of having too many passwords to manage in our digital lives. Many people reuse a password once they have created something that passes the complexity test of a password strength meter. In general, people follow similar patterns when creating memorable passwords by choosing root words that are family-oriented or related to their interests. Complexity is added to these root words in predictable patterns, such as placing numbers at the end of the password, leetspeak character substitution and keyboard patterns.

Common passwords in real-world attacks

Minimum password length is a good start at defending against some of the common types of password attacks, like a brute force attack. A brute force attack is when a bad actor takes a list of common or compromised passwords and systematically runs them against a user's email to gain access to a given account.

The password spraying attack is a specialized password attack commonly used by attackers that is reasonably effective and helps avoid detection by traditional password defenses. Instead of trying many different passwords on a single user account, the password spraying attack may try one or two common passwords across many different accounts and services. It may even span across many different organizations.

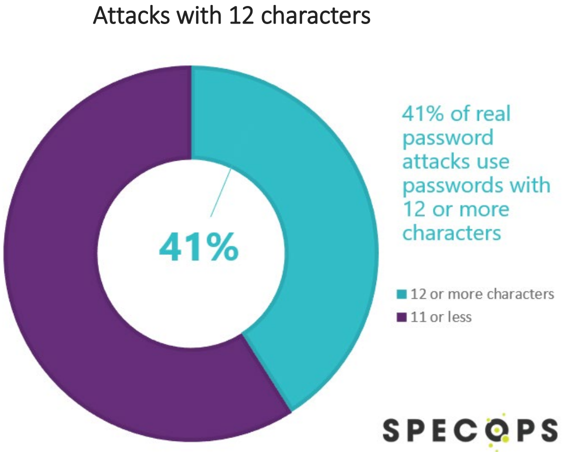
Password Spraying Attack
Using a small list of common passwords against many organizations and services.



The attacker picks passwords commonly used by end-users or found on breached password dumps. Password spraying attacks help avoid detection by many available traditional security monitoring solutions since the attack pattern looks similar to normal failed login attempts. The attempts do not lock out accounts or trigger other monitoring thresholds.

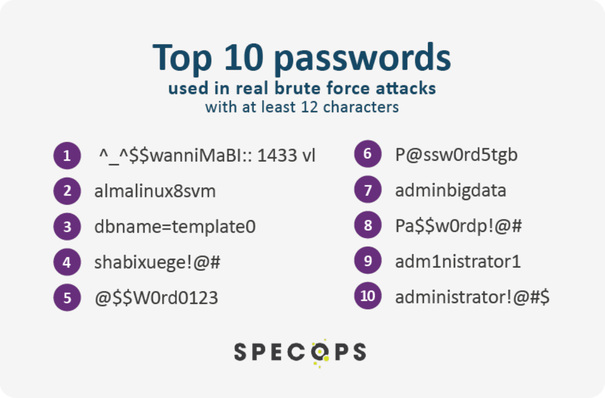
To protect against real attacks you'll have to go beyond just minimum password length, recommended by some regulatory bodies. For example, the National Institute of Standards and Technology (NIST) requires a minimum of 8 characters or more and it seems attackers are aware of this as 93 percent of the passwords used in these brute force attacks include 8 or more characters.

What about requiring special characters or complexity? Standards like PCI or HITRUST require different character types as part of your organization's password rules. Attackers seem to be taking these standards into account as well as our research team found that 68 percent of passwords used in real attacks include at least two character types.



Many organizations choose 12 characters as the minimum password length requirement so Specops Software analyzed the attack data coming from their honey pots. The team found that 41 percent of passwords used in real attacks are 12 characters or longer. Attackers are well aware of the standards recommendations and password requirements companies are using to fight these attacks. This data shows that attackers have adjusted their tactics to include longer passwords.

And while you might think something as simple as "password12345" would be what was found, here are the top 10 passwords used in real brute force attacks that are 12 characters are more. These passwords are long and complex, but also compromised, which is why requiring longer passwords is not enough to protect from real attacks.



Top 10 passwords
used in real brute force attacks
with at least 12 characters

1. ^_^$$wanniMaBI:: 1433 vl
2. almalinux8svm
3. dbname=template0
4. shabixuege!@#
5. @$$W0rd0123
6. P@ssw0rd5tgb
7. adminbigdata
8. Pa$$w0rdp!@#
9. adm1nistrator1
10. administrator!@#$

SPECOPS

Weak and Compromised Passwords in Action: How they are used in cyberattacks

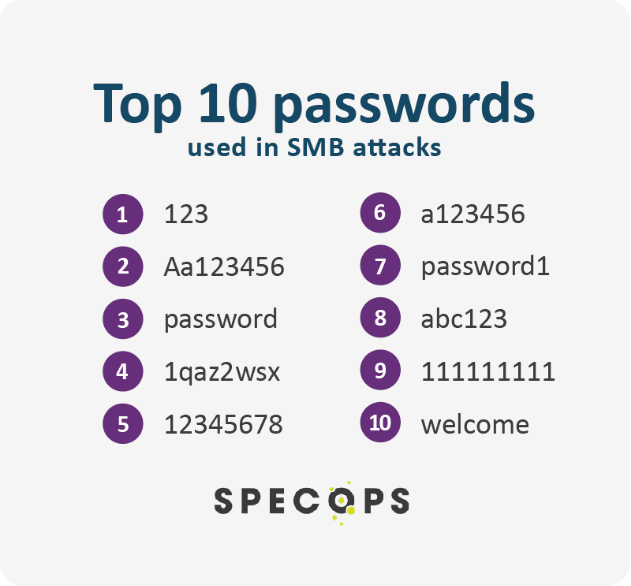
It's one thing to understand how many of your users are using weak passwords that could leave you vulnerable; it's another thing to see those weak passwords used in an attack against your organization.

The next sections will provide a break down of how weak and compromised passwords can give a hacker a golden ticket to your data and IP. Understanding what a wordlist is and realizing that the service desk could be the biggest piece of the puzzle increasing your attack risk, are important steps in assessing all potential password related vulnerabilities.

SMB Protocol Attacks

Weak passwords are an easy entry point for attacks almost anywhere in your network but recent events have put attention on the SMB protocol. Purple Fox, malware that was first discovered in 2018, has seen a recent rise in proliferation as hackers take advantage of a new attack method: weak passwords used over the SMB protocol.

SMB (Server Message Block) is a protocol mainly used by Windows computers to communicate with other network devices like printers and file servers. Active Directory users on Windows computers utilize the SMB protocol with their Active Directory password.



Top 10 passwords
used in SMB attacks

1	123
2	Aa123456
3	password
4	1qaz2wsx
5	12345678
6	a123456
7	password1
8	abc123
9	111111111
10	welcome

SPECOPS

Purple Fox first appeared in 2018 using phishing and exploit attack methods – both methods that required some sort of user interaction to initiate. The newer SMB attack method is of concern to security professionals because it means that Purple Fox no longer requires user interaction to propagate.

The Specops research team has been collecting data on what the SMB attacks look like using a global honeypot system, including what passwords these attackers are using. The team analyzed over 250,000 attacks on the SMB protocol over a period of 30 days. “Password” was found used in attacks over 640 times in that period.

What goes into a Wordlist?

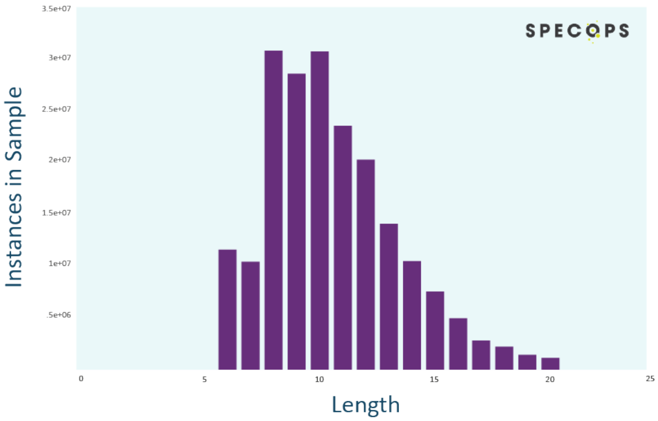
In June 2021, a large data dump was posted to a popular internet hacking forum. This dataset was termed “rockyou2021,” named after the popular password brute-force wordlist known as Rockyou.txt.

Media and Twitter alike were abuzz with what to do about RockYou2021. You would not be alone if you were wondering if or how you should protect your network from RockYou2021. The Specops software research team did a deep dive on the dataset and while some on Twitter were advising this dataset was full of junk data that didn’t need any action, our team’s verdict wasn’t quite the same.

The intent of this dataset was to be used to assist in the brute-force attacks on password hashes with the goal of finding a password in the wordlist to log into the service or system that the hash protects. This dataset was described as a combination of “COMB” (Collection of Many Breaches), and wordlists generated from Wikipedia, and other sources.

Wordlist
A list of possible inputs collected in plain text that are used in brute force attacks. Often made up of randomly generated words or words and character combos, neither of which is necessarily based on real breached data.

Password Length Frequency



The dataset trends towards longer passwords, necessitating the enforcement of either harder-to-remember longer passwords, to avoid collisions with the wordlist, or optimally, the use of passphrases.

Our team also looked into the complexity of the RockYou2021 records. Below you can find the breakdown of how many records fall into different complexity types as well as some examples taken from the RockYou2021 records.

Complexity type	Record count	% of RockYou2021	Examples
Lowercase letters & numbers *(mixedalphanum)*	**34,296,199**	**34.06%**	- *sta8342* - *residerais6*
Lower and uppercase letters w/ numbers *(loweralpha)*	**20,526,308**	**20.38%**	- *BEllow2588* - *peDiortho95*
Lowercase letters only *(mixedalpha)*	**15,398,980**	**15.29%**	- *nadajuez* - *namchaithailand*
Lower & Uppercase letters *(mixedalpha)*	**6,737,456**	**6.69%**	- *DenisedeRidder* - *BlackMightyWax*
Lowercase letters & special characters *(loweralphaspecial)*	**5,394,563**	**5.36%**	- *pimbava-os* - *@mb@|it*
Uppercase letters and numbers *(upperalphanum)*	**5,044,179**	**5.01%**	- *CIZAWOVY1* - *EDUARDO6592*
Lower & uppercase letters & special characters *(mixedalphaspecial)*	**2,432,456**	**2.42%**	- *All'Arrabbiatela* - *Baker_tentb*
Lowercase letters, special characters & numbers *(loweralphaspecialnum)*	**3,811,000**	**3.78%**	- *rhs;ysq52* - *promu|gat*
Numbers only *(numeric)*	**3,303,380**	**3.28%**	- *66748719* - *87925501*
Lower & uppercase letters, special characters & numbers *(mixedalphaspecialnum)*	**1,582,514**	**1.57%**	- *D3PR3Da7!0NS* - *75Henri-*

SPECOPS

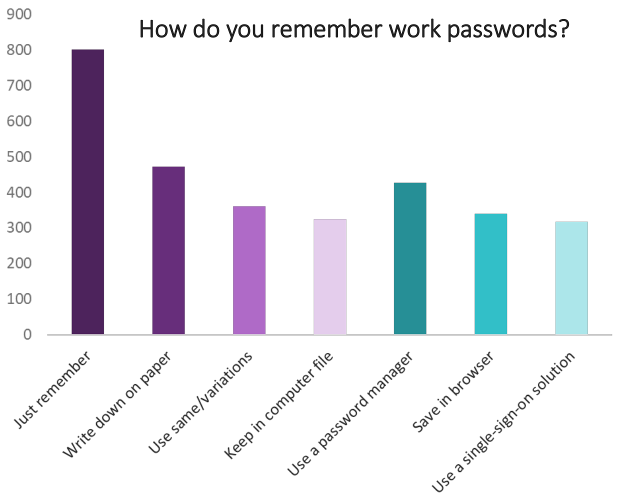
The above breakdown indicates that adding most of RockYou2021 to a breached password protection list is not required, as sufficient complexity rules could protect against over 95 percent of the records. By simply requiring upper, lower, numbers, and special characters, one would rule out a valid password being contained in the following categories (comprising of 96.5 percent of our sample).

At the end of the day, RockYou2021 was not a large dump of breached passwords (though it did contain some). However, it is still a wordlist which attackers may choose to use in their attacks against your network. Other notable breached password lists that could be used against your network:

- UK National Crime Agency's 230 million compromised password list
- Cit0Day with 226 million compromised passwords
- Collection #1 with 772 million accounts

Security Gaps with Enterprise Passwords

Specops Software surveyed more than 2,000 office workers to discover the role passwords play in their day-to-day lives, both personally and professionally. 54 percent of the people surveyed rely on insecure methods for managing their enterprise passwords such as writing down on physical paper (472 respondents), using the same or variations of the same password (361 respondents), and storing passwords in a computer file (325 respondents).



65 percent of the respondents reported sharing passwords at work and the majority of these people say the method they use to share passwords is to "just remember them." These shared passwords are likely to be weak or reused across multiple business systems since it is difficult for people to remember long and complex passwords.

Nearly half of the people surveyed (48 percent) have 11 or more passwords they have to remember for work. For personal use, the numbers were even higher with 71 percent of respondents reporting using 11 or more passwords. Using so many passwords in both personal and professional settings leads to poor password practices such as password reuse.

Businesses Fail to Verify Password Resets

Specops Software surveyed enterprises globally to understand how they were handling user verification at the IT service desk and found 48 percent of organizations do not have a user verification policy in place for incoming calls. The information was uncovered as part of our survey of more than 200 IT leaders from the private and public sectors in North America and Europe.

In addition, the survey revealed that 28 percent of the companies that do have a user verification policy in place are not satisfied with their current policy due to security and usability issues. For example, most of these companies rely on knowledge-based questions using static Active Directory information, such as an employee ID, a manager's name, or even HR-based information like the employee's date of birth or address – data that can easily be sourced by hackers. In fact, the NIST recommends against using knowledge-based questions because of their lack of security.

Real-life example: EA Games

To understand how wide-spread the risk is, look no further than the 2021 EA Games breach. A group of hackers, who were able to gain access to internal systems and steal data from game publisher Electronic Arts (EA Games) in part, by tricking an employee over Slack to provide a login token. A representative for the hackers told Motherboard in an online chat that the process started by purchasing stolen cookies being sold online for $10 and using those to gain access to a Slack channel used by EA, according to Vice. Since EA Games didn't have an enforced end-user verification software in place the hackers were successful in tricking the service desk.

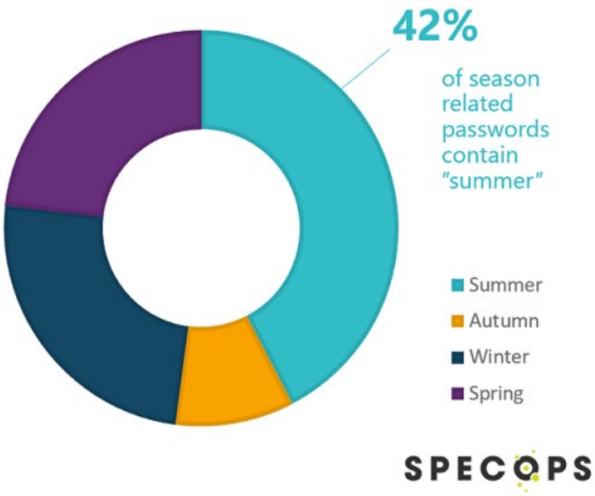
Once they gained access, the hackers stole the source code for FIFA 21 and related matchmaking tools, as well as the source code for the Frostbite engine that powers games like Battlefield and other internal game development tools. In all, the hackers claim they have 780GB of data, and are advertising it for sale on various underground forums. While most hackers are motivated by the profits of their exploits, the ramifications for an organization like EA could be devastating.

Compromised passwords: themes and patterns

While just about any password can be compromised and used in attacks on businesses, highlighting those that are more popular demonstrates the difficulty most people have coming up with a password that is not easy to guess. Many people reuse a password once they have chosen one that meets most complexity requirements, rather than memorizing multiple complex passwords. As it's common for people to choose root words based on their interests, Specops Software analyzed large data sets of compromised passwords in order to find recurring themes.

The results show that people turn to seasons, musicians, sports teams, movies, and TV shows when choosing passwords. Since this analysis was undertaken on known compromised passwords, these pop culture passwords are already being used by hackers in real-world attacks.

Seasons and months



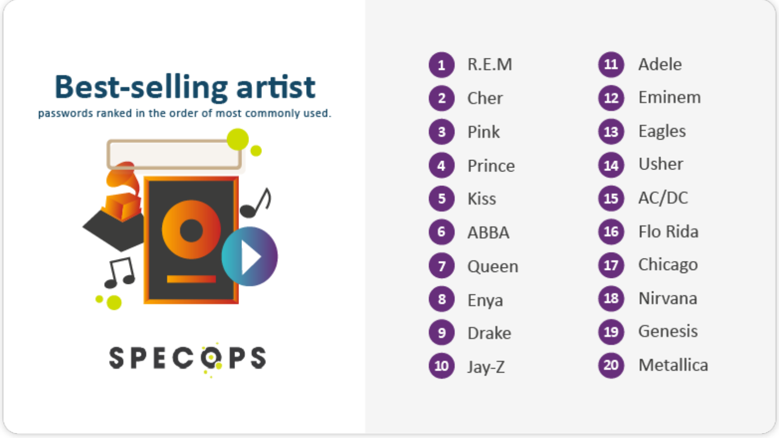
Summer was found to be the most popular season when looking at a password set of over 800 million leaked passwords.

Our team discovered which month of the year was most popular in passwords. May topped the list across multiple languages – English, German (Mai), French (Mai); whereas Swedish and Spanish preferred July (Juli) and June (Junio) respectively.

Best-selling artists

In honor of the 2021 Grammy awards, the Specops Software research team analyzed over 800 million passwords for any entry containing the artist or group name on Wikipedia's best-selling list.

The team pulled a few head-to-head pairings to answer the question of which artist is more popular in leaked passwords.

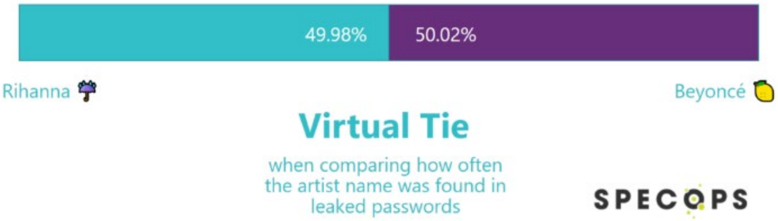


Best-selling artist

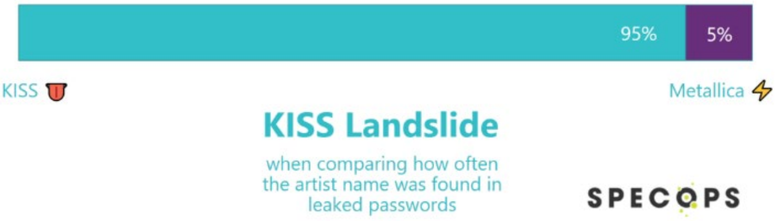
passwords ranked in the order of most commonly used.

1. R.E.M
2. Cher
3. Pink
4. Prince
5. Kiss
6. ABBA
7. Queen
8. Enya
9. Drake
10. Jay-Z
11. Adele
12. Eminem
13. Eagles
14. Usher
15. AC/DC
16. Flo Rida
17. Chicago
18. Nirvana
19. Genesis
20. Metallica

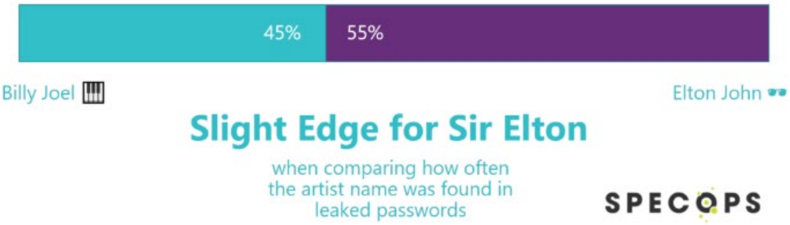
While Rihanna holds the top spot on Wikipedia’s best-selling list, Beyoncé fans have a slight edge in honoring their favorite in their password but it’s a virtual tie.



While true that KISS may be benefiting from the general use of the word in passwords, Metallica fans are way less likely to show their fandom in their passwords.



When comparing the two piano players, our team found Sir Elton John’s name was used slightly more in passwords than Billy Joel’s.

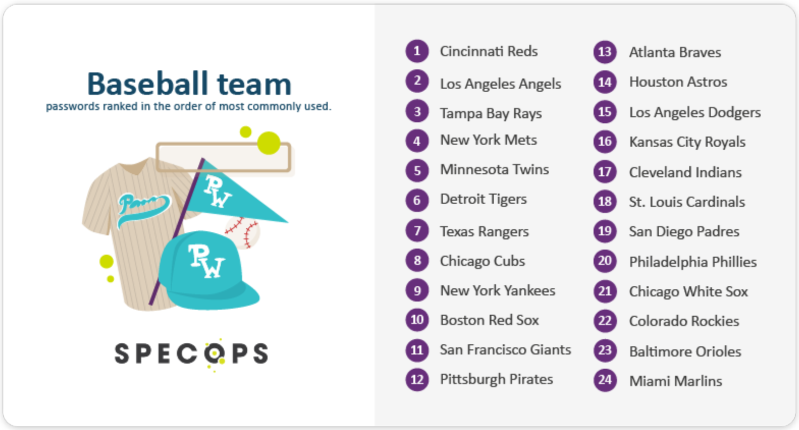


Baseball teams

The Cincinnati Reds, America’s oldest baseball team, tops the list of baseball teams in an analysis of Specops’ breached password list.

In total, the Specops Software research team found that ‘Cincinnati Reds’ appears within breached password lists almost 150,000 times.

The Los Angeles Angels, Tampa Bay Rays, New York Mets and Minnesota Twins round out the top five MLB teams identified in our analysis. In contrast, the Arizona Diamondbacks, Toronto Blue Jays and Oakland Athletics are the least likely MLB team names to be used in passwords, the research found.



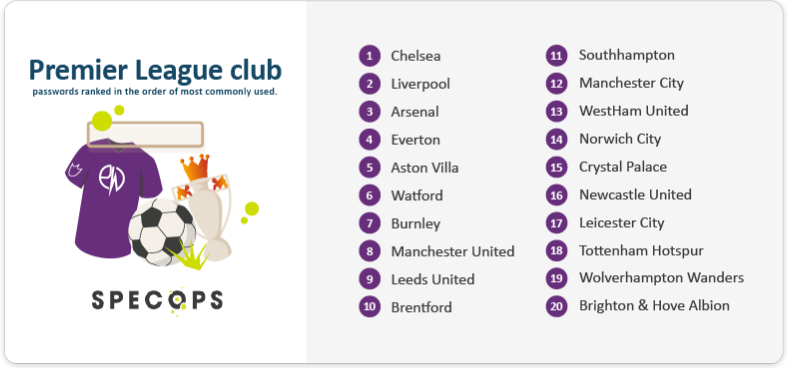
Baseball team
passwords ranked in the order of most commonly used.

1	Cincinnati Reds	13	Atlanta Braves
2	Los Angeles Angels	14	Houston Astros
3	Tampa Bay Rays	15	Los Angeles Dodgers
4	New York Mets	16	Kansas City Royals
5	Minnesota Twins	17	Cleveland Indians
6	Detroit Tigers	18	St. Louis Cardinals
7	Texas Rangers	19	San Diego Padres
8	Chicago Cubs	20	Philadelphia Phillies
9	New York Yankees	21	Chicago White Sox
10	Boston Red Sox	22	Colorado Rockies
11	San Francisco Giants	23	Baltimore Orioles
12	Pittsburgh Pirates	24	Miami Marlins

Premier League clubs

Chelsea, one of England's most successful football clubs, rank in first place on Specops' breached password list.

In total, the research found that 'Chelsea' appears within breached password lists almost 66,000 times.



Premier League club
passwords ranked in the order of most commonly used.

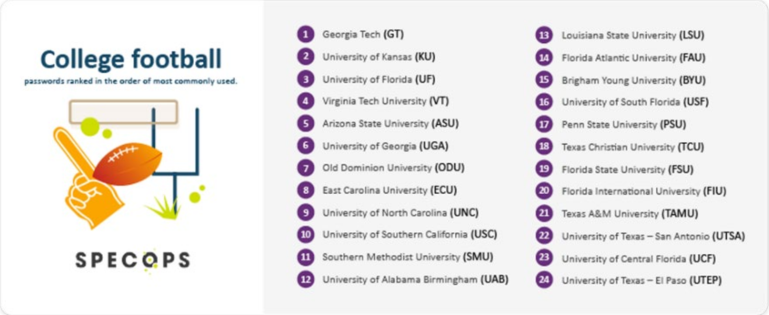
1. Chelsea
2. Liverpool
3. Arsenal
4. Everton
5. Aston Villa
6. Watford
7. Burnley
8. Manchester United
9. Leeds United
10. Brentford
11. Southhampton
12. Manchester City
13. WestHam United
14. Norwich City
15. Crystal Palace
16. Newcastle United
17. Leicester City
18. Tottenham Hotspur
19. Wolverhampton Wanders
20. Brighton & Hove Albion

SPECOPS

Liverpool, Arsenal, Everton and Aston Villa round out the top five teams identified in our analysis. In contrast, Brighton and Wolves are the least likely Premier League club names to be used in passwords, the research found.

College Football

The Specops Software research team looked at passwords related to top football playing schools and found that Georgia Tech or (GT), the University of Kansas or (KU) and the University of Florida or (UF) each appear more than 5 million times on breached password lists.



College football
passwords ranked in the order of most commonly used.

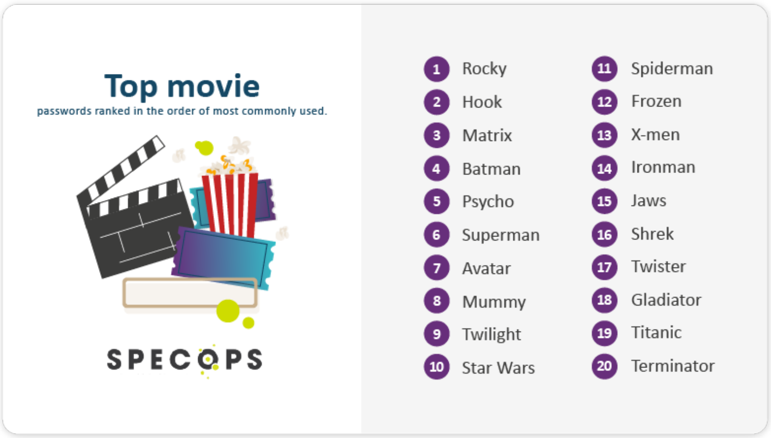
1. Georgia Tech (GT)
2. University of Kansas (KU)
3. University of Florida (UF)
4. Virginia Tech University (VT)
5. Arizona State University (ASU)
6. University of Georgia (UGA)
7. Old Dominion University (ODU)
8. East Carolina University (ECU)
9. University of North Carolina (UNC)
10. University of Southern California (USC)
11. Southern Methodist University (SMU)
12. University of Alabama Birmingham (UAB)
13. Louisiana State University (LSU)
14. Florida Atlantic University (FAU)
15. Brigham Young University (BYU)
16. University of South Florida (USF)
17. Penn State University (PSU)
18. Texas Christian University (TCU)
19. Florida State University (FSU)
20. Florida International University (FIU)
21. Texas A&M University (TAMU)
22. University of Texas – San Antonio (UTSA)
23. University of Central Florida (UCF)
24. University of Texas – El Paso (UTEP)

SPECOPS

University of Central Florida or (UCF), University of Texas – El Paso or (UTEP) and the University of California Los Angeles (UCLA) appear the least.

Top Movies

Fan favorite 'Rocky' took the #1 spot, showing up on breached password lists nearly 96,000 times, according to the research. Trailing close behind was 'Hook', which showed up in over 75,000 breached password lists and the 'Matrix' at more than 50,000.



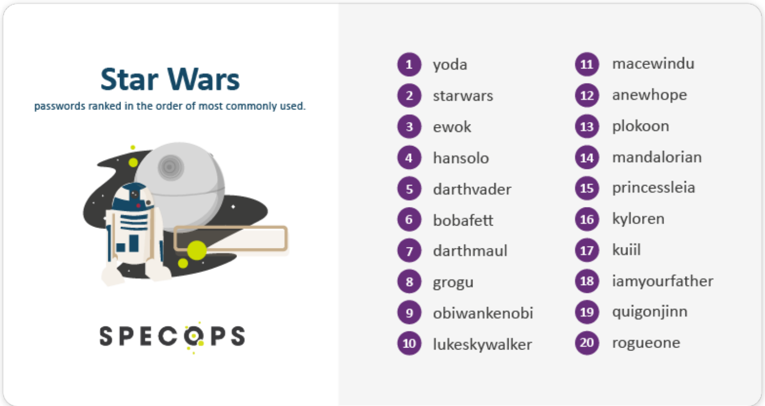
Top movie
passwords ranked in the order of most commonly used.

1. Rocky
2. Hook
3. Matrix
4. Batman
5. Psycho
6. Superman
7. Avatar
8. Mummy
9. Twilight
10. Star Wars
11. Spiderman
12. Frozen
13. X-men
14. Ironman
15. Jaws
16. Shrek
17. Twister
18. Gladiator
19. Titanic
20. Terminator

SPECOPS

Star Wars

According to the research, Yoda took the #1 spot, showing up on breached password lists nearly 37,000 times. After that, “starwars” itself took the number two spot, showing up over 22,000 times with the adorable “ewok” trailing close behind at over 17,000 times.



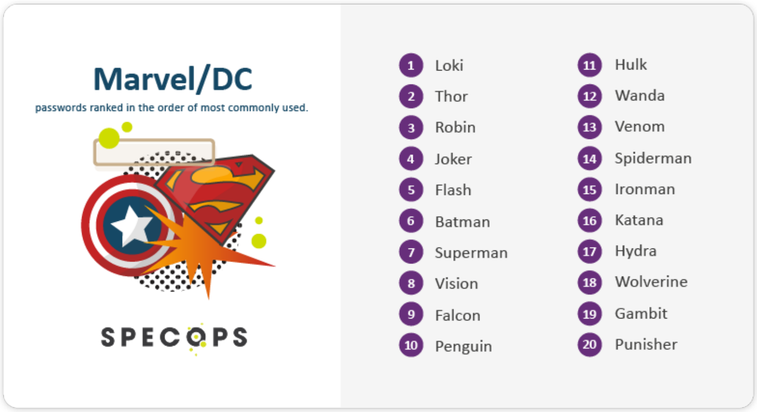
Star Wars

passwords ranked in the order of most commonly used.

1. yoda
2. starwars
3. ewok
4. hansolo
5. darthvader
6. bobafett
7. darthmaul
8. grogu
9. obiwankenobi
10. lukeskywalker
11. macewindu
12. anewhope
13. plokoon
14. mandalorian
15. princessleia
16. kyloren
17. kuiil
18. iamyourfather
19. quigonjinn
20. rogueone

Marvel vs. DC

According to our research, ‘Loki’ (Marvel) took the top spot, appearing on breached password lists more than 151,000 times. ‘Thor’ (Marvel), which appears almost 148,000 times and ‘Robin’ (DC), which shows up over 127,000 times to round out the top three.



Marvel/DC

passwords ranked in the order of most commonly used.

1. Loki
2. Thor
3. Robin
4. Joker
5. Flash
6. Batman
7. Superman
8. Vision
9. Falcon
10. Penguin
11. Hulk
12. Wanda
13. Venom
14. Spiderman
15. Ironman
16. Katana
17. Hydra
18. Wolverine
19. Gambit
20. Punisher

Bottom line: Address the Problem

Passwords are easy to attack because people often use vulnerable passwords that are easily guessed or already compromised. These passwords are vulnerable because people reuse them across various personal and professional platforms, and because they follow typical patterns and themes at the point of creation. This makes it more likely that they end up on breached lists which are then used repeatedly in password attacks.

Making passwords complex creates passwords that are difficult for people to remember, and easy for hackers to exploit. As long as people reuse passwords, making these more secure comes down to disallowing all known compromised passwords.

This is why it is so important to understand where your organization's password usage and policies could be leaving you vulnerable to an attack. Let 2022 be the year that your organization addresses the problem of password reuse before suffering the consequences of a cyber-attack.