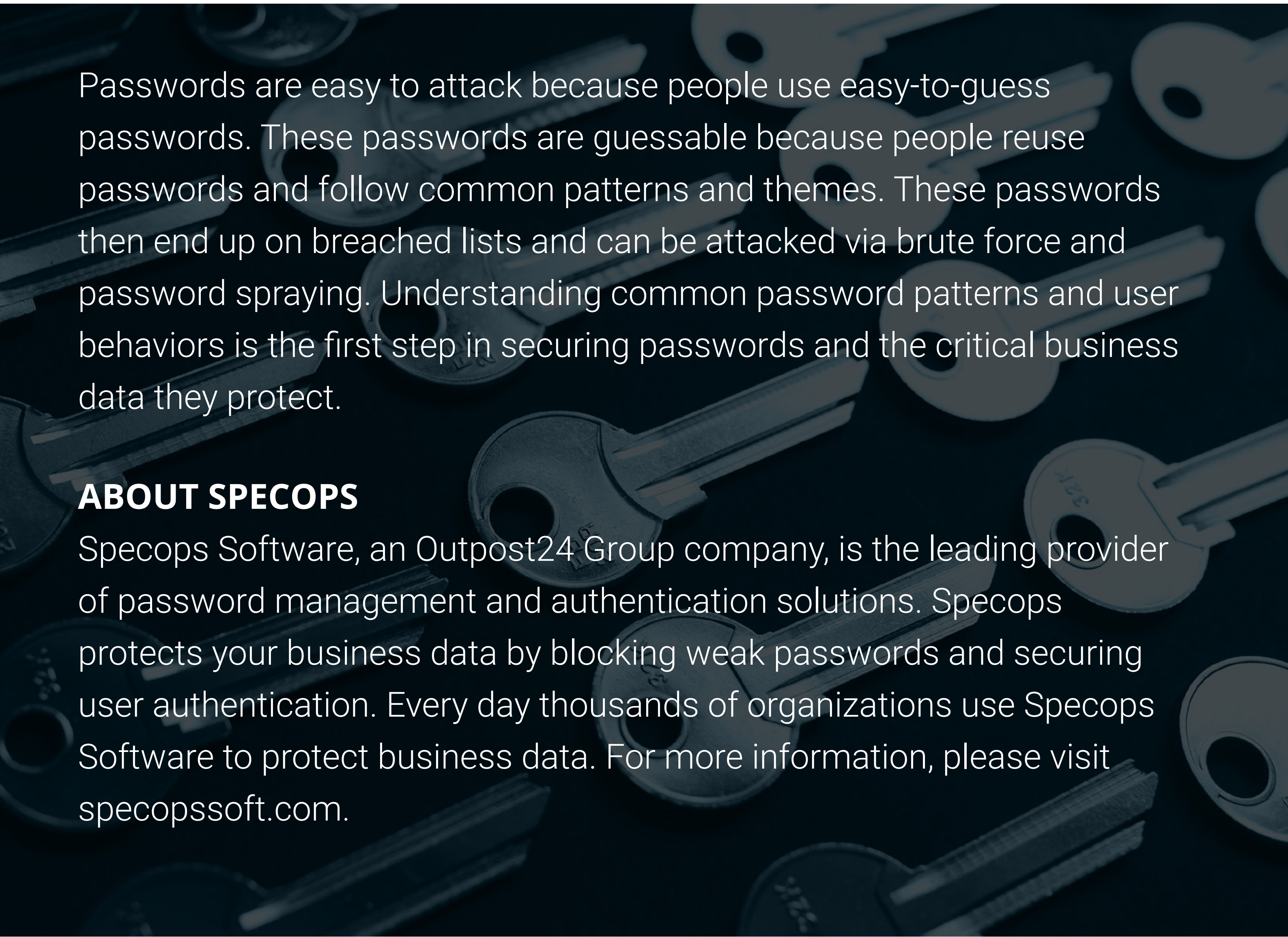
SPECOPS
AN OUTPOST24 COMPANY

Weak Password Report

2023



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.

1. Executive Summary

Poor password practices are putting businesses at risk. Data breaches continue to be a threat to all types of organizations across the globe, underscoring the importance of greater password security, as a means to protect our business data, as well as our digital ecosystem.

This year's Weak Password Report highlights why passwords are still the weakest link in an organization's network, and how stronger password policy enforcement can be your best defense.

The research in this report has been compiled through various methods, including:

- Our analysis of 800 million breached passwords, a subset of the more than 3 billion unique compromised passwords within the Specops Breached Password Protection list.
- Our analysis of passwords found in live attacks on our team's honeypot network, another source for compromised passwords blocked by the Specops Breached Password Protection list.

The highlights from this year's report include:

- 83% of compromised passwords satisfy the password length and complexity requirements of regulatory password standards.
- 88% of passwords used to attack RDP ports in live attacks are 12 characters or less.
- The most common base term found in passwords used to attack networks across multiple ports is still password.

The data in this report should bring awareness to this all-too-common problem. The next step is to act, which means blocking weak and compromised passwords, enforcing password length requirements, 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.

2. The Case for Password Protection

Poor password practices or policies can make your organization vulnerable to cyber-attacks. The unfortunate truth is that most people don't follow password best practices. According to a recent Password Manager Report, 41% of Americans rely on memory alone to track their digital passwords, suggesting the use of simple and repeatable passwords to make them easier to remember. Additionally, of those that choose to use an online password manager to store their information, nearly half store both personal and work passwords together.

Even with end-user training, password reuse and other risky practices are all too common, both for personal and business use. To protect corporate data, additional enforcement measures are required. For most business, this starts with protecting Active Directory, the universal authentication solution for Windows domain networks. Third-party password security software can strengthen Active Directory accounts. A secure password policy, preferably one that can block the use of compromised passwords, is most critical.

2.1 Password Length and Complexity Alone Is Not the Answer

There are several compliance regulations that set the standards for cybersecurity, including organizational password policies. Traditionally, these regulations have mainly endorsed length and complexity requirements in the password policy design. But, given the growing sophistication of password attacks, today's requirements now include checking credentials against a breached password list.

The Specops Software research team analyzed over 800 million compromised passwords and tested them against five different regulatory standards to see if they met the requirements set by each of these standards. Our analysis found that 83% of compromised passwords would satisfy the password complexity and length requirements of compliance standards.

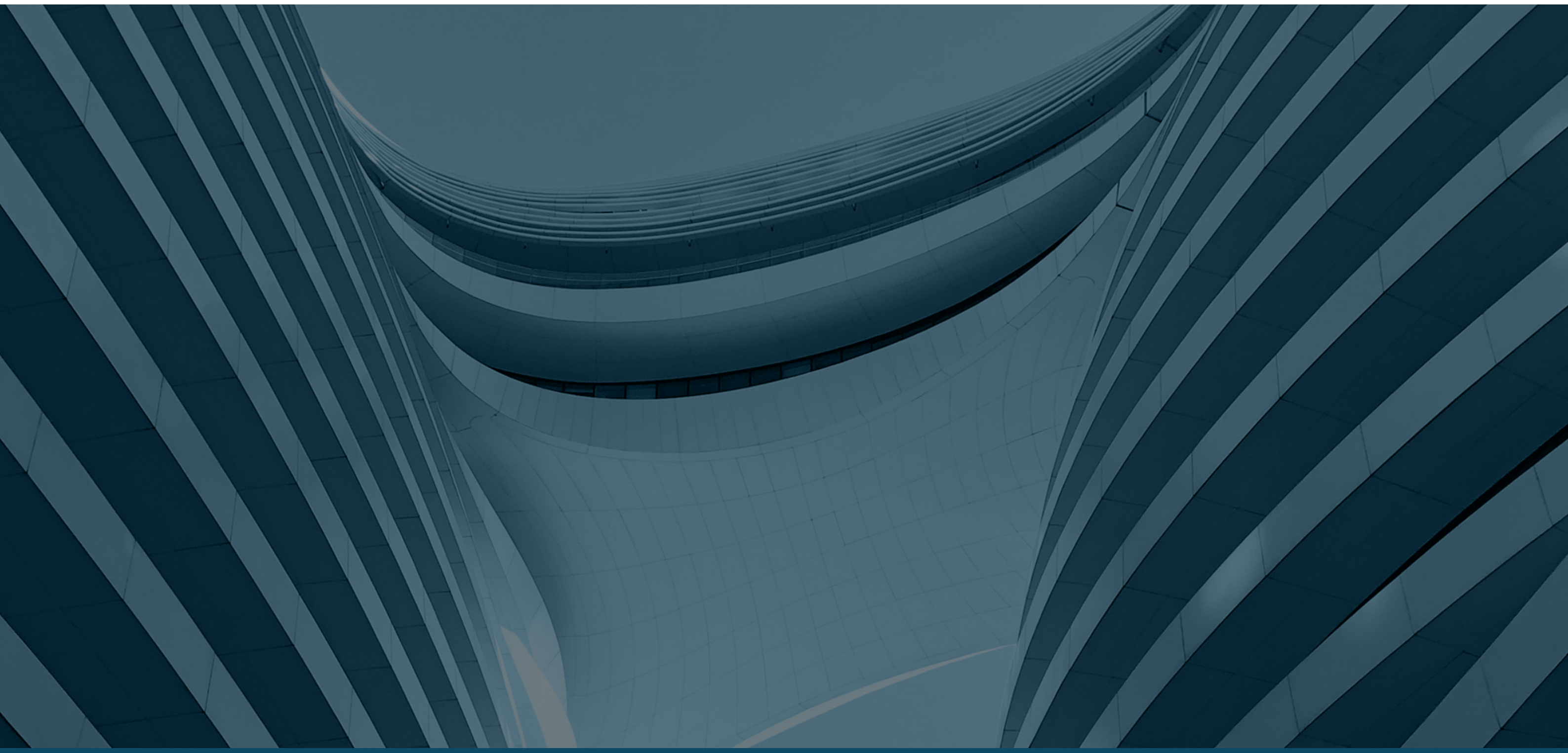
The regulatory standards we investigated were:

- NIST
- HITRUST for HIPAA
- PCI
- ICO for GDPR
- Cyber Essentials for NCSC

Whether you are following a regulatory standard or not, this data tells us that a compromised password check is critical for all organizations.

Recommended actions to prevent the use of compromised passwords

ICO/GDPR: Block the use of common and weak passwords. Screen passwords against a password list of the most commonly used passwords, leaked passwords from breaches, and guessable passwords related to the organization. Update the leaked password list regularly, and explain to users why their passwords have been rejected.



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

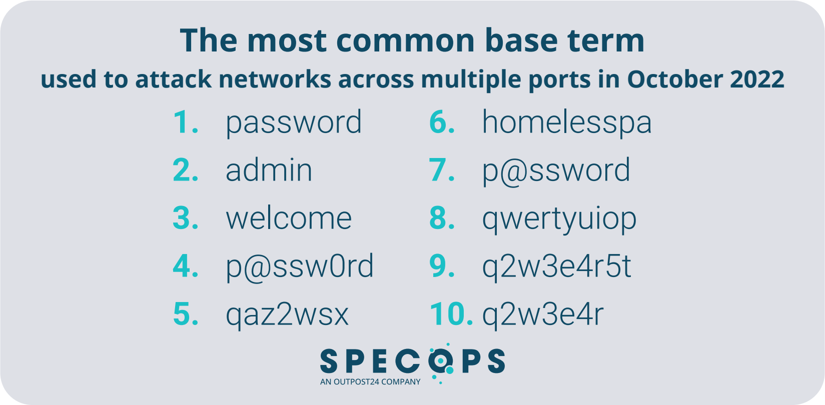
One common way that cyber criminals are gaining access to organization's sensitive data and networks is through brute force attacks. These attacks consist of using a list of common, probable, and even breached passwords to systematically run them against a user's email to gain access to a given account.

This section will provide a breakdown of how passwords can be an entry point to your organization's network — and what you can do for protection.

3.1 Brute Force and Password Construction

In October 2022, our research team took a look at passwords being used to attack RDP ports in live attacks and analyzed a subset of over 4.6 million passwords collected over the span of several weeks. We identified patterns in recent attacks and uncovered that more than 88% of passwords used in attacks were 12 characters or less. The most common password length found in this attack data was 8 characters at almost 24%.

Another key finding in password construction was the use of special characters. Passwords containing only lowercase letters were the most common character combination found, making up 18.82% of the set.



The most common base term

used to attack networks across multiple ports in October 2022

1. password
2. admin
3. welcome
4. p@ssw0rd
5. qaz2wsx
6. homelesspa
7. p@ssword
8. qwertyuiop
9. q2w3e4r5t
10. q2w3e4r

SPECOPS
AN OUTPOST24 COMPANY

These are common terms people use over and over again across different accounts, both professional and personal. Attackers are still finding success in attacking ports with weak, common, and leetspeak powered wordlists. Even if more sophisticated attacks are on an organization's radar, it's just as important to protect against the most basic tactics targeting the weakest link.

Most interesting about this dataset might be the inclusion of "homelesspa" – a password base term found in the 2016 MySpace leak, giving us insight into the lists used by attackers to attack networks. We also see this term in the NCSC Top 100k list published in 2019. This base term indicates that even if a wordlist or breach is "old," it is still worth protecting against as attackers are still using them to compile their attack lists.

Organizations looking to prevent the use of passwords like these must make use of password construction rules such as implementing the use of passphrases, and length-based password aging to encourage memorable long passwords. Those requirements, paired with a custom dictionary or compromised password screening, would be the best defense against passwords that could help threat actors gain access to your organization's network.

3.2 Real-life example: Nvidia

In February of 2022, GPU manufacturer Nvidia was the victim of a massive data breach conducted by the ransomware group LAPSUS$. The threat actor breached their network to steal employee passwords, as well as proprietary company information, and proceeded to leak the data online for ransom.

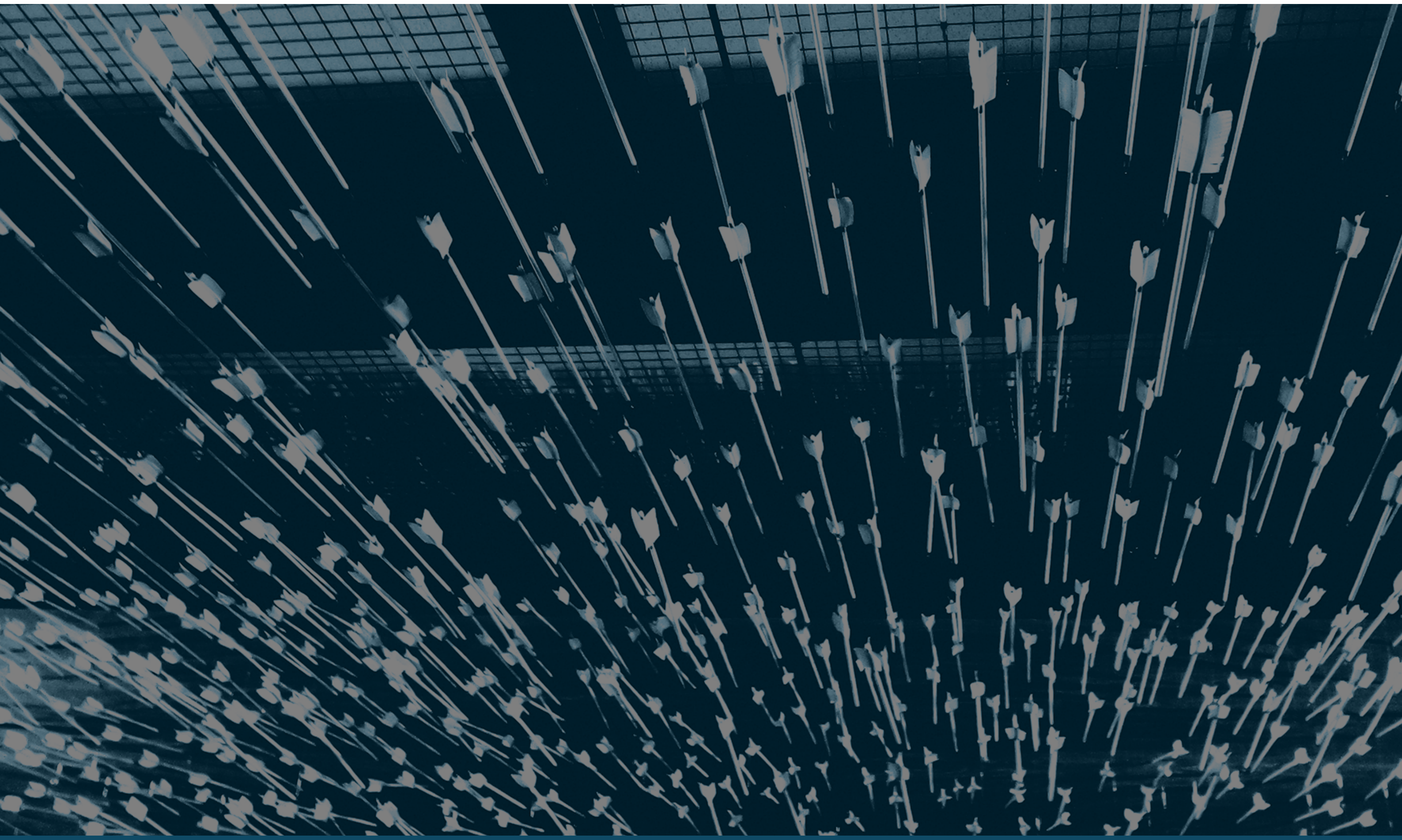
During the breach, thousands of employee passwords were leaked. Specops Software obtained 30,000 of these leaked passwords and added them to our database of compromised passwords. Nvidia later shared that all employees were required to change their passwords. Now that these passwords are no longer in use, we can look at a few examples to pinpoint the factors that led to their compromise.

Top 10 Base Words in Leaked Nvidia Passwords

1. nvidia
2. nvidia3d
3. mellanox
4. ready2wrk
5. welcome
6. password
7. mynvidia3d
8. nvda
9. qwerty
10. september

Finding "nvidia" in this list indicates the organization wasn't making use of a custom dictionary in its password protections. A custom dictionary list is set up to reject common and predictable passwords during the password creation process. These can include passwords relevant to your organization, including name, locations, services, any relevant acronyms, and even months of the year, as per the "September" example above.

The cyberattack on America's largest microchip company understandably sparked concern for data security. But it comes as no surprise when you consider that commercial and business-related companies are the most affected by ransomware attacks, according to Outpost24's 2023 Ransomware Report. Their data suggests that threat actors primarily target organizations that may have a higher capacity to pay a ransom.



4. Compromised Passwords: Themes and Patterns

In our analysis of the more than 800 million compromised passwords we've collected, there are several themes and patterns that emerge.

When it comes to password creation, there is a strong tendency to get inspired by world or cultural events. Many people look to their surroundings when creating their passwords and use their interests or cultural trends to influence the phrases they end up using for their passwords.

Hackers are aware of this tendency and use it as an opportunity to tap into commonly known terms or phrases to target unsuspecting victims.

4.1 Football is a universal (password) language

It is often said that football (soccer) is a universal language. Our research found this to be true within passwords.

As the FIFA 2022 World Cup kicked off in Qatar, our research team uncovered numerous World Cup-related terms in the compromised password database, many of which are mentioned frequently. "Soccer" tops the related terms list with over 140,000 inclusions, with "Football" coming in second place. England's international stadium Wembley also makes it into the top 10, appearing over 1,600 times in passwords.

When it comes to players, both current and former, a few stand out in the mentions. Grzegorz Lato, a former player from Poland's golden generation, topped the list appearing over 174,000 times. Another frequent appearance was Pele, arguably the greatest player ever, who landed just outside the top 10 with over 70,000 mentions. Current football players Messi and Ronaldo also made appearances on the mentions list, which comes as no surprise given the large fan bases each of these players currently has.

World Cup legend rankings
(in passwords)

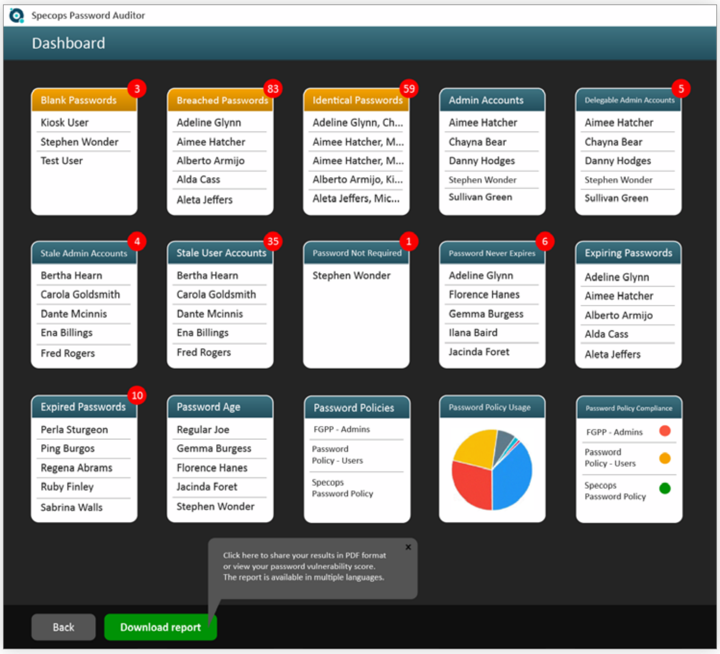
1. Lato
2. Carlos
3. Kane
4. Didi
5. Villa
6. Henry
7. Hagi
8. Milla
9. Xavi
10. Rossi
11. Pele
12. Santos
13. Moore
14. Messi
15. Vava
16. Walter
17. Kopa
18. Ronaldo
19. Monti
20. Zico

While there is no guarantee the more common terms contained within passwords will be attributed to a player every time, it is common for users to choose well-know terms and names, and highly likely there is intent when less common surnames appear.

5. Take action: Protect your organization with Specops

From ransomware to password guessing and brute force attacks, as long as threat actors continue to evolve their tactics, organizations must be proactive with their password protections to defend their overall network security.

Test your resilience against credential-based attacks with the free Specops Password Auditor. The read-only tool scans your Active Directory for password-related vulnerabilities, including which accounts are using compromised passwords.



Specops Password Auditor

Dashboard

Blank Passwords 3
Kiosk User
Stephen Wonder
Test User

Breached Passwords 83
Adeline Glynn
Aimee Hatcher
Alberto Armijo
Alda Cass
Aleta Jeffers

Identical Passwords 59
Adeline Glynn, Ch...
Aimee Hatcher, M...
Aimee Hatcher, M...
Alberto Armijo, Ki...
Aleta Jeffers, Mic...

Admin Accounts
Aimee Hatcher
Chayna Bear
Danny Hodges
Stephen Wonder
Sullivan Green

Delegable Admin Accounts 5
Aimee Hatcher
Chayna Bear
Danny Hodges
Stephen Wonder
Sullivan Green

Stale Admin Accounts 4
Bertha Hearn
Carola Goldsmith
Dante Mcinnis
Ena Billings
Fred Rogers

Stale User Accounts 35
Bertha Hearn
Carola Goldsmith
Dante Mcinnis
Ena Billings
Fred Rogers

Password Not Required 1
Stephen Wonder

Password Never Expires 6
Adeline Glynn
Florence Hanes
Gemma Burgess
Ilana Baird
Jacinda Foret

Expiring Passwords
Adeline Glynn
Aimee Hatcher
Alberto Armijo
Alda Cass
Aleta Jeffers

Expired Passwords 10
Perla Sturgeon
Ping Burgos
Regena Abrams
Ruby Finley
Sabrina Walls

Password Age
Regular Joe
Gemma Burgess
Florence Hanes
Jacinda Foret
Stephen Wonder

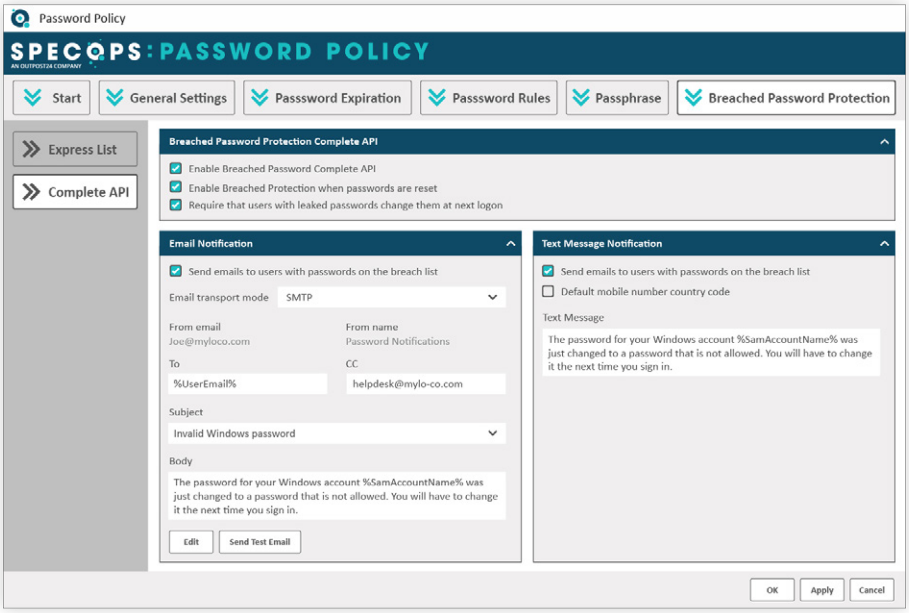
Password Policies
FGPP - Admins
Password Policy - Users
Specops Password Policy

Password Policy Usage

Password Policy Compliance
FGPP - Admins 🟥
Password Policy - Users 🟧
Specops Password Policy 🟩

Click here to share your results in PDF format or view your password vulnerability score. The report is available in multiple languages.

For better password security, Specops Password Policy encourages strong and unique passwords, that are harder to predict and crack. With the Breached Password Protection feature you can even block more than 3 billion unique compromised passwords collected by Specops Software.



Password Policy

SPECOPS: PASSWORD POLICY

Breached Password Protection Complete API

☑ Enable Breached Password Complete API
☑ Enable Breached Protection when passwords are reset
☑ Require that users with leaked passwords change them at next logon

Email Notification

☑ Send emails to users with passwords on the breach list

Email transport mode: SMTP

From email: Joe@myloco.com
From name: Password Notifications
To: %UserEmail%
CC: helpdesk@mylo-co.com
Subject: Invalid Windows password
Body: The password for your Windows account %SamAccountName% was just changed to a password that is not allowed. You will have to change it the next time you sign in.

Text Message Notification

☑ Send emails to users with passwords on the breach list
☐ Default mobile number country code

Text Message: The password for your Windows account %SamAccountName% was just changed to a password that is not allowed. You will have to change it the next time you sign in.

Request a demo or a free trial and see how we can help secure your weakest link.