SpyCloud

Special Report:

2021 U.S. Government Credential Exposure

270K

CREDENTIALS WITH .GOV EMAILS EXPOSED IN 2020

87%

.GOV EMPLOYEE PASSWORD REUSE RATE

79%

PASSWORD REUSE RATE FOR DEFENSE INDUSTRIAL BASE SUPPLIERS

Abcd1234

TOP EXPOSED PASSWORD ASSOCIATED WITH .GOV EMAIL ADDRESSES

Introduction

Organizations everywhere are caught in a vicious cycle of cyberattacks. Responding to these attacks is incredibly disruptive and costly; the average remediation cost for a single ransomware attack has more than doubled in the last year, from $761,106 to $1.85M. As financial impact from data breaches slammed organizations across the board, the public sector saw a 79% increase in average total cost, from $1.08 million in 2019 to $1.93 million in 2020. As attacks and costs both surge, it's become clear that the United States government must brace itself for this new era of cybercrime.

There is arguably no bigger producer, collector, consumer, and disseminator of data on the planet than the United States government. And yet its vast network of employees at the federal, state and local levels, including its contractors, happen to be some of the more careless practitioners of credential hygiene according to our analysis – particularly with their .gov account passwords, which may be the only security measure standing between highly sensitive assets and criminal eyes.

Among the agencies that require layered defenses like multi-factor authentication (MFA), there is a false belief that it's enough to stop determined cybercriminals. With the uptick in phishing and malware campaigns targeting government employee credentials and web session cookies in 2020 – a 67% increase over the previous year – MFA is simply not enough.

The U.S. government relies heavily on information technology to improve efficiencies and optimize citizen engagement. Data held by government agencies is extremely valuable to cybercriminals (especially those working on behalf of countries with long histories of hostility toward the U.S.) as it includes personally identifiable information (PII) on government employees and citizens, as well as access to classified assets and intellectual property.

As this report explains, the prevalence of password reuse and loose credential security protocols are gifts to cybercriminals that expose the U.S. to significant risks. Yes, human behavior makes password habits difficult to control, but the current situation is untenable. It demands immediate attention and action to fix, along with a new framework for credential security that applies to employees, suppliers, and citizens; one in which:

- ✓ **Users are blocked from choosing and reusing passwords that have previously been compromised.**
- ✓ **Malware-infected machines are quickly investigated and remediated.**
- ✓ **Stolen data is negated early in the attack lifecycle, cutting off criminals' ability to profit from it.**

Critical Infrastructure and Services in the Crosshairs

On May 7, 2019, the city of Baltimore was hit by a ransomware attack demanding the equivalent of $76,000 in bitcoin. Attackers broke in through an open server in Baltimore's network and installed a back door to move across the city's computers, searching for valuable servers to infect. To spread the ransomware, it used an NSA-developed software called Eternal Blue in conjunction with a technique known as "pass-the-hash," which leverages stolen credentials without having to crack the passwords. The city refused to pay the ransom. Their recovery lasted several weeks and cost at least $18 million.

Baltimore ultimately became a poster child for the consequences of ransomware targeting government infrastructure. Sadly, they wouldn't be the last. As the pandemic upended traditional IT and security operations in 2020, nearly 2,400 U.S.-based governments, healthcare facilities, and schools were victims of ransomware. These attacks disrupted medical treatment, forced ambulances to be rerouted, and disabled public transportation.

In the United States, cyberattacks have been a cause for concern for years. Not only has the frequency of breaches increased, but so have the global and economic implications. In 2018, the United States topped the list of countries financially affected by cybercrime; industry experts estimate that the U.S. government faced costs of over $13.7 billion as a result of cyberattacks. In the last three years, ransomware attacks on the government alone have cost $52.88 billion in recovery and downtime. The number of people affected is estimated to be around 200 million.

Now ransomware is targeting U.S. critical infrastructure. This includes systems and assets supporting emergency services, telecommunications networks, and energy production and transmission facilities. Currently, ransomware attacks are occuring at a relentless pace – an estimated 4,000 attacks happen every day (one every 11 seconds).

The following major incidents became big media headlines in just a 6 month span:

- **December 2020: Federal law enforcement received numerous reports of ransomware attacks against K-12 educational institutions. These attacks targeted school computer systems, slowing access, and in some cases rendering the systems inaccessible to remote learning.**

- **December 2020: Attackers infiltrated at least 18,000 U.S. government and private networks in the SolarWinds supply chain attack, an unprecedented campaign that opened doors for follow-on attacks in 2021**.

- **May 2021: Colonial Pipeline announced that it was the victim of a ransomware attack that led to temporary disruption in the delivery of gasoline and other petroleum products across much of the southeast U.S. Colonial paid over $2 million in ransom, later revealing that the attack started with a single compromised password.**

- **June 2021: JBS, a meat processing company, was targeted with ransomware that affected the company's operations and threatened food supplies. The company reportedly paid $11 million in ransom.**

These events, ransomware or otherwise, all share a similar pattern: stolen or compromised credentials were leveraged by criminals to access networks and spread infections before anyone noticed.

Addressing the Password Problem

Over the last several years, the use of stolen or compromised credentials has emerged as the #1 attack vector leading to breaches. The public sector is no exception.

DEPARTMENT OF
DEPARTMENT OF
Username
JonSmith23
Password
MainStreet9
LOGIN
Username
JonSmith23
Password
MainStreet9
LOGIN
Username
JonSmith23
Password
MainStreet9
LOGIN

Password reuse presents significant security risks for government agencies and contractors, especially when employees bring their bad password hygiene to work. Too often, employees reuse corporate credentials as personal logins and vice versa. When third-party sites are subject to data breaches, reused employee logins give criminals easy paths to corporate data. For example, if an employee uses their work email and password to log onto a social media site, a criminal who breaches that site can easily connect the dots to access that employee's work account and more.

Unfortunately, due to human error, negligence and lack of resources, passwords and the people who use them are the weakest link in cybersecurity and the most common vehicle for cybercriminals to infiltrate government accounts.

Governments spend immense sums of money on cybersecurity defense, consultants and threat detection tools, such as firewalls, security information and event management (SIEM), and antivirus products. All of these tools have their place and can be very valuable, but they do little to address the fact that the overwhelming majority of attacks could be avoided if better attention was paid to passwords.

For any organization lacking the resources and solutions to protect themselves, it can feel impossible to get ahead of ransomware. Focusing on password security, however, makes addressing ransomware fairly straightforward; even the most under-funded localities can prevent it by understanding and negating the root cause of these attacks.

How Bad Credential Habits Fuel Attacks

We know the Colonial Pipeline ransomware attack started with a single compromised password found in a batch of stolen credentials from another breach. The use of stolen credentials to penetrate networks and install ransomware is, simply put, the easiest path for criminals.

For many years, organizations have been victims of data breaches that siphon vast troves of user data, including usernames and passwords. The spoils from these breaches are eventually made available on criminal marketplaces to anyone who wants to buy them. Because of the prevalence of password reuse, once criminals acquire exposed login credentials from one breach, they can use them to unlock more lucrative accounts.

This means that if a set of stolen credentials from a third-party breach contains a .gov email domain, criminals have an obvious clue that they could gain access to the network and potentially sensitive government information.

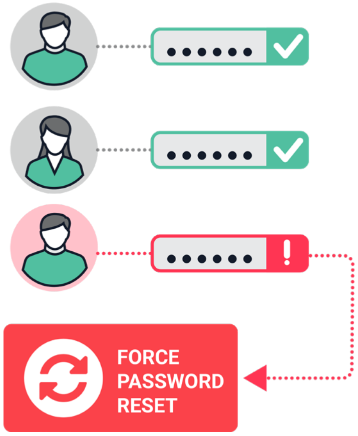
In our analysis of recaptured breach data, SpyCloud identified:

- 269,690 plaintext government credentials leaked in 465 breaches.
- More than 1 million pairs of exposed emails and passwords for corporate accounts at the 27 largest companies in the defense industrial base.
- 800,000 exposed corporate credentials (more than 7,000 per company) for employees at the 109 Fortune 1000 companies in the energy sector.

These exposures provide potential avenues for bad actors to access government resources and create massive risk in the government supply chain.

In addition, when it comes to government employees' password reuse habits, SpyCloud research shows that 87% are using the same passwords across .gov and personal accounts.

BAD HABIT →	CRIMINAL ADVANTAGE
We Choose Weak, Common Passwords Regardless of all the advice out there about the importance of strong passwords, users will choose sequential numbers and dictionary words or add a ! or 1 to the end of their password (especially when prompted to change passwords every 90 days by IT). Memorable passwords may seem unique to users – but they often are not.	**Password Spraying Attacks** Easy-to-remember passwords are also easy for bad actors to guess, making consumers vulnerable to password spraying. This is a brute force attack where a cybercriminal uses a list of usernames and common passwords to try to gain access to a particular site. Once they get a match, they'll test that same username and password combination against as many accounts as possible.
We Reuse Passwords Across Multiple Accounts An analysis of the SpyCloud database found a 60% password reuse rate among users exposed in more than one data breach in 2020. For employees with a .gov account, that rate is even worse: 87%. If a .gov user account shares a password with a personal account that is breached, it's easy for criminals to connect the dots and gain access to government data.	**Credential Stuffing Attacks** Password reuse literally enables credential stuffing, an attack that uses automation to check legitimate credential pairs against a number of websites to see which additional accounts can be taken over. Currently, an estimated 3.6 million of these attacks target Americans every day, and the FBI and CISA have recently begun issuing warnings about these brute force attacks.
We Click Links & Download Attachments from Unfamiliar Sources It's human nature to click any link or file that lands in our inbox, whether we recognize the sender or not. In worst-case scenarios, innocent clicks lead to our machines becoming infected with keylogger malware. In fact, 94% of malware is delivered by email.	**Keylogger Malware** Malware with keylogging components can record a user's every move, capturing browser history, session cookies, files, system information, and login data for corporate and third-party resources. In many cases, this information enables criminals to bypass MFA and directly access networks, opening the door for ransomware attacks.



Forced Reset: Closing the Government's Largest Cybersecurity Gap

U.S. government agencies are targeted in part because they are inadequately prepared and attackers know it. In its Federal Cybersecurity Risk Determination Report and Action Plan, the Department of Homeland Security (DHS) found that:

> ***"Agencies do not understand and do not have the resources to combat the current threat environment, agencies do not have standardized cybersecurity processes and IT capabilities, which impacts their ability to efficiently gain visibility and effectively combat threats, agencies lack visibility into what is occurring on their networks and especially lack the ability to detect data exfiltration."***

As we are seeing now, the situation at the city and state level is even more unstable. As was the case with Baltimore, many city governments use older operating systems, hardware and software, making them easier to attack. The reasons for this are largely due to lack of funding, which is not likely to change any time soon. Unfortunately, cybercrime wasn't much of a priority when the Justice Department laid out its $500 million grant program. Worse yet, FEMA indicates that in 2020, only 2% of DHS preparedness grants were used for cybersecurity. While the Biden administration has taken an aggressive stance on cybersecurity and indicated more stringent policies to come, the persistent complacency in basic credential security and password hygiene is unsustainable.

Local Government

This sector has the lowest ability of all sectors to stop data encryption and to restore data using backups. As a result, local governments have one of the highest propensities to pay the ransom – further encouraging attackers to target them.

Federal Government

Federal agencies are more skilled in stopping ransomware than local government due to their high investment in trained IT professionals and SOCs. In response, attackers focus on extortion-style attacks where they steal sensitive data and then threaten to expose it unless a ransom is paid.

Government Contractors/Supply Chain

Government contractors are attractive targets for cyber attacks because the U.S. federal government entrusts highly sensitive information to these private companies. Stolen credentials are leveraged to gain access to "secure" networks and wreak havoc within organizations — and potentially up the supply chain, as we are witnessing with the fallout from the SolarWinds attack. SpyCloud research found that 79% of passwords at the largest defense industrial base suppliers (private companies with government privileges) are reused across corporate and personal accounts.

Everyone employed by or doing business with the U.S. government must take cybersecurity seriously. Credential management offers the most impactful and practical place to start.

Preventative Measures

Continuously Monitor for Compromised Credentials

While criminals often use previously-breached data to access accounts, organizations can use that same data to protect themselves. The ability to continuously check whether user credentials show up in third-party breaches and underground marketplaces allows government organizations to quickly secure .gov accounts and prevent criminals from monetizing the data.

Keep Eyes on the Supply Chain

Government work relies on partnerships with private businesses, but those outside organizations are also vulnerable to attack, which in turn puts agencies at risk. Visibility into suppliers' risk of credential-based cyber attacks is critical. If exposures from data breaches and malware infections are found, agencies can choose to limit access to their data until the affected supplier has taken corrective action.

Educate Your Workforce

Email is still one of the most common distribution methods for malware, including ransomware. An innocent click on the wrong link or attachment can activate the malicious code that infects systems and deletes data. With humans being the weakest link in every security chain, ongoing training programs may not transform employees into impenetrable human firewalls, but they can encourage better credential stewardship.

Adjust Password Policies to Prevent Password Reuse

Criminals are playing the long game with data from past breaches by weaponizing previously-exposed passwords and common variations. While traditional password policies were rooted in a unique mix of characters and length, that method is no longer sufficient. For today's password policies to be effective, users should be given guardrails for password creation. Maintaining a repository of banned passwords will force users to choose stronger passwords and block them from using one that has previously been exposed.

Follow NIST Guidelines

In response to rampant password reuse, the National Institute for Standards and Technology (NIST) updated its Digital Identity Guidelines to modernize password creation for the new era of cybercrime. Discarding the long-held philosophy that passwords must be long and complex, the new guidelines recommend that user passwords should be "easy to remember" but "hard to guess." In addition to updating its password standards, NIST also issued its Cybersecurity Framework Profile for Ransomware Risk Management, which acknowledges that "ransomware attacks often start with credential compromise" and asserts that "proper credential management is an essential mitigation."

Detect Credential-Stealing Malware

Botnet-infected machines recording employee's keystrokes and screens are something we consistently detect at SpyCloud. Criminals have creative ways to convince unsuspecting users to download and install credential-stealing malware. While antivirus and endpoint protection solutions can help detect infections on corporate systems, some malware strains can slip through the cracks — plus, employees' personal systems may not be protected. Agencies should implement an early warning solution that flags infected employees so incident response teams can mitigate before criminals cause harm.

Compared to the hundreds of high priorities faced by state and local governments, addressing credential security and password reuse doesn't look like much of a priority on paper. But the current situation is not sustainable. The ransomware recovery process alone is expensive and time-consuming, costing government organizations nearly $18.9 billion in 2020. Many under-funded agencies providing critical services or public goods don't often have the luxury of stalling. Considering the severity of recent attacks, it's fair to say that bolstering credential security and preventing password reuse is now a matter of national security.

To truly prevent data breaches, ransomware, and other targeted attacks, government agencies and affiliated organizations must stop criminals before they act: this means detecting and remediating compromised passwords before criminals have a chance to use them to cause harm.

About SpyCloud

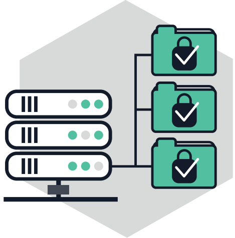
SpyCloud protects consumers, employees, suppliers, and citizens globally from the dangers of compromised identity. Its solutions make breached information actionable to prevent fraud, enabling a proactive, automated response that negates the value of stolen data before it can be used to cause harm. Its data also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include four of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to over 100 cybersecurity experts who aim to make the internet a safer place.

To learn more and see an overview of your agency's exposed data, visit spycloud.com/government.

Employee ATO Prevention

Protect your agency from breaches and ransomware attacks.

Learn More →



Active Directory Guardian

Automatically detect and reset exposed Windows accounts.

Learn More →

Third Party Insight

Monitor suppliers' exposures and share data to aid in remediation.

Learn More →

VIP Guardian

Protect your highest-risk users from targeted account takeover.

Learn More →

Consumer ATO Prevention

Protect your users from account takeover fraud and unauthorized transactions.

Learn More →

SpyCloud

Learn more at spycloud.com/government