SpyCloud

2021 Report: Breach Exposure of London's FTSE 100 (and their Subsidiaries)

Overview

It's human nature: people reuse passwords. Unfortunately, those reused passwords can easily become exposed to cybercriminals and used for malicious intent. According to the 2020 Verizon Data Breach Investigations Report, the use of weak and stolen credentials ranked as the most common hacking tactic for the fourth year in a row.

Password reuse represents a particularly significant security risk for organisations, which house valuable corporate secrets and represent lucrative targets for cybercriminals. Employees frequently reuse corporate credentials as personal logins, regardless of security guidelines that prohibit such behavior. When those third-party sites are subject to data breaches, reused employee logins provide easy entry points to corporate systems and networks.

In addition to corporate credentials, data breaches expose a wealth of personal information that can enable cybercriminals to bypass security measures, take over accounts, and compromise enterprise networks. Employees, trusted partners, and suppliers with privileged access can all be vulnerable to account takeover and business email compromise.

With well over 100 billion breach assets collected to date, SpyCloud maintains the world's largest repository of recovered stolen credentials and personally identifiable information (PII). SpyCloud researchers continually monitor the criminal underground for breach data that has become available to cybercriminals, using human intelligence to gain access to stolen data as soon as possible after a breach occurs.

To provide a snapshot of the breach exposure affecting major enterprises, we examined SpyCloud's entire database to see what breach data we could tie to FTSE 100 companies and their subsidiaries. To do so, we searched for breach records containing corporate email domains, excluding "freemail" domains that are available to consumers. For example, if a FTSE 100 employee signed up for a breached third-party site using their corporate email address, example@employer.com, we were able to tie the resulting breach record to their employer organisation.

Companies with multiple subsidiaries face an expanded attack surface that is easy to lose track of, so we felt it was important to include them in our analysis for a full picture of the FTSE 100's breach exposure.

We were able to identify over **39 million breach assets** within our dataset tied to employees in the FTSE 100 and their subsidiaries. The threat facing security teams at these companies is significant.

Bear in mind, this analysis excludes breach data tied to employees' personal aliases, which can also be tied to corporate identities and used for illicit gain. It will include some employees who have moved on to other companies. However, we hope that this analysis provides a window into the scale of the account takeover risks facing large organisations and the importance of monitoring employee credentials for weak and reused passwords.

About SpyCloud Data

Truly Actionable Breach Data to Prevent Account Takeover

SpyCloud uses Human Intelligence (HUMINT) to quickly recover breach data, often within days of the breach occurring. Our unique data cleansing and password cracking process reveals compromised credentials faster and with greater match rates. Access to this massive breach database enables organisations to quickly identify and take action on exposed accounts, preventing those exposures from progressing to account takeovers. SpyCloud safeguards more than 2 billion employee and consumer accounts from account takeover and follow-on attacks like credit card fraud, phishing, and ransomware. **Learn more at spycloud.com.**

100+ B
Recovered Breach Assets

23+ B
Recovered Passwords

27+ B
Email Addresses

200+
PII Types

Key Findings

1. The volume of breach data tied to FTSE 100 employees is staggering.

Of the more than 39 million breach assets we found, nearly 2.6 million were corporate email address + plaintext password pairs (that's 26,000 per company, on average). If employees have reused these passwords, criminals can easily exploit the exposed credential pairs to gain access to corporate systems.

2. Employees of the FTSE 100 and their subsidiaries are reusing passwords at a higher rate than the average person.

Among the FTSE 100 employees who appear in more than one breach, we found a password reuse rate of 76%, including exact matches and slight variations that criminals can easily match. The worst offenders? Companies in the Energy and Real Estate industries, both at 80%. By comparison, across the whole SpyCloud breach database, the password reuse rate is 57%.

3. The credentials of 15,692 C-level FTSE 100 executives are available on the criminal underground—and 25% are from the Consumer Discretionary industry.

Executives make compelling targets for targeted cyber attacks, including business email compromise (BEC), also known as CEO fraud, which is a leading cause of financial losses due to cybercrime. Companies in the Consumer Discretionary sector collectively have 3,939 exposed C-level credentials (an average of 188 per company).

4. Credentials are only part of the story.

Beyond exposed passwords and potentially compromised users, bad actors have access to a wealth of compromised PII that can be used in targeted attacks – almost 19 million PII assets tied to FTSE 100 employees are available to cybercriminals. The industry with the highest amount of exposed PII? Financials, with 23% or 4.4 million exposed PII assets.

At a Glance: Breach Exposure of the FTSE 100

9,582

TOTAL BREACH SOURCES

Total number of breaches in the SpyCloud dataset that include records tied to FTSE 100 corporate email addresses.

8,313,590

TOTAL CORPORATE BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. Ex: Information tied to jsmith@acme.com within a set of data stolen in a breach of example.com.

39,690,559

TOTAL BREACH ASSETS

A breach asset is a piece of information contained within a breach record. Ex: a password, an address, a phone number.

2,589,187

TOTAL PLAINTEXT CORPORATE CREDENTIALS

Total number of FTSE 100 corporate email addresses and plaintext password pairs that have appeared in a data breach and are available to criminals. If employees have reused these passwords, criminals can easily exploit the exposed credential pairs to gain access to corporate systems.

15,692

TOTAL C-LEVEL EXECUTIVES EXPOSED

Exposed corporate credentials that are tied to FTSE 100 executives with high-ranking titles, putting them at increased risk of targeted account takeover attempts and business email compromise (BEC) fraud.

76%

PASSWORD REUSE INDEX

Among the FTSE 100 employees who appear in more than one breach, this is the rate of password reuse we have observed. This includes exact passwords and slight variations that criminals can easily match.

3,347

POTENTIALLY INFECTED EMPLOYEES

SpyCloud recovers some data collected by botnets. Credentials appearing in this data indicate that affected employees have malware with a keylogging component installed on their personal or corporate systems.

Corporate Credential Exposure of the FTSE 100

Exposed Corporate Credentials

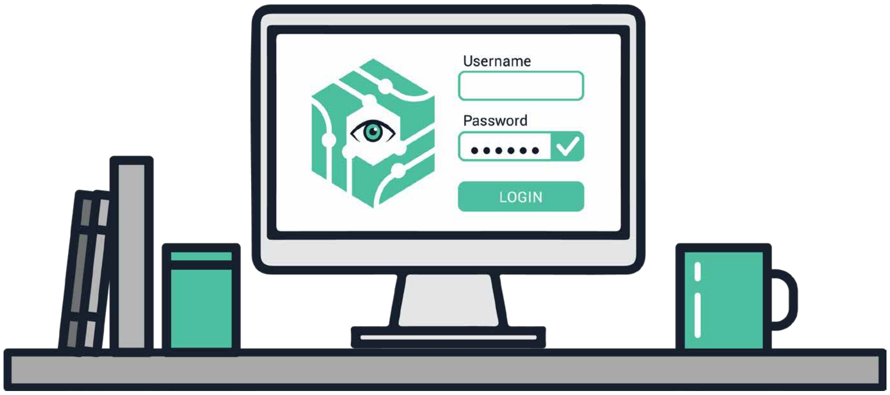
Across the SpyCloud dataset, we discovered 2,589,187 pairs of credentials with FTSE 100 or subsidiary corporate email addresses and plaintext passwords. While not every credential pair will match active corporate login details, the ones that do match represent substantial risk for these enterprises—and their customers and partners.

When credentials are exposed in a data breach, cybercriminals inevitably test them against a variety of other online sites, taking over any other accounts protected by the same login information. If those stolen credentials contain a corporate email domain, criminals have an obvious clue that they could provide access to valuable enterprise systems, customer data, and intellectual property.

In theory, corporate passwords should be strong given the importance of the assets they protect and the robust guidance often provided by corporate security teams. In practice, many employees practice bad password hygiene at work, and some corporate password policies even encourage bad habits. Outdated policies like strict complexity rules and mandatory quarterly password rotations make passwords harder to remember, leading employees to make insecure choices like recycling versions of their favorite passwords. That's why the password guidance from the National Cyber Security Centre (NCSC) recommends expiring passwords only when necessary, and implementing a password blacklist, which steers users away from common and compromised passwords.

In the SpyCloud database, we found:

Industry	Total Exposed Corporate Credentials
Basic Materials	62,317
Consumer Discretionary	279,820
Consumer Staples	310,009
Energy	362,113
Financials	684,624
Health Care	216,099
Industrials	253,098
Real Estate	1,273
Technology	26,802
Telecommunications	383,809
Utilities	9,223
Total	**2,589,187**



Password Reuse:

Password reuse is rampant. An analysis of the SpyCloud database found a 57% password reuse rate among email addresses in our database exposed in more than one breach. That rate is even worse for employees of the FTSE 100 and their subsidiaries; though you can imagine the stakes (and security measures) are especially high, we found an average password reuse rate of 76%.

Within our dataset of FTSE 100 corporate breach exposures, we examined how many employees with more than one exposed login have reused the same password or a close variation across multiple sites, then assigned a Password Reuse Index to each industry. The higher the percentage, the greater the rate of employee password reuse.

Employees with multiple reused passwords in our dataset may or may not reuse passwords at work—we can't tell for sure without checking their actual work passwords. However, password reuse across personal accounts does provide an indication of employees' overall password hygiene.

TOP 50 REUSED PASSWORDS

george password 123456
welcome 12345 liverpool Password
linkedin password1 sunshine
charlie aaron431 *0295F867E58AA24
[company name]1 12345678 Password1
chelsea [company name] 123456789
welcome1 [company name].com matthew
qwerty arsenal monkey everton
scotland daniel mac273 111111
tigger tigers rangers Thomas
holiday hannah bluefish william
oliver andrew jessica charlotte
discounts 3sYqo15hiL summer
jasper 0295F867E58AA24 letmein
sophie joshua

In the SpyCloud database, we found:

Rank	Industry	Password Reuse Index
1	Energy	80%
2	Real Estate	80%
3	Consumer Staples	77%
4	Telecommunications	76%
5	Health Care	75%
6	Consumer Discretionary	74%
7	Financials	72%
8	Industrials	72%
9	Basic Materials	69%
10	Technology	65%
11	Utilities	39%

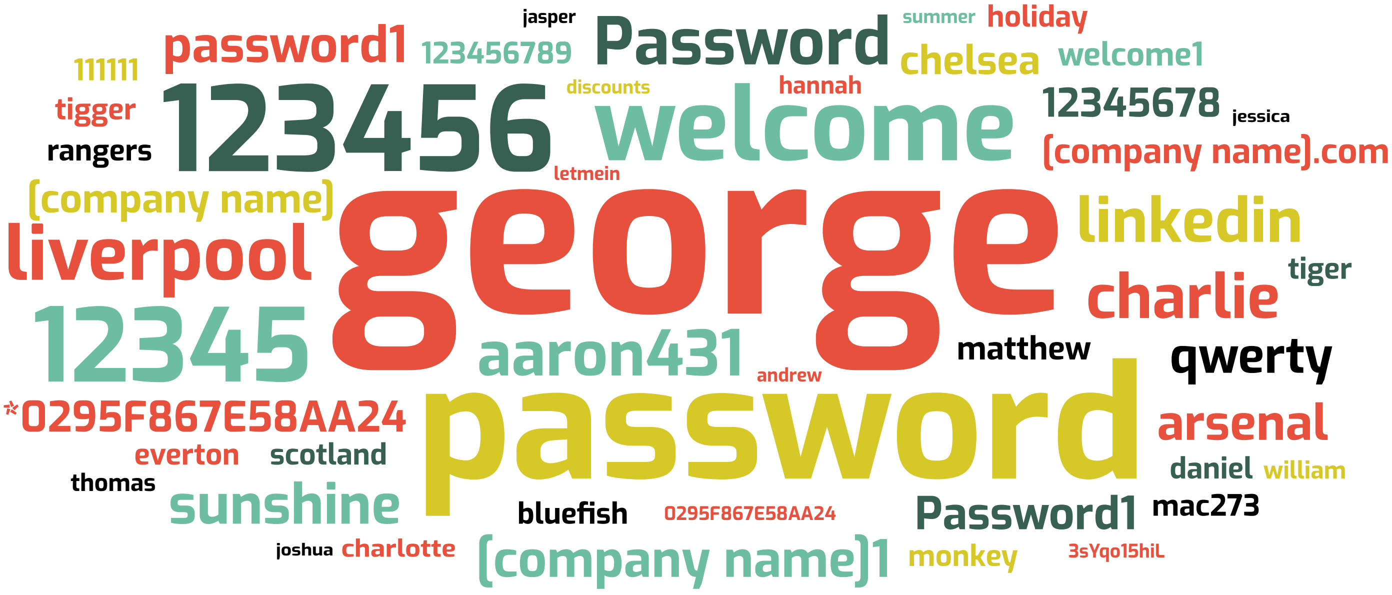
Favorite Passwords of FTSE 100 Employees

With hundreds of accounts to keep track of, it's no wonder people take shortcuts to remember their login credentials. In addition to recycling variations of a few favorites across every account, people often use simple passwords that are easy to remember—and easy for criminals to guess. Criminals often use lists of common passwords in password spraying attacks, putting accounts with weak passwords at risk even if the user hasn't intentionally reused that password.

FTSE 100 employees follow the same patterns as the rest of us. Each of the passwords below appeared hundreds or even thousands of times within our dataset. (We've redacted company names, which appeared very frequently.)

While most of these examples would fail to pass basic corporate password policies, people tend to transform a base password in predictable ways to bypass complexity rules. For example, 'password' might become 'Password1' or 'Passw0rd!' at work. Unfortunately, criminals are well-aware of these patterns, and sophisticated account checker tools make it easy for criminals to test variations of exposed passwords at scale.

Popular Passwords of FTSE 100 Employees



THE PASSWORD
george
APPEARED 10,576 TIMES

THE PASSWORD
password
APPEARED 8,746 TIMES

THE PASSWORD
123456
APPEARED 8,478 TIMES

Credentials Collected by Malware

The Danger of Infected Employees

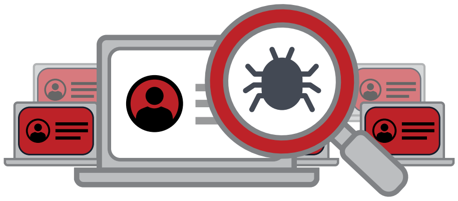
Not all of the exposed data in this report comes from data breaches. SpyCloud also recovers some information collected by botnets. Malware with keylogging components, or “stealers,” can siphon information such as browser history, autocomplete data, cookies, screenshots, system information, crypto wallets, and login credentials from an unsuspecting user’s infected system.

Like breach data, information stolen by botnets is collected by cybercriminals, shared in small circles, and sometimes posted on hacking web forums. When SpyCloud is able to recover some of these bot logs, we parse out the infected victim’s username, URL, and password in order to help consumers and organisations protect themselves. For this report, we searched these records for FTSE 100 corporate email addresses to identify employees who may be using infected personal or corporate systems.

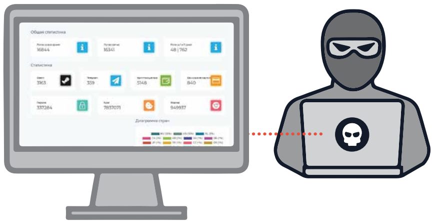
In total, SpyCloud has identified 3,347 potentially infected employees within the FTSE 100 and subsidiaries, an average of 33 per company.

That may not sound like a lot per company, but the breadth of data captured by these infections can have disastrous consequences for organisations, whether the affected device is personal or corporate. Malware with keylogging components can record the employee’s every move, capturing browser history, files, system information, and login data for corporate and third-party resources. Bad actors can use this information to bypass multi-factor authentication, log into corporate networks, steal sensitive data, authorize fraudulent transactions, and more. Even without exact corporate logins, criminals can easily blackmail, extort, trick, or impersonate the victim to extend their access to corporate resources.

1. Threat actor distributes malware to users. This might take the form of a phishing email or advertisement that entices the user to download a malicious file.



2. Users' infected systems send data to the threat actor's C&C.



3. Threat actor sees results in an admin panel, which can include stolen credentials, crypto wallets, system information, browser data, and files.

4. Threat actor monetizes stolen data by draining accounts and selling stolen information to other criminals.

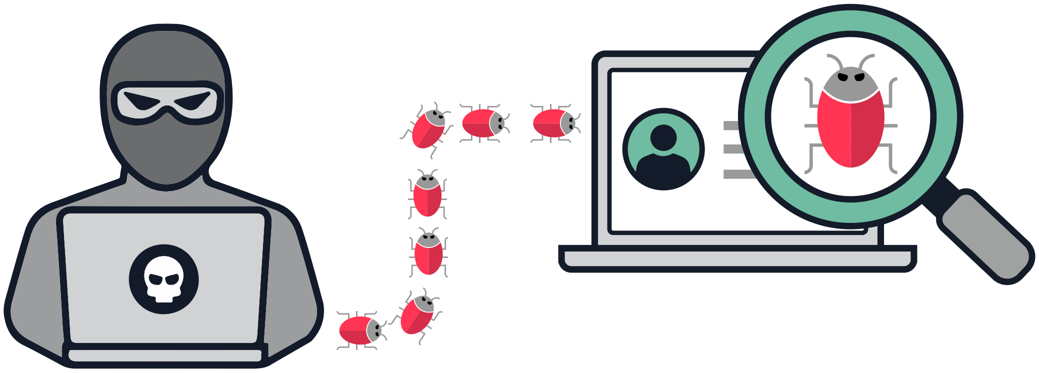
What About Infected Consumers?

In addition to infected employees, we also identified over 143,000 potentially-infected consumers of FTSE 100 services. These are users of FTSE 100 (and subsidiaries') consumer-facing sites where botnet logs show that they were infected while entering their username and password on the login page (e.g. jim@hotmail.com was infected while logging into signin.ftse100company.com).

Because of the scope of this report, the true number of infected consumers for these sectors is likely higher; for example, we excluded many consumer-only domains from this analysis. We've also nixed credentials with usernames instead of email addresses because it's unclear whether they are employee or consumer records. However, each one of these infected consumers is at extremely high risk of account takeover, identity theft, and online fraud, which can result in substantial losses and brand damage for affected organisations.

Here are just a few ways cybercriminals exploit consumers' stolen information:

- **Steal a victim's identity to commit fraud, such as opening loans in their name**
- **Transfer funds from crypto wallets, investment portfolios, payment applications, and other accounts**
- **Place fraudulent orders using credit card information or gift cards stored within accounts**
- **Siphon loyalty points associated with accounts**
- **Commit warranty fraud using stored device information**
- **Change shipping addresses to facilitate package theft and drop-shipping**
- **Stalk or blackmail victims using browser history and other stolen data**
- **Sell login details and browser fingerprints to other criminals**



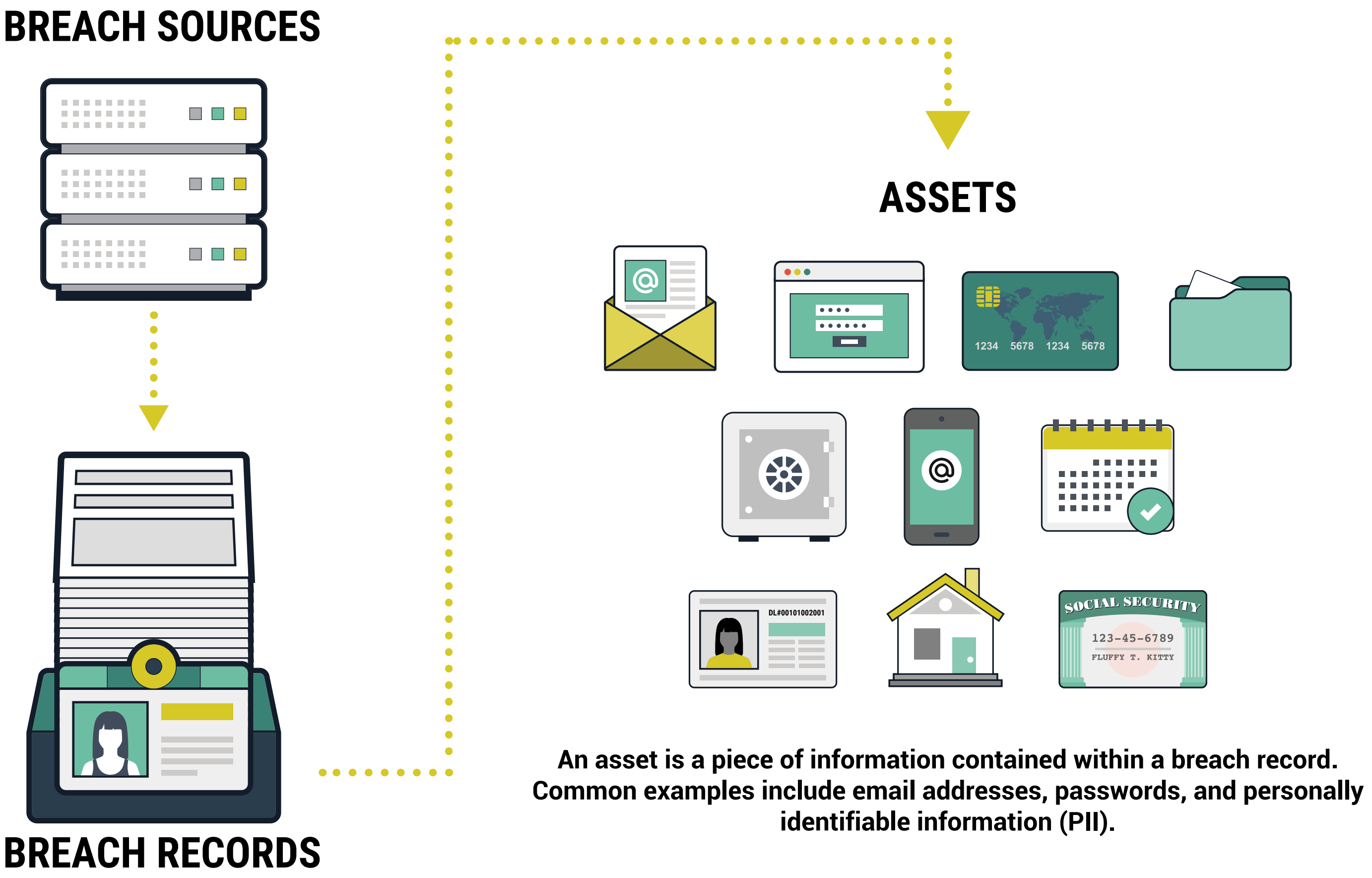
Beyond Credentials: Other Breach Exposures by Asset Type

A breach asset is a piece of information connected to a single breach record. In addition to login credentials, breach assets can include phone numbers, addresses, social security numbers, credit ratings, and much more—any type of information that can be obtained in a data breach. While stolen credentials provide an obvious entry point for malicious actors, other types of breach assets can also provide tremendous value to cybercriminals, whether for consumer fraud or as a means of gaining access to enterprise networks, data, intellectual property, and funds.

Criminals may engage in highly-targeted, manual attacks against victims with privileged access to corporate resources, such as C-suite leaders, senior executives, system administrators, and developers. Given the potential payoff associated with these targets, it's no wonder criminals are willing to invest substantial effort and creativity to take over their accounts.

In total, SpyCloud has collected 39,690,559 breach assets tied to FTSE 100 employees.

Within the SpyCloud dataset, we have segmented certain types of breach assets into categories to help quantify different types of breach exposure. Let's break down how a few of these asset types can be used by cybercriminals and look at FTSE 100 employee exposure for each asset type.



An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Asset Type: Personally Identifiable Information (PII)

What It Is

Personally identifiable information (PII) is data that could be used to identify an individual person. For the purposes of this report, SpyCloud has excluded some forms of PII that have been broken out into separate categories below, such as phone and financial assets. However, this category includes many other types of personal data such as addresses, NINOs, and credit ratings.

How It Helps Criminals

Personally identifiable information can provide criminals with many lucrative paths for committing fraud or stealing corporate data, particularly when they have access to full packages of victims' information, or "fullz." Using stolen PII, criminals can:

- **Steal a victim's identity to commit fraud, such as opening loans in their name**
- **Create new accounts to use as synthetic identities**
- **Craft detailed, credible spear phishing messages**
- **Submit fraudulent applications**

TOTAL PII ASSETS	AVERAGE PER COMPANY
18,960,895	189,609

TOTAL PHONE ASSETS	AVERAGE PER COMPANY
540,961	5,410

Asset Type: Phone Assets

What It Is

Phone assets are stolen phone numbers.

How It Helps Criminals

In combination with stolen credentials, criminals can use phone assets to bypass multi-factor authentication using tactics such as [SIM swapping and phone porting.](#) With a simple phone call to a mobile carrier and some light social engineering, criminals can divert a victim's phone service to their own device. Once the attacker has control of the victim's phone number, they receive all SMS-based authentication messages and can easily log into sensitive accounts (even corporate accounts) undetected.

07623 is your PIN code
ACCESS GRANTED
07623

Asset Type: Financial

What It Is

Financial assets include credit card numbers, bank account numbers, and tax IDs. While this information all technically qualifies as PII, we have separated it into its own category due to the severity of the exposure.

How It Helps Criminals

Criminals can use stolen credit card numbers and other financial information to:

- **Make fraudulent purchases**
- **Drain funds from accounts**
- **Resell card numbers to other criminals**
- **Collect victims' tax refunds**

TOTAL FINANCIAL ASSETS
63,147

AVERAGE PER COMPANY
631

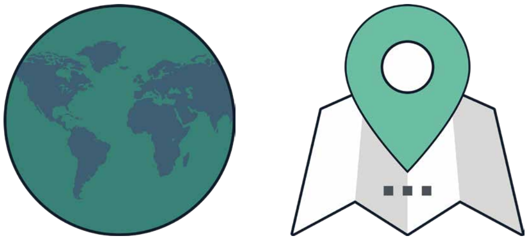
TOTAL GEO ASSETS
521,242

AVERAGE PER COMPANY
5,212

Asset Type: Geolocation

What It Is

Geolocation assets consist of latitude and longitude pairings that pinpoint users' physical locations. This is typically the location of the IP that a user last logged in from. That location sometimes correlates with their address, but not always, which is why this data has been separated from PII assets.



How It Helps Criminals

Criminals can use geolocation data (or addresses) to craft targeted attacks against high-value victims such as employees with privileged access to corporate data.

Examples include:

- **Using a VPN to mimic traffic from a user's location, avoiding controls that flag logins from unexpected locations**
- **Crafting spear phishing emails that reference the user's location, such as an event invitation that contains a malicious link**
- **Guessing the answers to knowledge-based security questions**

Asset Type: Social

What It Is

Social assets include social media handles that may have been tied to the breached account.

How It Helps Criminals

Social assets can help criminals connect the dots between personal and corporate identities, which can be particularly useful in targeted attacks. An attacker may move laterally from one account to another, first compromising a social media account with limited protections in place and then using that access to compromise higher-value accounts or accounts belonging to the victim's trusted associates. Data shared on social media may also provide the attacker with insights that can aid in answering security questions or crafting believable spear phishing attacks.

TOTAL SOCIAL ASSETS	AVERAGE PER COMPANY
2,266,178	22,662

TOTAL ACCOUNT ASSETS	AVERAGE PER COMPANY
1,792,521	17,925

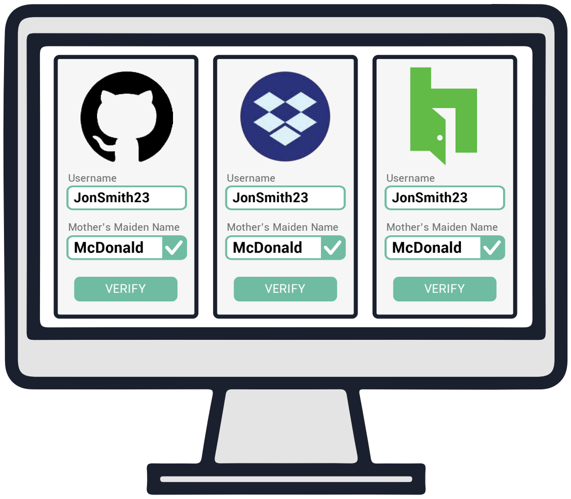
Asset Type: Account

What It Is

Account assets are data related to the breached account itself—including secret answers to the security questions that many sites use as an extra layer of authentication. Account assets also encompass user activity records, such as the date an account was created and most recent login date.

How It Helps Criminals

Access to users' secret answers makes it easy for attackers to bypass authentication measures and take over accounts. In addition, criminals may use account activity records to engender trust and convince users to share additional information, such as their password. For example, an attacker might list recent actions a user has taken on specific dates and ask them to "verify" their validity by taking a risky action like clicking a phishing link.



Username
JonSmith23
Mother's Maiden Name
McDonald ✓

Username
JonSmith23
Mother's Maiden Name
McDonald ✓

Username
JonSmith23
Mother's Maiden Name
McDonald ✓

100 COMPANIES
AND THEIR SUBSIDIARIES

SPANNING THESE ICB INDUSTRIES

Basic Materials
Consumer Discretionary
Consumer Staples
Energy
Financials
Health Care
Industrials
Real Estate
Technology
Telecommunications
Utilities

9,582 TOTAL BREACH SOURCES

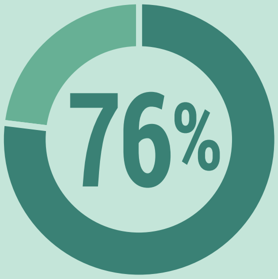
The number of breaches within the SpyCloud database that include records tied to FTSE 100 corporate email addresses.

8,313,590 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.
Average number of breach records per parent company: 83,196

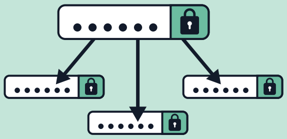
39,690,559 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).
Average number of assets per parent company: 396,905



PASSWORD REUSE INDEX

A metric that measures how many of these companies' employees have more than one credential exposure and have reused a password or a close variation across several sites.



TOP 10 PASSWORDS
Used by FTSE 100 Employees

1. george	6. liverpool
2. password	7. Password
3. 123456	8. linkedin
4. welcome	9. password1
5. 12345	10. sunshine

18,960,895

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, NINOs, credit ratings, and more.
Average PII Assets per parent company: 189,609

2,589,187 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

25,892 Average Number of Exposed Passwords per Parent Company

15,692 Potentially Exposed C-Level Executives

3,347 Potentially Infected Employees

Employees who have used a machine infected with malware to log into a domain or portal with a corporate email address and provided a password to that destination.

Your Plan of Action

SpyCloud's analysis of FTSE 100 companies' exposure as a result of third-party breaches has revealed more than 39 million breach assets in criminals' hands, nearly 2.6 million of which are plaintext passwords tied to FTSE 100 & subsidiary employees. Combined with high rates of password reuse, these exposures represent significant account takeover risks for these organisations and the companies that do business with them.

Attackers actively test stolen credentials against different accounts to exploit bad password habits and gain access to corporate systems and data. Even worse, stolen PII and account data make it easy for criminals to craft highly targeted, creative attacks that cause great harm and are difficult to detect.

Enterprises must be able to trust the identities of the employees, consumers, and suppliers logging into their networks—and safeguard the corporate assets and IP behind those logins. The answer is to build early detection and remediation of exposed credentials into their cybersecurity strategy, and the best method, simply put, is to use SpyCloud.

The SpyCloud Difference

Building a security program around technologies that proactively leverage data acquired through Human Intelligence (HUMINT) tradecraft very early in the breach timeline is a critical path to success. SpyCloud's solutions, backed by the world's largest repository of recovered stolen credentials and PII, enables enterprises to stay ahead of account takeover by detecting and automatically resetting compromised passwords early, before criminals have a chance to use them.

Our customers continue to tell us their ability to prevent account takeover hinges both on access to relevant data (including the most plaintext passwords in the industry) and in being able to make that data operationally actionable through automation.

Employee ATO Prevention

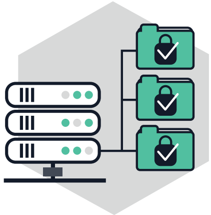
Protect your organisation from breaches and BEC due to password reuse.

Learn More ⟶

VIP Guardian

Protect your highest-risk executives from targeted account takeover.

Learn More ⟶



Active Directory Guardian

Automatically detect and reset exposed Windows accounts.

Learn More ⟶

Third Party Insight

Monitor third party exposures and share data to aid in remediation.

Learn More ⟶

Consumer ATO Prevention

Protect your users from account takeover fraud and unauthorized purchases.

Learn More ⟶

See Your Account Takeover Risk →

Discover how many breach records we have associated with your email address and your domain as a whole. Once you know, you can take action.

SpyCloud

Learn more at spycloud.com