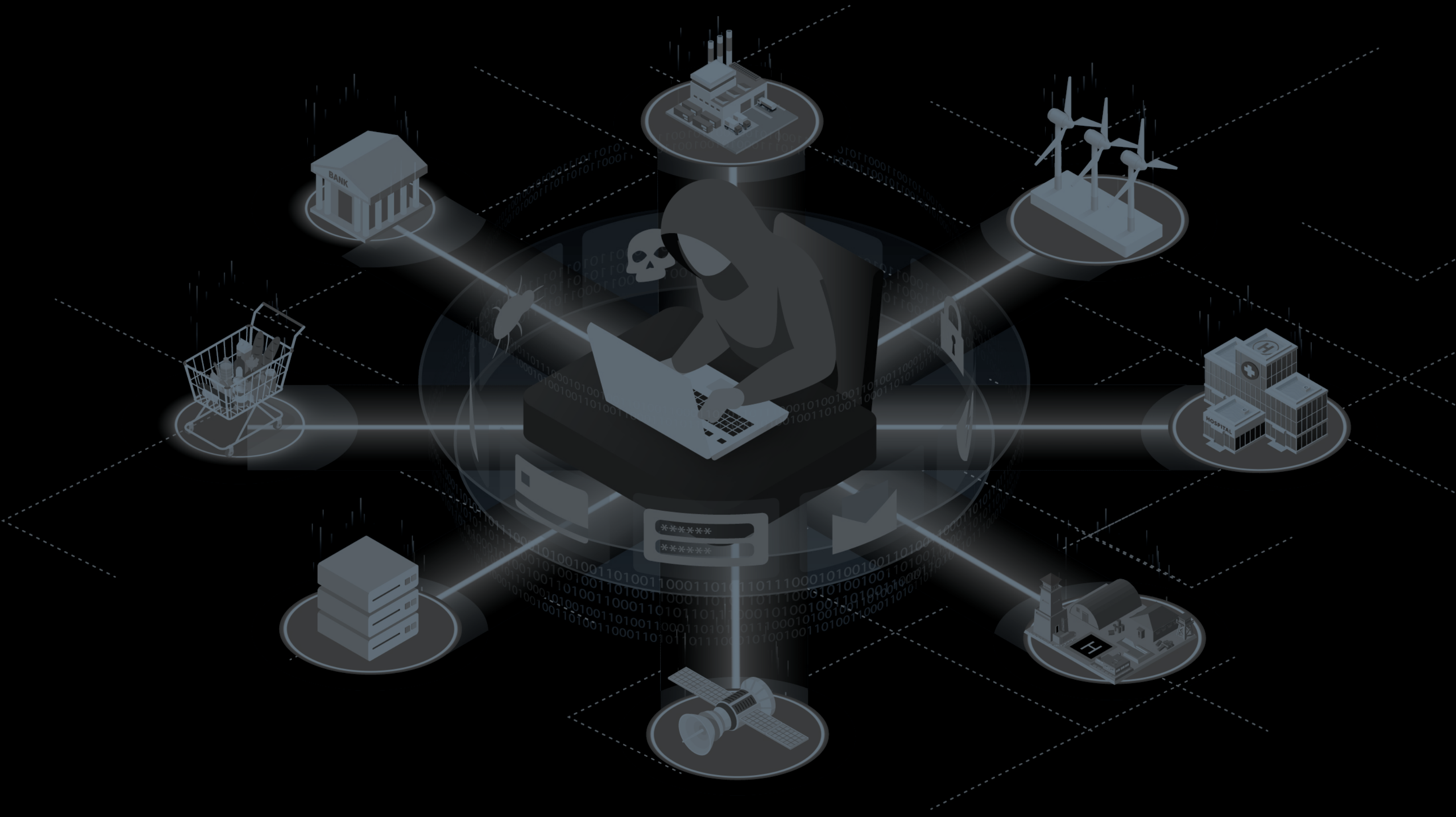
2022 Report:

# Identity Exposure of London's FTSE 100 (and Their Subsidiaries)



SpyCloud

SpyCloud

## Table of Contents

## Overview

The rapid move toward the digital age continued in 2021, as more organisations embraced hybrid work models. With employees juggling even more logins for web and cloud apps, many looked for productivity shortcuts such as reusing their passwords. Password reuse is not a new problem. But the explosion of digital tools played well into cybercriminals' hands because employees' poor habits didn't change – and every new employee device and digital account only gave malicious actors more opportunities to compromise enterprises.

As data breaches continue to leak credentials at a massive scale, password reuse creates significant security risks for organisations. A single set of employee credentials that have been exposed in a third-party breach leaves the door wide open for malicious actors to gain entry into the corporate network. And in many cases, attackers have much more information at their disposal to increase their success rate, including highly sensitive personally identifiable information (PII) siphoned from malware-infected devices that can be used to circumvent MFA.

With well over 200 billion assets recaptured to date from the criminal underground, SpyCloud maintains the industry's largest repository of recovered stolen credentials and PII, collected as quickly as possible after exposure using human intelligence. To provide a snapshot of the identity exposure affecting major enterprises, we examined SpyCloud's entire database to see what data we could tie to London's FTSE 100 companies and their subsidiaries.

To perform our analysis, we searched for records containing FTSE 100 and subsidiary 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, such as jonsmith@example.com, we were able to associate the resulting breach record to their employer.

For our analysis, we looked at more than **51 million** breach assets in our database tied directly to FTSE 100 and subsidiary employee emails. In this report, we take a look at the top patterns across all 11 industry clusters and provide a detailed analysis of the findings.

## About SpyCloud Data

SpyCloud's proprietary engine collects, curates, enriches, and analyzes recaptured data from breaches, malware-infected devices, and other sources from the criminal underground – transforming it into actionable insights that enable enterprises to quickly identify legitimate users vs. potential criminals using stolen information, and take action to prevent account takeover, ransomware, and online fraud.

Learn more at spycloud.com.

**200+**
**Billion**
Recaptured Assets

**25+**
**Billion**
Total Passwords

**30+**
**Billion**
Email Addresses

**50+**
Breach Sources Collected Per Week

## Key Findings

### 1. Password reuse is prevalent among employees of FTSE 100 companies and subsidiaries.

SpyCloud researchers found a **64% password reuse rate** among FTSE 100 and subsidiary email addresses in our database that have been exposed in more than one breach. The worst offenders are consumer discretionary companies (65% reuse rate) and industrials (64%). This average is 4 points higher than the 60% password reuse rate we see across our entire database, but it's even more concerning because high password reuse is a trend we see with FTSE 100 employees year after year. It means that even their old exposures matter; criminals will use them against the employees and their enterprises for years as long as the habit remains unchanged. It's also a growing concern among CISOs in light of intensifying ransomware attacks that are stemming from exposed, reused credentials. Despite education from corporate security teams, vendors, and the media, employees continue to disregard best practices – there's clearly a disconnect between awareness and action.

### 2. Exposure among FTSE 100 and subsidiaries is growing in the double digits.

Breach records associated with FTSE 100 employees grew 21% year-over-year to **10 million**. A breach record is a set of data tied to a single user within a given breach, and includes individual breach assets (pieces of data within a record) such as a password and phone number. The quantity of breach assets tied directly to FTSE 100 employees grew 29% year-over-year to **51 million**. Financials, consumer discretionary, and industrials are the top three sectors with the highest numbers of both breach records and exposed assets. The assets include **2.75 million** corporate email address and plaintext password pairs associated with FTSE 100 and subsidiary employees. These staggering numbers show that cybercriminals' job is only getting easier — they don't need sophisticated techniques when they have access to an abundance of logins.

### 3. PII exposure grew by 45% since 2020, providing more fodder for phishing, fraud, and other malicious attacks.

We found nearly **27.6 million PII assets** tied to FTSE 100 companies and subsidiaries, representing a **45% increase** from last year's analysis. This is a big concern because cybercriminals use PII in social engineering and phishing schemes to gain access into a company and steal sensitive data. For example, details gleaned from PII enable them to create credible spear phishing messages or answer account security questions and bypass or reset MFA. When we look at the average exposed PII per company, energy, telecommunications, and healthcare rise to the top.

### 4. The financials industry has the worst – and most severe – overall exposure.

Financials fared the worst of all 11 industries in breach, credential, and PII exposure, ranking at the top based on their high numbers in each of those areas. The nearly **2.2 million** exposed breach records among financials represent **22% of the total** across all FTSE 100. Of the 2.75 million total FTSE 100 exposed pairs of email addresses and passwords, 714,405 (26%) come from financials. Additionally, the number of exposed PII assets in this industry – nearly 6.13 million – comprises nearly 22% of the total FTSE 100 PII exposure. The financials industry also has the highest number of geolocation assets (149,779 or nearly 29% of the total across all sectors), social assets (882,359 or 24% of the total), and account assets (517,857 or 20% of the total). It's especially concerning to see such extensive exposure among employees of an industry that's entrusted with guarding large amounts of consumers' PII and financial data.

## At-a-Glance: Identity Exposure of the FTSE 100

**10,246**

### TOTAL BREACH SOURCES

Total number of breaches in the SpyCloud database that include records tied to FTSE 100 employees and their subsidiaries.

**10,048,474**

### 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.

**51,038,410**

### TOTAL BREACH ASSETS

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

**2,756,512**

### TOTAL PLAINTEXT CORPORATE CREDENTIALS

Total number of FTSE 100 and their subsidiaries' employee email address and plaintext password pairs that are available to criminals. If employees have reused these passwords, criminals can easily exploit the exposed credential pairs to gain access to corporate systems.

**15,896**

### TOTAL C-LEVEL EXECUTIVES EXPOSED

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

**64%**

### PASSWORD REUSE

Among the FTSE 100 and their subsidiaries' 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.

**9,522**

### MALWARE-INFECTED EMPLOYEES

FTSE 100 employees whose data appears in recaptured botnet logs from infostealer malware. This high-severity exposure puts them at high risk of ATO and fraud, and makes the enterprise vulnerable to ransomware attacks.

## Corporate Credential Exposure of the FTSE 100

### Exposed Corporate Credentials

Across the SpyCloud dataset, we discovered more than **2.75 million pairs of credentials** with FTSE 100 or subsidiary corporate email addresses and plaintext passwords. With 714,405 of those associated with financials, this industry has the highest number of exposed credentials by far. Rounding out the top three are telecommunications and energy.

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 use 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 password guidance from the National Cyber Security Centre (NCSC) recommends expiring passwords only when necessary and implementing a password blocklist, which steers users away from common and compromised passwords.

**In the SpyCloud database, we found:**

| Industry | Total Exposed Corporate Credentials |
|---|---|
| Basic Materials | 59,695 |
| Consumer Discretionary | 313,835 |
| Consumer Staples | 323,983 |
| Energy | 375,492 |
| Financials | 714,405 |
| Health Care | 224,147 |
| Industrials | 297,595 |
| Real Estate | 1,370 |
| Technology | 32,181 |
| Telecommunications | 404,893 |
| Utilities | 8,916 |
| **Total** | **2,756,512** |

## Password Reuse

**Within our dataset of FTSE 100 and subsidiary corporate breach exposures, we found a 64% average password reuse rate.** We calculated the average password reuse rate by taking the number of employees using the same exposed plaintext password across multiple sites, then divided by the number of all employees with exposed passwords.

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 their third-party breach-exposed accounts does provide an indication of employees' overall password hygiene.

### TOP 100

**REUSED PASSWORDS OF 2021**

george password 123456 welcome liverpool
12345 Password password1 charlie sunshine
*0295F867E58AA24 12345678 aaron431 GSK1
chelsea welcome1 123456789 arsenal matthew
[redacted].com qwerty mac273 monkey tigers
scotland everton Daniel rangers 111111
tigger hannah Thomas holiday william
oliver andrew charlotte summer jessica
letmein sophie jasper broomfield discounts
liverpool1 rebecca 3sYqo15hiL 0295F867E58AA24
welcome1 joshua football michael princess
discount celtic abc123 chocolate
louise charlie1 alexander equityDev
changeme [redacted].com newyork victoria
sterling Passw0rd benjamin richard
postman orange michelle jordan
72e138475b4eb2ec London 1234 buster
caroline olivia samuel 456a33 vining1
elephant robert jennifer arsenal1 ginger
australia cameron wealth shopping

**In the SpyCloud database, we found:**

| Rank | Industry | Average Password Reuse |
|---|---|---|
| 1 | Consumer Discretionary | 65% |
| 2 | Industrials | 64% |
| 3 | Consumer Staples | 63% |
| 4 | Technology<br>Utilities | 62% |
| 5 | Energy<br>Financials<br>Health Care | 60% |
| 6 | Telecommunications | 59% |
| 7 | Basic Materials | 51% |
| 8 | Real Estate | 46% |

## Favorite Passwords of FTSE 100 Employees

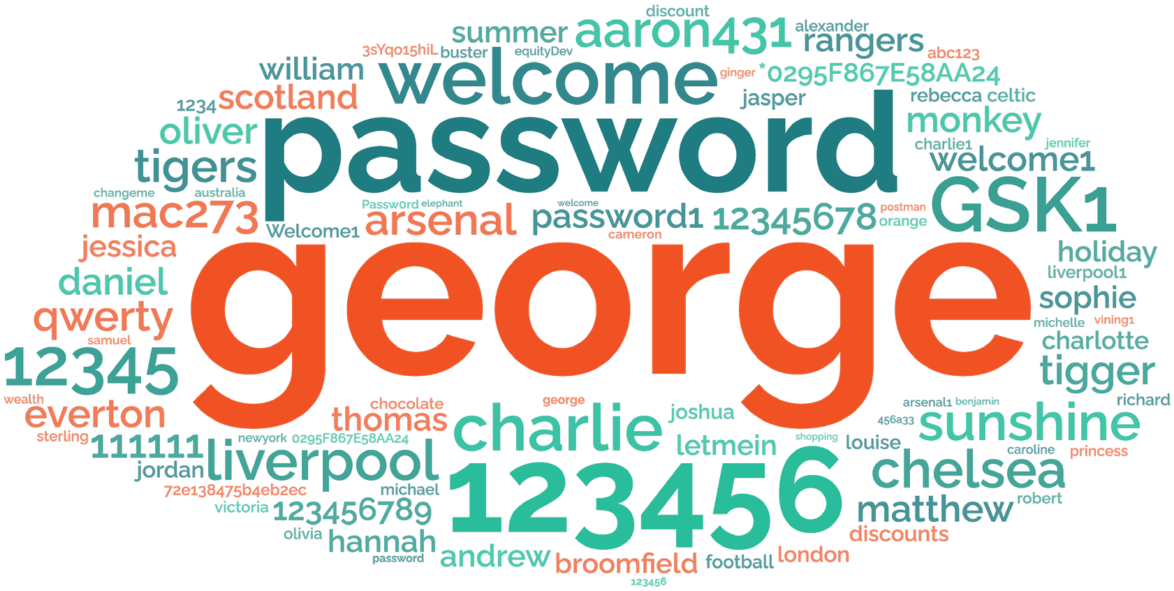
With hundreds of accounts to keep track of, it's no wonder people take shortcuts to remember their login credentials. In addition to recycling variations of a few favorites across every account, people often use simple passwords that are easy to remember – and easy for criminals to guess. Criminals often 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.

One of the worst shortcuts employees can take is to include their company's name in their passwords; it's one of the first things criminals will enter into their account checker tools when they're trying to crack corporate passwords. However, banning the use of the company name in passwords may not be enough. Organisations need to find ways of protecting employees from themselves.

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 appear 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 automated tools make it easy for them to test variations of exposed passwords at scale.



**george**

**appears in 12,570 passwords**

**password**

**appears in 9,879 passwords**

**123456**

**appears in 8,938 passwords**

# Data Siphoned by Malware

## The Danger of Infected Employees

Not all of the exposed data in this report comes from data breaches. SpyCloud also recaptures information collected by botnets. Malware with keylogging components, or "infostealers," can siphon information such as browser history, autocomplete data, web session cookies, screenshots, system information, crypto wallets, and login credentials from an unsuspecting user's infected device.

Like breach data, information stolen through malware infections is collected by cybercriminals, shared in small circles, and sold on criminal marketplaces.

When SpyCloud recaptures these bot logs, we parse out the infected victim's username, password, URL, and cookies in order to help organisations protect themselves and their users. For this report, we searched these records for FTSE 100 and subsidiary corporate email addresses to identify employees who may be using infected personal or corporate devices.

**In total, we've identified 9,522 malware-infected employees within the FTSE 100 and their subsidiaries.** Consumer staples, telecommunications, and consumer discretionary are the industries with the highest infection numbers.

The breadth of data captured by these infections can have disastrous consequences for enterprises, whether the affected device is personal or corporate. Malware siphons everything from browser history to login data for work and third-party resources. Bad actors can use this information to bypass MFA, log into corporate networks, steal sensitive data, authorize fraudulent transactions, and more. Even without exact corporate logins, criminals can easily extort, trick, or impersonate the victim to extend their access to corporate resources.

Stolen credentials are often the first attack vector for cybercriminals, and ransomware poses a major risk from infected employee devices. A recent SpyCloud report found that **IT security professionals ranked compromised credentials as the second riskiest entry point in ransomware attacks** (not far behind phishing). The risk is especially high when employees' devices are infected with malware that steals authentication data, given that a specialized criminal group known as initial access brokers sell those freshly harvested employee credentials to ransomware operators. This perhaps explains why 79% of our surveyed security leaders and practitioners said that last year's high-profile ransomware attacks elevated their concern about compromised and weak credentials used by their employees and customers.

Keep in mind that one infected device can expose hundreds of credential pairs given the prolific number of applications and work accounts each employee has. And even after the device is cleaned up, those exposed credentials continue to put the organisation at risk.

## Risk From Infected Consumers Just As High

In addition to infected employees, we've also identified **393,546 infected consumers** of FTSE 100 services, with 54% of them in the consumer discretionary industry.

These are users of FTSE 100 and subsidiary consumer-facing sites where botnet logs show that they were infected while entering their username and password on the login page (e.g., jim@example.com was infected while logging into signin.ftse100company.com).

Consumers with infected devices cost enterprises a lot of internal resources (customer service hours, manual reviews) and money (fraud losses), impacting their bottom line. The risk of fraud and identity theft is especially high because malware often siphons data that establishes a browser or device fingerprint (a combination of operating system, IP address, browser type, system fonts, browser extensions, bookmarks, and other data). Companies frequently use browser fingerprints to authenticate customers, and cybercriminals can use the fingerprints to successfully impersonate consumers without raising any red flags.

One of the most widely used Windows infostealers that SpyCloud researchers observed over the course of the last year is RedLine Stealer. Available for purchase on the underground for about £ 635 GBP (or £ 160 GBP a month as malware-as-a-service subscription), RedLine Stealer is typically distributed through phishing campaigns, malicious search results for free or cracked software, and comment links in online videos. And it's an especially tricky malware to fight – security researchers found it can masquerade as legitimate downloads for software, such as Windows updates.

The true number of infected consumers for these industries 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.

Why are infected consumers the organisation's problem? Here are just a few ways cybercriminals exploit information stolen via malware:

- 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

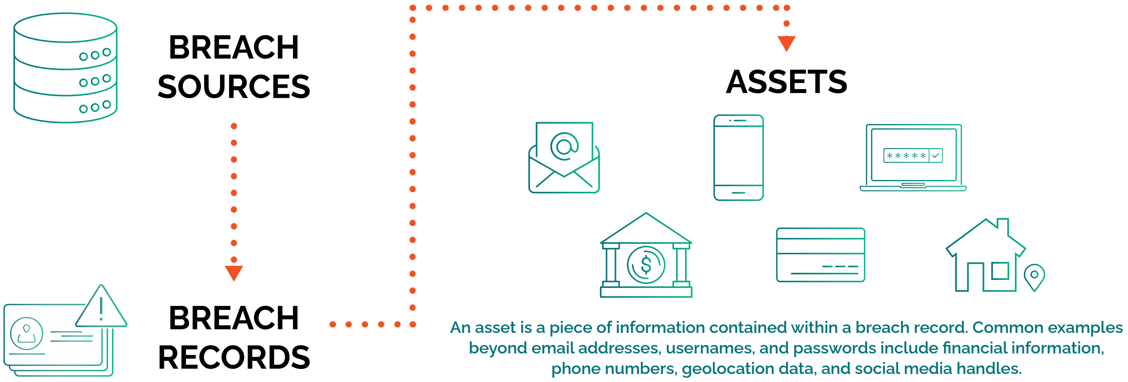
## Beyond Credentials: Other Exposures by Asset Type

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 create tremendous value for 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 **51 million breach assets** tied to FTSE 100 and subsidiaries' employees last year. This represents a **28.6%** increase from last year's analysis. We also found 83,983 records tied to the C-suite, which puts the companies at high risk for targeted schemes such as business email compromise, also known as CEO fraud, which are a leading cause of financial losses stemming from cybercrime.

Within the SpyCloud dataset, we have segmented certain types of assets into categories to help quantify different types of 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 beyond email addresses, usernames, and passwords include financial information, phone numbers, geolocation data, and social media handles.

## 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

PII 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
- Craft detailed, credible spear phishing messages
- Answer security questions to reset MFA
- Submit fraudulent applications

TOTAL **PII** ASSETS

**27,564,681**

AVERAGE PER COMPANY

**275,647**

TOTAL **PHONE** ASSETS

**676,076**

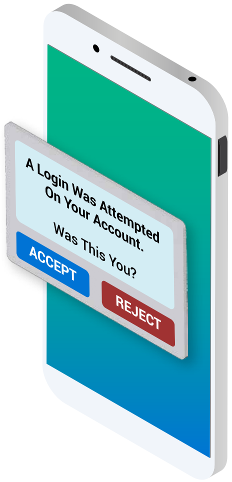
AVERAGE PER COMPANY

**6,761**

## 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 undetected.

## 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

TOTAL **GEO** ASSETS

**524,468**

AVERAGE PER COMPANY

**5,245**

TOTAL **FINANCIAL** ASSETS

**69,256**

AVERAGE PER COMPANY

**693**

## 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 harm your enterprise by:

- Making fraudulent purchases on corporate cards
- Reselling card numbers to other criminals
- Draining funds from accounts
- Collecting victims' tax refunds

## Asset Type: Social

### What It Is

Social assets include social media handles that are 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 |
|---|---|
| 3,656,672 | 36,567 |

| TOTAL **ACCOUNT** ASSETS | AVERAGE PER COMPANY |
|---|---|
| 2,554,481 | 25,545 |

## 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.

## Asset Type: Combo List Appearances

### What It Is

Short for combination list, a combo list contains pairs of passwords and usernames or email addresses obtained from various breaches. SpyCloud finds that the vast majority of the data we see in combo lists is old – ingested months or even years prior to the list publication. Our focus is on recapturing data immediately after a breach occurs.

### How It Helps Criminals

Inexpensive or even freely available on the underground, combo lists are used for credential stuffing. Cybercriminals take advantage of the high password reuse rates among users and try the logins from the combo lists on other websites or apps. Any accounts using the same credentials found on a combo list remain in jeopardy. Combo lists serve as a good reminder that even old data can still be useful to criminals.

TOTAL **COMBO LIST** COLLISIONS

**2,176,979**

AVERAGE PER COMPANY

**21,769**

INFOGRAPHIC

# 2022 FTSE 100 Identity Exposure

SpyCloud

**100**

**COMPANIES**

**AND THEIR SUBSIDIARIES**

## SPANNING THESE INDUSTRIES

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

**10,246**

### TOTAL BREACH SOURCES

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

**10,048,474**

### TOTAL BREACH RECORDS

A breach record is the 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.

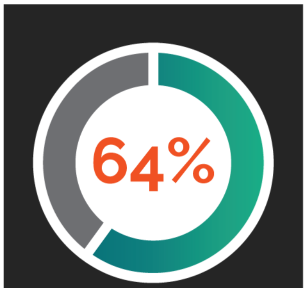
**Average number of breach records per parent company:**
100,485

**51,038,410**

### 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:**
510,384



### PASSWORD REUSE RATE

A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

### TOP 10 PASSWORDS

Use by FTSE 100 employees

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

**27,564,681**

### TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, NINOs, credit ratings, and more.

**Average PII Assets per parent company:** 275,647

**2,756,512**

### 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.

**27,565** Average number of exposed credentials per company

**15,896** Potentially exposed C-level executives

**9,522** Malware-infected employees

## Your Plan of Action

SpyCloud's analysis of FTSE 100 companies' and their subsidiaries' exposure as a result of third-party breaches and malware-infected devices has revealed more than 51 million assets in criminals' hands, 2.75 million of which are plaintext passwords tied to company employees. Combined with high rates of password reuse, these exposures represent significant account takeover risks for these organisations and the companies and consumers doing business with them.

To defend against account takeover, malware, ransomware and other malicious cyberattacks, FTSE 100 companies cannot bet solely on their employees to keep them safe and rather should think of users as consumers whose behavior expands the attack surface multi-fold. To minimize exposure and safeguard data, enterprises need to enforce strong enterprise password policy with SSO where possible, create clear company policies on the use of business and personal devices, enforce multi-factor authentication on critical accounts, and mandate the use of password managers, as well as leverage continuous, actionable intelligence into their users' exposure – especially in industries entrusted with a vast amount of sensitive consumer data.

Essentially the enterprise must protect users from themselves. But breaking bad cyber hygiene habits is an uphill battle. The most effective way to minimize your exposure is by using data from the criminal underground against the adversaries. This data adds an advanced layer of protection by helping you understand your riskiest users (such as those with stolen device fingerprints due to a malware infection) and take corrective action before criminals can exploit that data.

## About SpyCloud

SpyCloud transforms recaptured data to protect businesses from cyberattacks. Our products leverage a proprietary engine that collects, curates, enriches, and analyzes data from the criminal underground, driving action so enterprises can proactively prevent account takeover and ransomware, and protect their business and consumers from online fraud. Our unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings.

SpyCloud customers include half of the 10 largest global enterprises, midsize companies, and government agencies around the world. Headquartered in Austin, Texas, SpyCloud is home to over 150 cybersecurity experts who aim to make the internet a safer place.

### Enterprise Protection

Learn More

### Consumer Fraud Protection

Learn More

### Cybercrime Investigations

Learn More

### Data Partnerships

Learn More

Learn more at **spycloud.com**

SpyCloud