SpyCloud

2021 Special Report:

Telecommunications Industry Credential Exposure

Introduction

Telecommunications companies have always faced unique cybersecurity challenges. They build, control and operate the critical infrastructure used to communicate and store enormous amounts of sensitive data. They are also responsible for securing a huge number of mobile subscribers' accounts as well as their personal data. While telcos have made significant improvements in securing their networks in recent years, two challenges are stubbornly persistent:

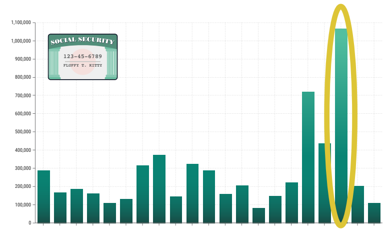
- Telecom executives and employees remain guilty of poor cyber-hygiene and password reuse.
- Data breaches continue to impact telecom customers every day.

Addressing the first challenge is fairly straightforward, as this report will explain. Addressing the second one, however, is more nuanced. Collectively, the telecom sector has maintained the position that while they secure customer accounts and the communications infrastructure we all depend on, they are less responsible when those customers fail to protect themselves. In other words, "other companies' account compromises" are not their responsibility.

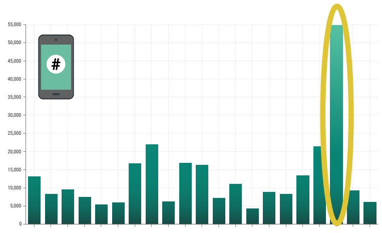
This seems logical, but breach data tells another side of the story.

Bad Habits of Telco Execs and Employees Expose Customers and Other Industries to Fraud

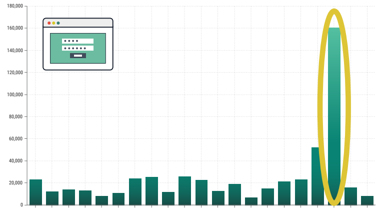
Each year, SpyCloud analyzes its entire database of over 130 billion assets collected from data breaches to demonstrate the scope of exposure affecting large enterprises. In 2021, our researchers found **543 million breach assets tied to employees at Fortune 1000 companies – up 29% from last year.** There are 11 telcos total in the Fortune 1000. As you can see in the illustration below, in terms of exposed assets ***per company***, telecom outpaces every other industry – including high-risk sectors such as Finance, Technology, Health Care and Defense – by a very wide margin.



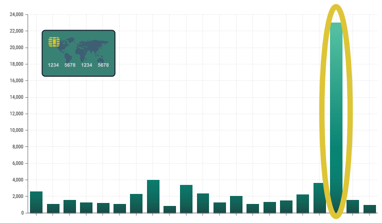
1,068,698
Exposed PII



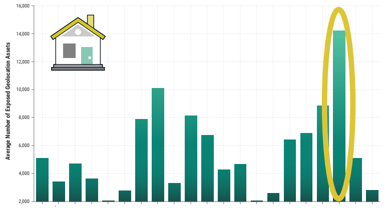
54,917
Exposed Phone Assets



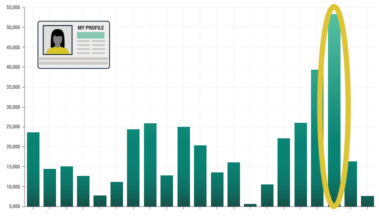
552,601
Exposed Passwords



23,029
Exposed Financial Assets



14,229
Exposed Geolocation Assets



53,350
Exposed Social Assets

37%

Increase in telecom fraud since 2017.[1]

93%

Of attempted mobile transactions in 2019 were fraudulent.[2]

50%

Surge in usage of mobile banking apps in 2020.[3]

2x

Fraud attacks in 2020 as the digital economy transformed.[4]

Every industry is vulnerable to cybercrime, but perhaps none more so than telecommunications. The infrastructure telcos operate is so vast that even false alarms can force them to shut down critical services. **A big reason for the industry's vulnerability is its high rate of password reuse.** SpyCloud has found that 76% of telco employees reuse passwords (or close variations) across multiple accounts. The use of stolen credentials is the leading cause of account takeovers (ATO) and data breaches. In fact, according to Verizon, 61% of breaches last year involved credentials.

Looking at the 11 telecom companies in the Fortune 1000, SpyCloud found nearly 40 million assets available to criminals, stolen from over 6,500 breaches. These pieces of data include email addresses, plaintext passwords, phone numbers, date of birth, home addresses, financial assets, and social handles.

Of those 40 million pieces of information from telco employees in criminal hands, over 6 million of them are credential pairs – plaintext passwords and corporate email addresses – that enable criminals to quite literally breach a person's work account (and potentially other personal accounts reusing those passwords) with little effort.

Taken as a whole, it rounds out to over 550,000 credential pairs per company – that's 8 per employee. On average, SpyCloud has found 8-10 exposures per email address in our database regardless of the industry, so this telecom-specific number is typical but no less alarming.

These exposures can not only cause damage to an organization's bottom line, but also its reputation among customers.

There is no excuse for anyone leaving corporate data exposed to criminals, regardless of industry. But employees and execs of telcos have a significantly larger responsibility. The enormous amounts of sensitive customer data they store is what makes them a magnet for criminals in the first place. When stolen, this customer data – names, addresses, passwords, credit cards, etc – provides fuel for criminals to perpetrate all kinds of malicious acts against other sectors, including ATO, financial fraud, ransomware, and even more impactful supply chain attacks.

So much of our lives (both business and personal) depend on telecom services and mobile devices, which is why providers tend to store a lot more of our data than other businesses. That data can get in the wrong hands in a variety of ways – a pilfered employee laptop, for example. The problem of stolen data is exceedingly worse in telecom because employees in this sector serve countless customers every day as part of a call center or help desk role and often have large amounts of sensitive customer data stored on poorly secured web apps. When those jobs are remote, they may have that data on unmonitored devices they use for both work and personal functions. This, along with password reuse, leaves the door open for ATO via brute force or credential stuffing attacks.

Working-From-Home Introduces New Mobile Security Challenges

At the height of the pandemic, cybercriminals found countless new opportunities in the form of a newly remote workforce. Even prior to the pandemic, employees using personal mobile devices for work purposes (like checking email or reviewing a document) presented complicated challenges for IT departments. Phishing attacks may be more successful on mobile devices because of the nature of the symbiotic, trusting relationships we have with them, and also because the screen size can make it harder to notice malicious emails or websites. Mobile devices are also easier to lose or have stolen than, say, a laptop, which in turn could lead to loss of critical data and productivity.

According to Verizon's 2021 Mobile Security Index, more than one in five companies said their mobile-device security was compromised in the past year.

Stolen Phone Numbers Are More Valuable Than You Think

When consumers learn that criminals have access to their social security numbers or passwords, they often feel violated. Those pieces of data are considered highly personal and thus kept closely guarded. Phone numbers are a different story. For the most part, those are not so secret, so they shouldn't be of much value to a criminal, right?

In recent years, as more digital services adopt multi-factor authentication (MFA), personal smartphones have become the primary touchpoint for businesses to confirm consumers are who they say they are. The theory is that criminals might have a user's password, but they probably don't have their physical phone. However, the right combination of stolen credentials allows criminals to bypass MFA using tactics such as SIM swapping and phone porting. With a simple call to a mobile carrier and some light social engineering, criminals can divert a consumer'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.

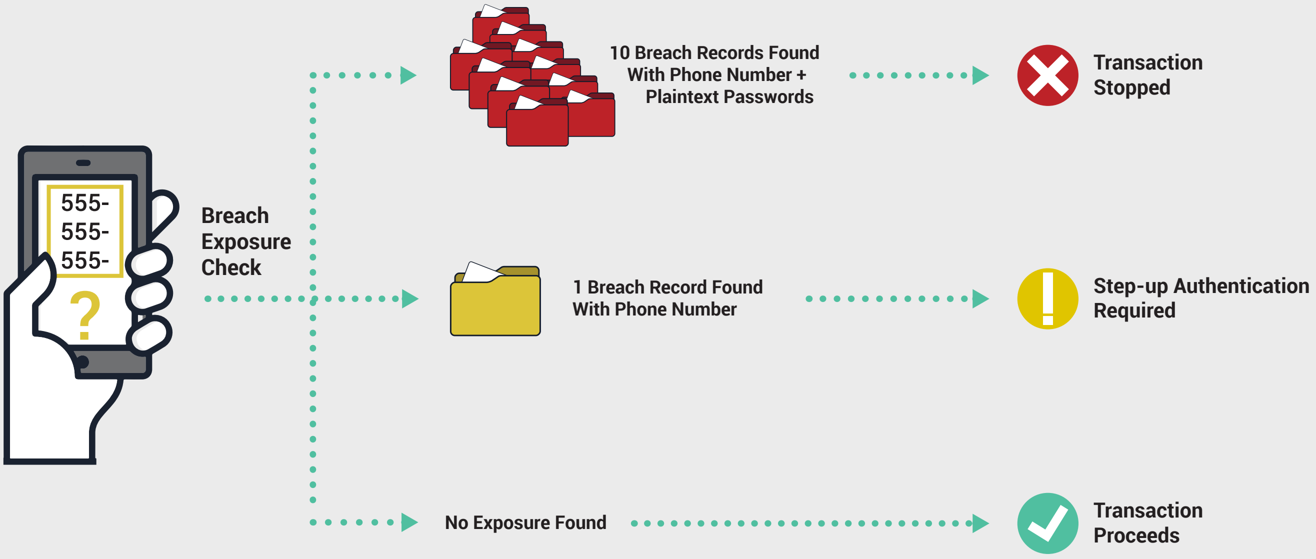
07623 is your PIN code
ACCESS GRANTED
07623

The severity of stolen phone assets tends to be glossed over. To consumers, the proliferation of telemarketing scams and robo calls proves phone numbers are already in the wrong hands. But this thinking ignores the fact that for nearly every business or service a consumer engages with digitally – including the federal government – phone numbers are their primary identifier. Therefore, telcos are highly encouraged to **treat phone numbers as primary identifiers of risk**. If criminals hijack a phone account to bypass MFA and intercept banking transactions, for example, they have compromised both the victim's financial service and the victim's mobile account. To telcos, this should be cause for alarm because they are now considered responsible for two account compromises at once.

SpyCloud Tip

Currently, there are over 3 billion phone assets in SpyCloud's database. In fraud risk algorithms, most organizations are used to checking usernames and email addresses for breach exposure, but adding phone numbers to that equation offers more robust insights than third-party identity authentication systems can provide.

In the example illustrated below, SpyCloud can search for breach records associated with the phone number, which could be flagged if it has been previously associated with fraud.


555-
555-
555-
?
Breach Exposure Check
10 Breach Records Found With Phone Number + Plaintext Passwords
Transaction Stopped
1 Breach Record Found With Phone Number
Step-up Authentication Required
No Exposure Found
Transaction Proceeds

This is a factor in fraud worth paying attention to. Even if you have already authenticated a user by other means, the ability to check that user's phone number against SpyCloud's database can reveal additional exposures that could help determine whether to delay or block a possible fraudulent transaction. It is very possible that a bad actor has taken over a user's account or even fooled biometric validation systems.

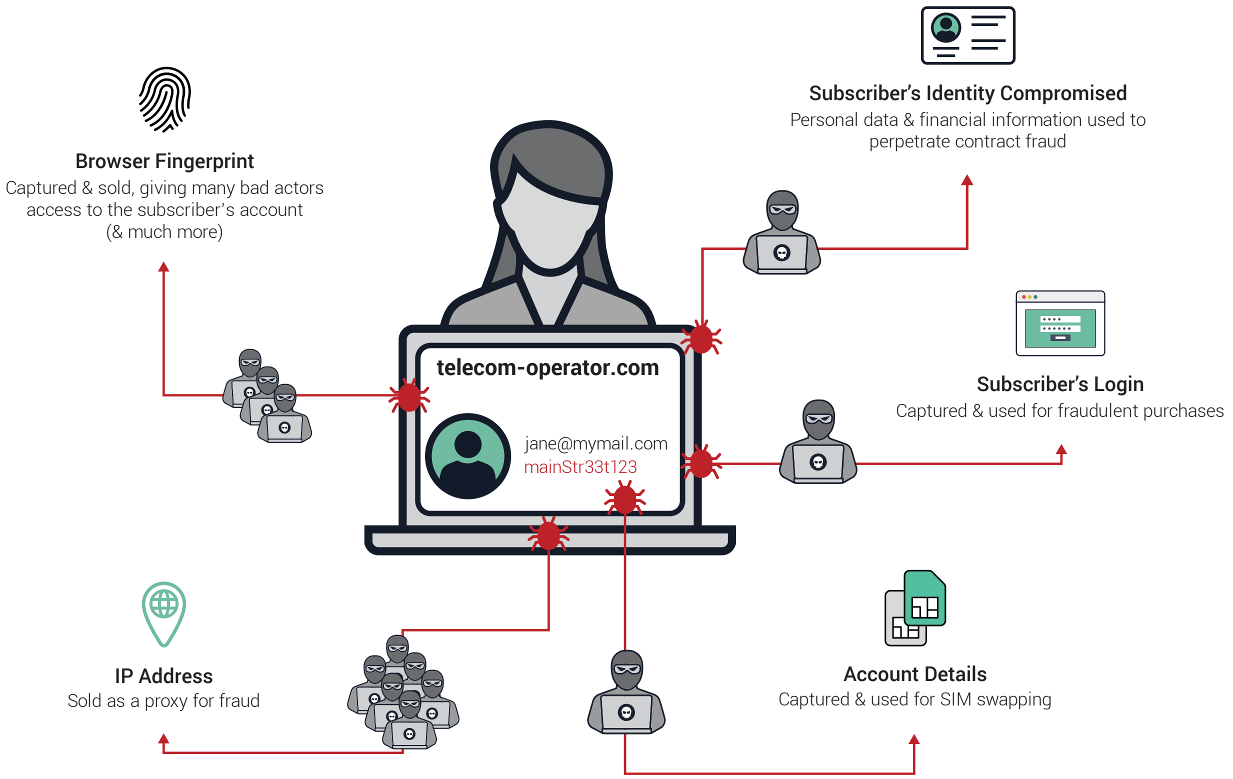
Malware Infections: From Employees to Consumers, It's a Problem for Telcos

To the dismay of security teams everywhere, people habitually click any link or file that lands in their inbox, whether they recognize the sender or not. In worst-case scenarios, innocent clicks lead to users' devices becoming infected with keylogger malware.

Malware with keylogging components can record a user's every move, capturing browser history, files, system information, and login data for corporate and third-party resources. SpyCloud identified 28,201 potentially infected Fortune 1000 employees, with telcos having the second highest total (after the Technology sector) at 2,328.

While all exposed credentials can put enterprises at risk, employees using systems infected with malware are particularly dangerous. That holds true regardless of whether the infection is located on the employee's personal or corporate system, both because of the breadth of data collected and the high likelihood of crossover usage between devices. Within SpyCloud's data, we regularly see evidence that employees have used infected personal devices to access enterprise resources.

Unfortunately, the malware problem doesn't end with telecom employees. SpyCloud identified 59,669 potentially infected consumers of their services. These are users of the telecoms' consumer-facing sites, where keylogger malware is harvesting the usernames and passwords (along with other personal and system information) for bad actors.

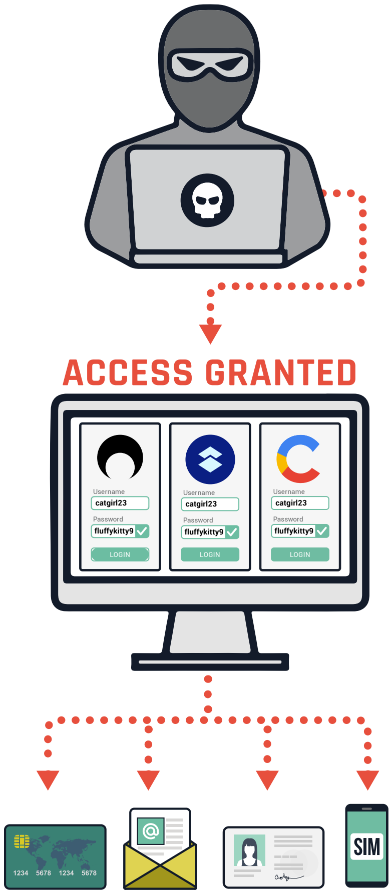

Subscriber's Identity Compromised
Personal data & financial information used to perpetrate contract fraud
Browser Fingerprint
Captured & sold, giving many bad actors access to the subscriber's account (& much more)
telecom-operator.com
jane@mymail.com
mainStr33t123
Subscriber's Login
Captured & used for fraudulent purchases
IP Address
Sold as a proxy for fraud
Account Details
Captured & used for SIM swapping

The true number of infections is likely higher because our analysis excluded many consumer-only domains. It also removed credentials with usernames instead of email addresses because it's unclear whether they are employee or consumer records. However, each one of these is at extremely high risk of ATO, identity theft, and online fraud, which can result in substantial losses for individuals and brand damage for affected businesses.

The Consequences of Account Takeover

Criminals typically takeover accounts for profit, pure and simple. Just as there are different approaches to ATO, there are countless ways to commit fraud.

With stolen data, criminals will:



Drain financial accounts, crypto wallets or loyalty point balances

Criminals will take control of financial accounts and immediately wire or transfer the balance from victims' accounts. In a twist on this concept, there has been a huge uptick in peer-to-peer payments fraud, up 733% since 2016.

Make fraudulent purchases

Another quick scheme: criminals will purchase goods using stolen or stored credit card or gift card data. In fact, 40% of all fraudulent activity associated with an account takeover occurs within a day.

Commit telecom subscription fraud

Combining fake and legitimate (stolen) customer data, criminals can create new "synthetic" identities to enable the fraudulent use of telecom services. Once established, these fake subscriptions give criminals access to value-added services, including TV, and internet, and new mobile financial services.

Exploit victims' work accounts

Criminals may try to locate and steal corporate IP and deploy business email compromise scams, which resulted in $1.8B in losses in 2020 alone.

SIM swap victims to bypass MFA

In a SIM swap attack, criminals transfer a victim's phone number to their own SIM card in order to bypass multi-factor authentication and take over sensitive accounts.

ATO is a scary and dangerous threat with the potential to inflict significant financial harm on businesses and individuals. With so many entry points into cloud-based systems and networks, ATO presents one of the greatest risks to our digital world. Criminals don't need to use sophisticated technologies to breach firewalls or other security measures intended to protect the enterprise. They just need passwords or phone numbers.

Even with all of the security measures businesses put in place to prevent these attacks, the needle is moving in the wrong direction. In 2019, ATO was the top fraud method with a 72% year-over-year increase on financial accounts alone. In 2020, with COVID-19 disrupting our world, the year-over-year growth was startling – over 300%. And criminals owe much of it to bad online habits.

BAD HABIT →	HOW CRIMINALS EXPLOIT IT
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). 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. Password spraying 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 email addresses in our database exposed in more than one breach in 2020. That rate is even worse for telco employees; we found an average password reuse rate of 76%.	**Credential Stuffing Attacks** Credential stuffing makes it possible for criminals to profit from even very old breach data that they buy on the dark web and successfully take over multiple accounts. Credential stuffing tools let criminals test credential pairs against a number of websites to see which additional accounts they can take over; hence why password reuse is so dangerous.
We Click On Links 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 devices becoming infected with keylogger malware.	**Keylogger Malware** Malware with keylogging components can record a user's every move, capturing browser history, files, system information, and login data for corporate and third-party resources. Among Fortune 1000 telcos, SpyCloud found 2,328 infected employees and nearly 60,000 infected consumers.

Preventative Measures

We recognize that fraud is a challenge that is constantly evolving, and its impact is not limited to the telecommunications industry. This makes combating and planning for schemes difficult, but there are common steps and best practices telecom companies can pursue that apply to many (if not all) forms of fraud. At the root of them all is a heightened awareness of exposed credentials and an increased vigilance about protecting them.

✓ Use Phone Numbers as Identifiers of Risk

In the entirety of the SpyCloud database, there are nearly 3 billion phone numbers that have been exposed in data breaches. A phone number is an identity marker that can be used to impersonate victims through SIM swaps, but on the flip side, it's also something that can be used to flag potentially fraudulent transactions, based on the number of times the phone number has been exposed in breaches. For some SpyCloud customers, even 1 appearance of a subscriber's phone number means the subscriber will go through another form of step-up authentication before the transaction will be approved. Ultimately, each company's risk tolerance will vary.

✓ Monitor Credentials for Compromise

It only takes one breach exposure for bad actors to break in, especially when passwords are reused to the degree we're seeing today (60% in 2020 according to SpyCloud's analysis). The ability to know which of your users' credentials have been exposed is critical to mitigating breach risk – and to keeping your subscribers' information locked down.

✓ Implement Multi-Factor Authentication

Implement MFA for as many of your public-facing websites as possible, as well as for internal resources that handle sensitive and confidential data. While it's not foolproof protection (attackers constantly seek out new techniques to thwart defenses), it provides an obstacle that may not be worth the effort to defeat for criminals looking to profit from low-effort credential stuffing attacks.

✓ Educate Employees and Subscribers

Cybersecurity teams should train users about preventative measures such as MFA, use of password managers, and recognizing phishing attempts, but they should also leverage proactive monitoring services that send alerts when user information is found in a data breach.

Once a cybercriminal knows the password for one account, they will test it on other accounts, and if the account owner has reused the password, the criminal has easy access. If the stolen credential includes a company email domain, the bad guys have a pretty good idea of where they might be able to access a corporate network and potentially valuable enterprise systems, customer data or intellectual property. That makes it extremely important for companies to identify vulnerable accounts early so they can lock them down and force password changes before they can be compromised.

With so many employees and customers, telcos will always be a criminal target, but taking preventative steps can go a long way to thwarting attackers and protecting the business community that depends on those services.

The SpyCloud Difference

SpyCloud's solutions are backed by the largest repository of compromised credentials and PII in the world. SpyCloud researchers collect an estimated one billion new breach assets per month, infiltrating criminal communities to recover stolen data early in the breach timeline so we can notify our customers of exposures as soon as possible – often months or even years before a breach becomes public.

Protect your mobile subscribers and employees from
credential exposures & account takeover fraud.

Request a Demo