

3.8 Billion Stolen Credentials are out there! How about yours?

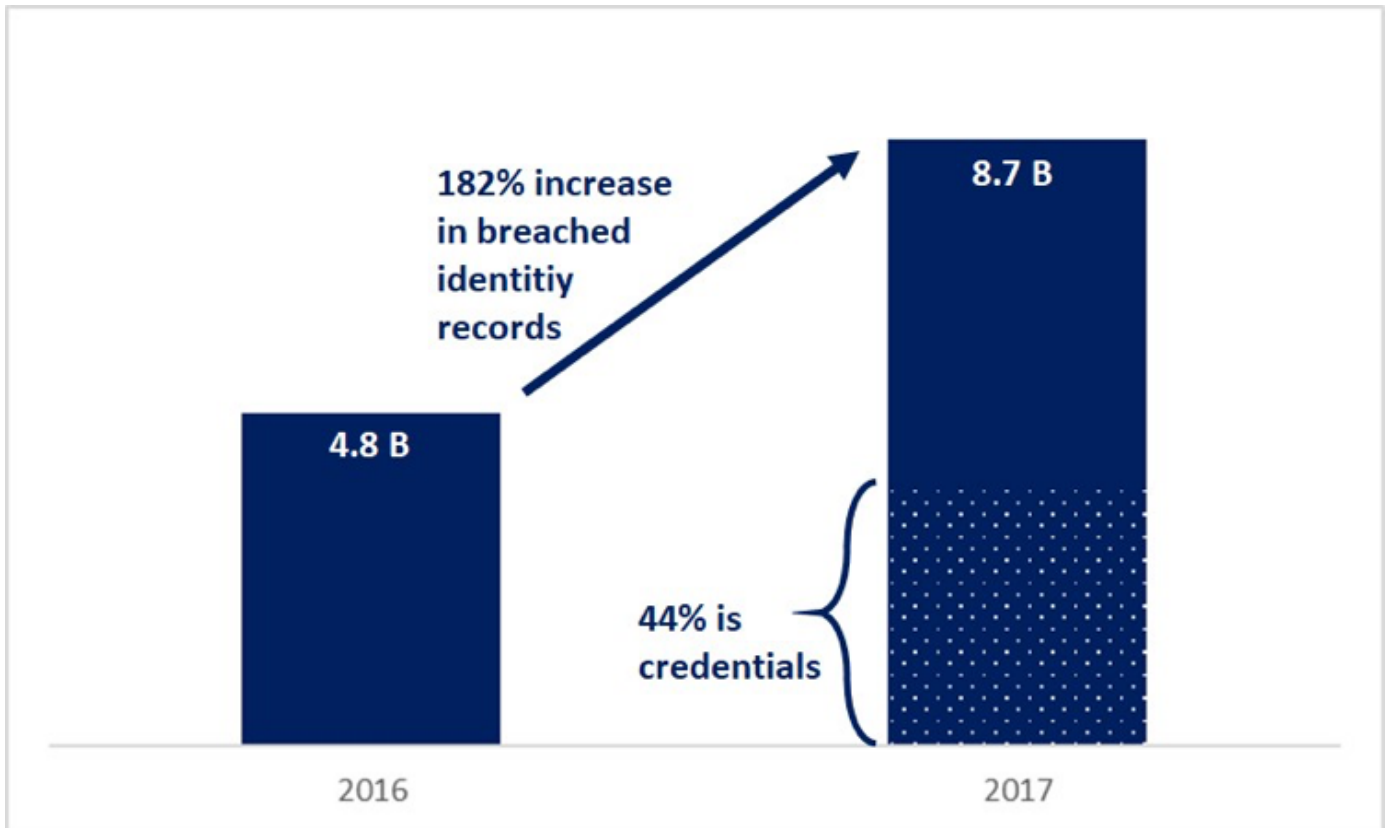
According to the 4iQ Identity Breach Report, 8.7 billion (detected and verified) raw identity-record data are on the surface, deep, and dark web in 2017, that is 182% increase compared to previous year. 44% of this data (around 3.8 billion) are usernames, passwords, and other credential information.



You may hack through credential stuffing

Credential stuffing is a method that hackers use to infiltrate a company's system by automated injection of breached username/password pairs. We can see credential stuffing in 2017 – OWASP Top 10 critical web application security risks report under the second most critical risk: Broken Authentication. Hackers use credentials to bypass anti-spam and firewall devices and access users' accounts. Once inside the company network, they can send phishing emails or compromise company systems/data. Note that

attackers just need to gain access to only a few account, or just one admin account to compromise the system. According to OWASP report, hackers do money laundering, social security fraud, and identity theft, or disclose legally protected highly sensitive information.



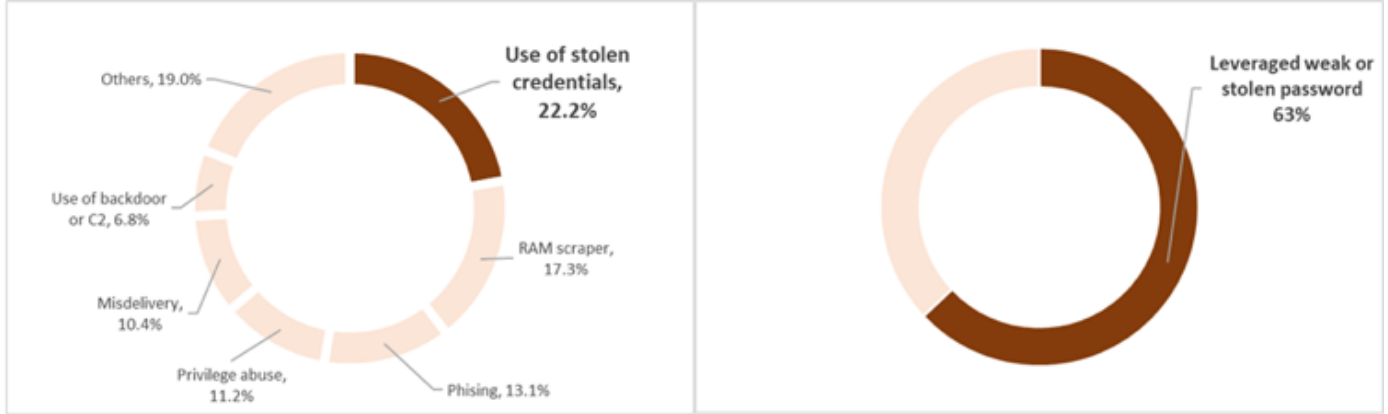
There are even some popular tools to ease credential stuffing. For instance, Sentry MBA can repeatedly try username/password list for a targeted website. It uses an IP address list to route the traffic through so that the source of login attempts vary. It even has built-in OCR capabilities for bypassing CAPTCHA-like counter-measures. Most people use same username/password combination on multiple login sites (cross credential use). If a breach list of a site is acquired, the attackers can use the same list for another

site by credential stuffing tools like Sentry MBA. The research shows that 1% to 2% success rate on cross credential use.

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

How bad is the situation?

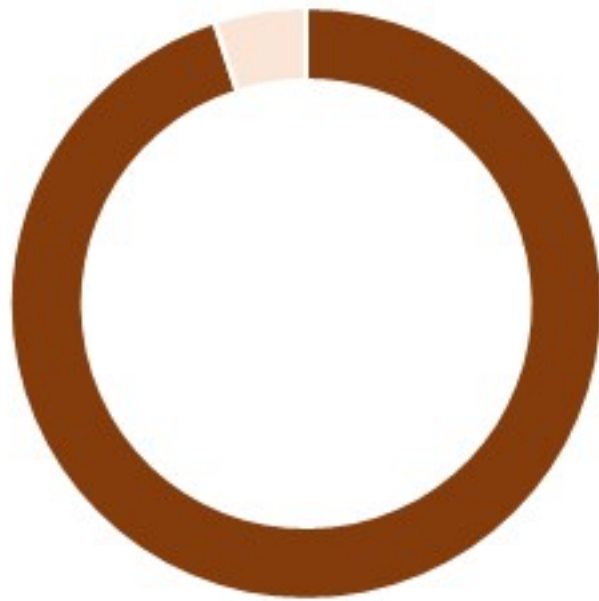
Use of stolen credentials is reported as #1 reason in 2018 Verizon Data Breach Investigations Report with being the cause of 22% of all breaches in 2017. 6 out of 10 confirmed data breaches in 2016 leveraged weak or stolen passwords.



Data Source: 2018 Verizon DBIR

Data Source: 2017 Verizon DBIR

NormShield has one of the largest commercial databases of hacked credentials to uncover client exposure and conducted a survey, which reviews trends and insights from Cyber Risk Scorecard key data points that include detailed external security risk data from cyber risk scoring for 5,217 organizations across multiple industries and over one million active assets on the Internet, including web and network devices. NormShield found a whopping 95% of respondents had exposed user credentials (for more information download [NormShield Cyber Security Risk Brief 2018](#)).



95%
**Had exposed user
credentials**

Industrial based comparison

NormShield 2018 Cyber Security Risk Brief also provides industry report cards (shown below) that gives a industrial-based comparison for different risk categories based on easy-to-understand A-F letter grading. While companies in Financial Services and Technology relatively better in Credential Management (even though they only receive an average score of F), companies in Healthcare, Professional Services, Education, and Retail perform very poorly and receive F.

Categories	Credential Management	Patch Management	IP Reputation	SSL Strength	DNS Security
Financial Services	D	D+	D+	B+	B
Healthcare	F	D-	F	C+	B
Professional Services	F	D-	D	B-	B
Technology	D-	D	D	B-	B+
Education	F	F	F	C+	B-
Retail	F	F	F	B	B-

Simple Steps to Prevent

- Use 2-factor authentication
- Change passwords at least quarterly
- Train employees:
 - Do not use company credentials for personal use (social media, online purchasing, etc. Research shows that nearly 75% of people still use duplicate passwords across multiple systems
 - Use different password for business, personal and banking
- Monitor cyber data leaks continuously

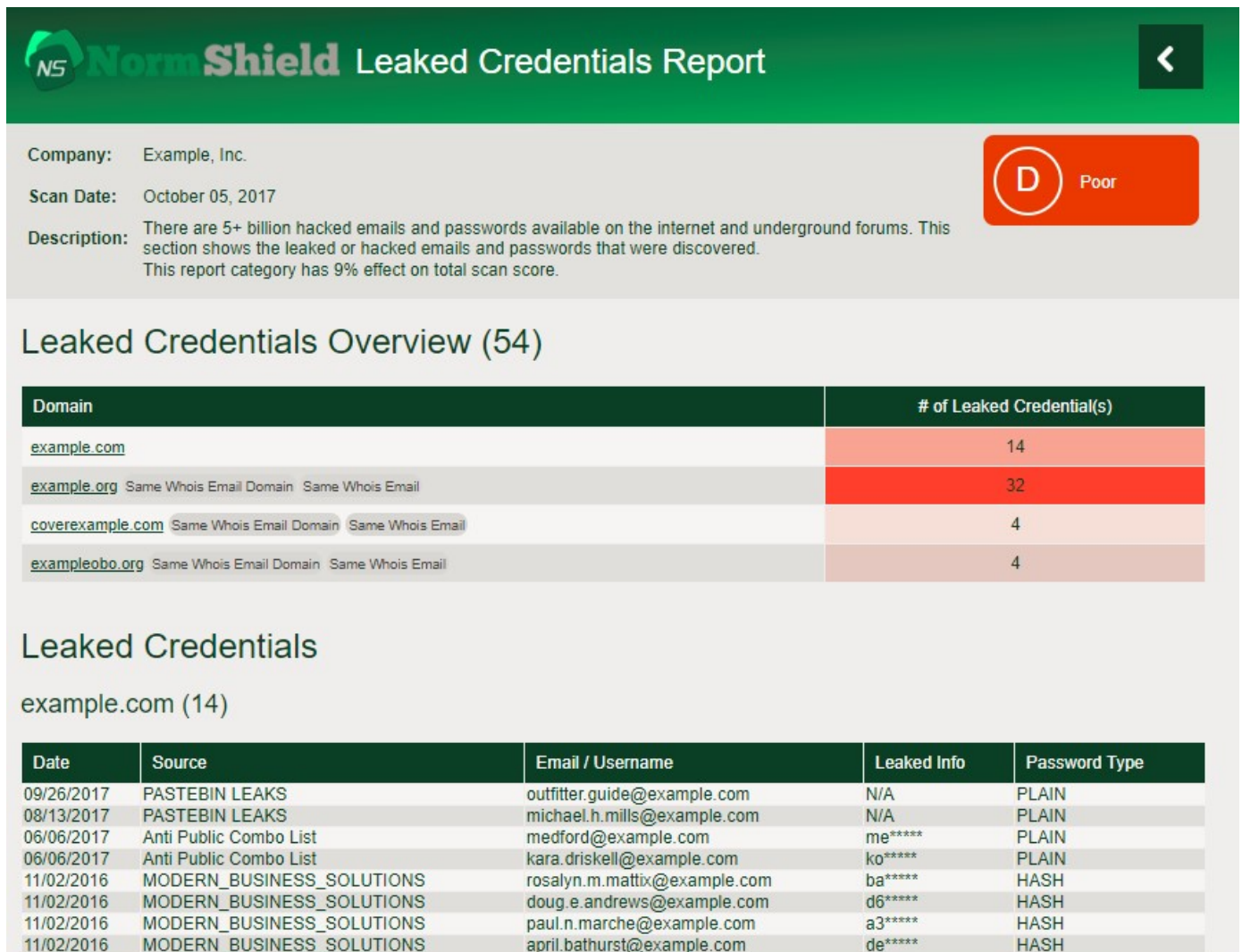
How to monitor data leaks and manage credentials

There are free tools for searching breach accounts.

NormShield also provide such a **free service** [here](#).

However, manual search will not be efficient. NormShield Cyber Risk Scorecard monitors surface, deep, and dark web

and provides not only leaked credentials with details but also an assessment of a company's cyber risk (which can be used for benchmarking).



NS NormShield Leaked Credentials Report

Company: Example, Inc. Scan Date: October 05, 2017

Description: There are 5+ billion hacked emails and passwords available on the internet and underground forums. This section shows the leaked or hacked emails and passwords that were discovered. This report category has 9% effect on total scan score.

D Poor

Leaked Credentials Overview (54)

Domain	# of Leaked Credential(s)
example.com	14
example.org Same Whois Email Domain Same Whois Email	32
coverexample.com Same Whois Email Domain Same Whois Email	4
exampleobo.org Same Whois Email Domain Same Whois Email	4

Leaked Credentials

example.com (14)

Date	Source	Email / Username	Leaked Info	Password Type
09/26/2017	PASTEBIN LEAKS	outfitter.guide@example.com	N/A	PLAIN
08/13/2017	PASTEBIN LEAKS	michael.h.mills@example.com	N/A	PLAIN
06/06/2017	Anti Public Combo List	medford@example.com	me*****	PLAIN
06/06/2017	Anti Public Combo List	kara.driskell@example.com	ko*****	PLAIN
11/02/2016	MODERN_BUSINESS_SOLUTIONS	rosalyn.m.mattix@example.com	ba*****	HASH
11/02/2016	MODERN_BUSINESS_SOLUTIONS	doug.e.andrews@example.com	d6*****	HASH
11/02/2016	MODERN_BUSINESS_SOLUTIONS	paul.n.marche@example.com	a3*****	HASH
11/02/2016	MODERN_BUSINESS_SOLUTIONS	april.bathurst@example.com	de*****	HASH

To act now and learn your cyber risk score on Credential Management among other categories, visit www.normshield.com