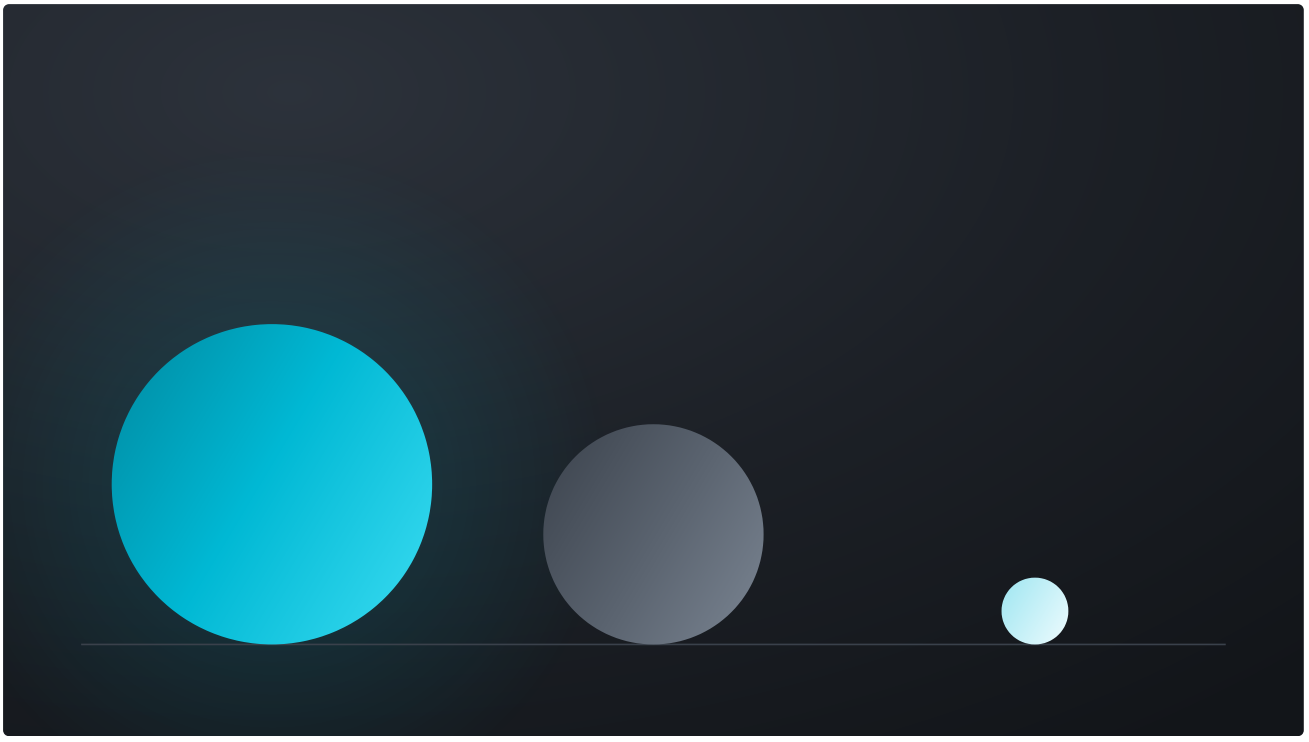
Black Shard

RESEARCH REPORT

Breaches loaded into Have I Been Pwned, January to March 2026

Every breach the service loaded in the quarter put another list of email addresses within reach of anyone who wants it, and nine of the thirty-two carried passwords. A firm whose staff reuse a password between a shopping site and the office mailbox inherits each of those nine.



Entity	Black Shard Pty Ltd · ABN 66 696 910 773
Document ID	BS-RPT-09
Classification	Public
Version	1.3
First published	12 May 2026
This edition	16 November 2026
Figures	Breaches added 1 Jan to 31 Mar 2026, read 12 May 2026

Executive summary

Have I Been Pwned loaded 32 breaches between 1 January and 31 March 2026, covering 198,871,187 accounts, or 198.9 million in round figures. January carried 8 breaches and 131,170,154 accounts, February 12 breaches and 62,005,326 accounts, and March 12 breaches and 5,695,707 accounts.

In the whole of 2025 the service loaded 91 breaches covering 2,877,214,727 accounts, or 2.9 billion in round figures. The 32 breaches of the quarter are 35 per cent of the 91 the service loaded in all of 2025, and their accounts are 6.9 per cent of that year's.

Have I Been Pwned is the public index of breached accounts. A breach reaches it after its data has been circulating, so the load date marks the point at which an exposure became searchable, and the credentials in it had usually been in criminal hands for some time before that. Every one of the 32 breaches exposed email addresses; 9 of them exposed passwords as well, covering 51,475,355 of the 198,871,187 accounts, and the other 23 exposed no password. The lists with passwords are tested as address and password pairs against every mailbox, portal and remote access gateway the attacker can find. The lists without them feed phishing and password spraying, where one common password is tried against every address on the list.

For a small or mid-sized firm the question the quarter puts is plain. Staff sign up to suppliers, conferences, software trials and shopping sites with their work address, and some of them use the office password to do it. When one of those sites is breached and loaded, the office password is in the list, and the attacker signs in with it.

The service flagged 3 of the 32 breaches as sensitive, 1 in January and 2 in March; a sensitive breach is left out of every public search and is shown only to the verified owner of the address or of the domain.

- Search your domain on the service and read which staff addresses appear in which breaches.
- Put phishing-resistant multi-factor authentication on email and remote access, so a password in a list is no longer enough to sign in.
- Give every staff member a password manager and make the office password one that exists nowhere else.

Method

The figures come from the public breaches feed the service publishes, which lists every breach it holds with the date it was added, the number of accounts in it, the kinds of data exposed and two flags, verified and sensitive. We read the feed on 12 May 2026, took every breach whose added date falls between 1 January and 31 March 2026, grouped those breaches by month, and summed their account counts.

The added date is the day the service loaded the breach. The breach itself may have happened months or years earlier, and the service's own documentation treats the breach date as a guide only, because breaches are often discovered and reported long after the incident. A month with a large count is a month in which a large exposure became searchable, and from that day the list is something anyone can test against a sign-in page.

Accounts are counted per breach, as the service counts them: the number of email addresses it loaded, which is usually lower than the figure reported in the press because of duplicates in the source data. An address that appears in two breaches is counted twice. The figures cover the breaches the service had loaded for the window by the day of reading. No breach is named here, because the names of the sites matter less than whether your staff had accounts on them.

Run the same search on your own domain

The service answers one question about a whole domain: which addresses on it appear in which breaches. A domain search asks you to prove you control the domain first, by a record in its DNS, a file or tag on its website, or an email to one of the standard administrative addresses. Once the domain is verified, the search lists every address on it the service has seen, the breaches each appears in, and the kinds of data each breach exposed. Sensitive breaches are included for a verified domain, which a public search of a single address never shows. A domain with few breached addresses is searched free of charge and a larger one takes a subscription.

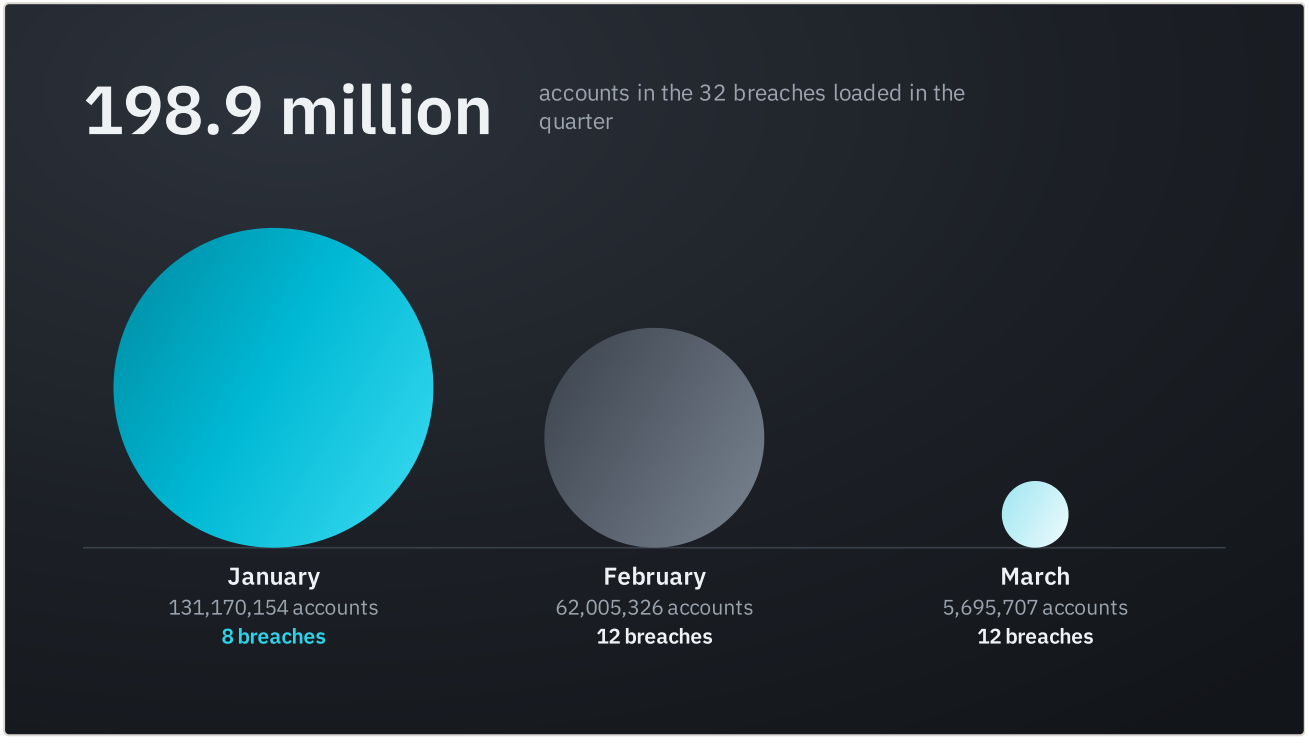
Read the result against your staff list. An address that belongs to someone who has left should already be disabled; confirm it is. For a current staff member, the question is whether the breach exposed a password and whether that password was, or is, the office one. Where it was, change it, look at that account's sign-in history since the load date, and check the mailbox for forwarding rules and sign-in alerts that did not come from the owner. Shared and role addresses deserve the same reading, because they carry the oldest passwords and the least ownership.

Keep the search current. The service publishes the most recently added breach as a single call, and its documentation describes the loop a firm can script: watch that call, and run the domain search again when a new breach appears. A staff member can also register their own address with the notification service and be told directly when it turns up in a new load.

The service also publishes its list of passwords seen in breaches, which a password manager or an identity platform can check by sending the first part of a hash and never the password itself. A firm that blocks any password on that list at the point it is set removes the most common way a breached credential comes home.

The quarter, month by month

ACCOUNTS IN THE BREACHES LOADED EACH MONTH, JANUARY TO MARCH 2026



January carried the most accounts in the fewest breaches; March carried the fewest accounts in as many breaches as February. Source: Have I Been Pwned breaches feed, breaches added 1 January to 31 March 2026, read 12 May 2026.

January carried 8 breaches and 131,170,154 accounts, February 12 breaches and 62,005,326 accounts, and March 12 breaches and 5,695,707 accounts. The average breach loaded in the quarter held 6.2 million accounts; the average breach loaded in 2025 held 31.6 million.

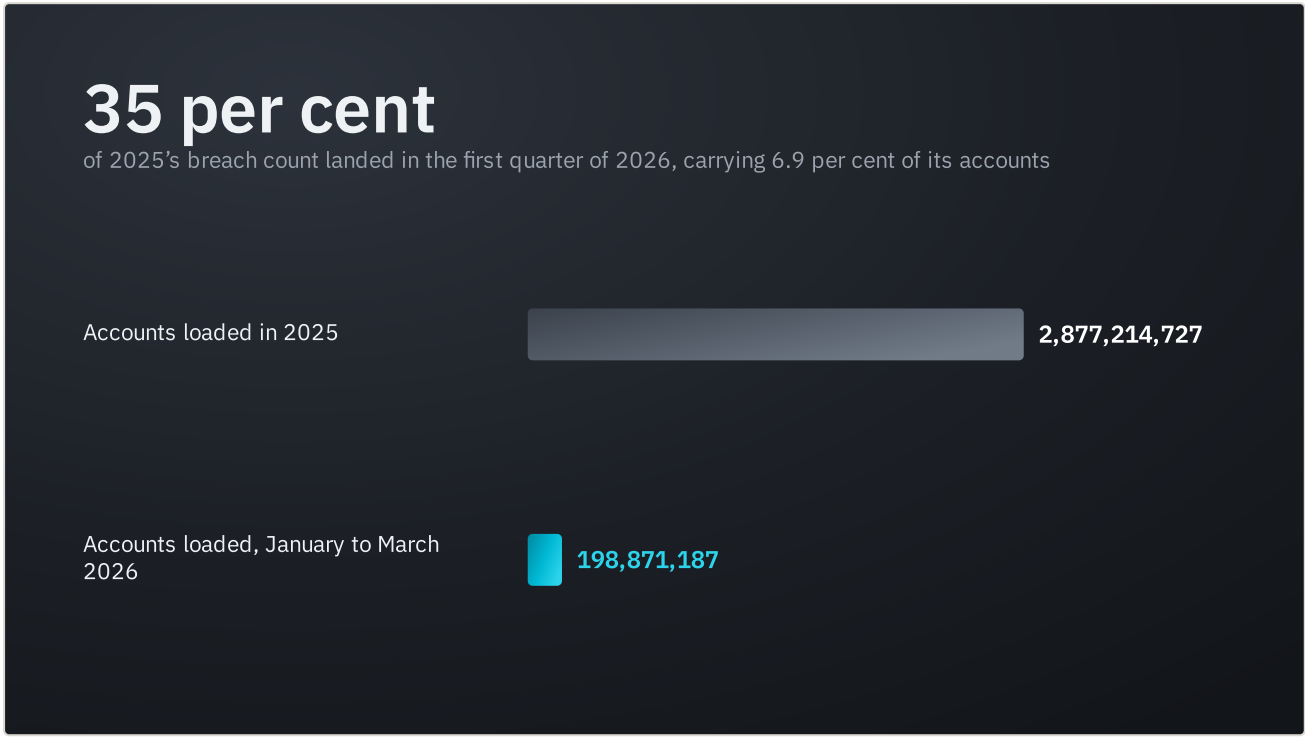
The months are uneven because the feed is driven by what arrives: one large consumer platform can carry more accounts than every other breach in the quarter together, and a month of small business and forum breaches can carry hardly any. The breach count is the steadier measure of how often exposures surface; the account count measures how many people each one reached.

The service marked all 32 as verified, its flag for a breach whose data it was able to attribute to the site named. An unverified load is one whose data could not be attributed beyond reasonable doubt to the site it was said to come from, and the service keeps such loads in the index because the addresses in them are real. A quarter in which every load was verified is a quarter in which each breach had a known source.

A small firm reads the monthly pattern as a schedule for its own checks. A domain search run once a quarter catches what was loaded since the last one; a check that runs on each new load turns the same work into something that happens the week the exposure surfaces.

Against the whole of 2025

THE QUARTER AGAINST THE WHOLE OF 2025



The quarter carried 35 per cent of 2025's breach count and 6.9 per cent of its accounts. Source: Have I Been Pwned breaches feed, breaches added 1 January to 31 March 2026, read 12 May 2026.

In the whole of 2025 the service loaded 91 breaches covering 2,877,214,727 accounts, or 2.9 billion in round figures. The 32 breaches of the quarter are 35 per cent of the 91 the service loaded in all of 2025, and their accounts are 6.9 per cent of that year's.

Breaches arrived at a faster pace than they did in 2025, and they were smaller. That is the shape to expect: a handful of very large breaches dominate any year's account total, and a quarter without one of them looks light by

accounts while the number of distinct exposures keeps rising. The lists attackers test against small firms are assembled from thousands of smaller breaches, each contributing the staff of a few hundred businesses.

The comparison also shows why a firm cannot wait for a headline. Most of the breaches that reach the service never make the news. The ones that do are the largest by accounts, and the small ones are where a staff member's office password sits.

What a loaded breach does to a firm that reuses passwords

The attack that follows a loaded breach that carried passwords is credential stuffing: the list of addresses and passwords is fed to software that tries each pair against popular sign-in pages, including the business email platforms most Australian firms use. The pairs that work are sold on or used. A password reused between a breached site and the office is a working pair.

The sign-in that results looks like the staff member. It comes with the right password and often from a residential connection in the right country, and it lands in a mailbox that holds client correspondence, invoices and the password reset links for every other system the person uses. From there the attacker reads, sets a forwarding rule, and waits for an invoice whose bank details can be changed. None of it needed a weakness in the firm's own systems; it needed one staff member's account on a site the firm had never heard of.

Multi-factor authentication breaks the chain for the sign-ins that honour it, which is why it is the first control after the password manager. It is bypassed where the second factor is a push notification the person approves out of habit, or where the attacker steals the signed-in session instead of the password. Phishing-resistant methods, a passkey or a hardware key, close the first route for email and remote access. A stolen session is answered by short session lifetimes, sign-in conditions that require a managed device, and revoking every session the moment a mailbox shows a rule or a sign-in the owner did not make. The remaining risk is the system that was left out: the legacy portal, the shared mailbox, the supplier login with the old password. Read the domain search result against the list of accounts excluded from multi-factor authentication, because an exposed password on an excluded account is the pair that works.

The service flagged 3 of the 32 breaches as sensitive, 1 in January and 2 in March; a sensitive breach is left out of every public search and is shown only to the verified owner of the address or of the domain. Those are breaches of sites a person may not want associated with their name, and the ones most likely to be used for pressure as well as for sign-in. The firm sees them in a verified domain search, and the reading is done quietly, with the person, and only to the extent of changing the password and checking the account.

What to do

The work takes a day for a firm of ordinary size, and most of it is reading a list and talking to the people on it.

1. Verify your domain with the service and run a domain search. Keep the result with the date it was run.
2. For every current address in the result, establish whether the exposed password is in use anywhere at the firm, and change it where it is.
3. Confirm every departed address in the result is disabled, and that its mailbox and licences are closed.
4. Roll out a password manager to every staff member, with the office password generated inside it and held nowhere else.

5. Enforce phishing-resistant multi-factor authentication on email, remote access and every system that holds client information, and keep a dated list of the accounts excluded from it.
6. Block passwords that appear in the service's breached password list at the point they are set, through your identity platform or the password manager.
7. Run the domain search again on each new load, or on a calendar at least once a quarter, and name the person who acts on the result.
8. Rehearse the first hour after a stuffed credential works: revoke the sessions, reset the password, remove forwarding rules, read the sign-in history and tell the client whose invoice was in the mailbox.

We run credential exposure monitoring for clients, reading each new load against their domains and acting on the addresses that appear, and we roll out multi-factor authentication and password managers across a firm with the exceptions named and closed. A firm that wants the first search done and the controls in place can engage us for both.

Our record

Black Shard builds and defends the systems Australian organisations run on.

The record is as held at 16 November 2026, the date this edition was revised.

- SMB1001:2026 Gold, issued by CyberCert, valid 16 Jun 2026 to 17 Jun 2027.
- Essential Eight Maturity Level 3, assessed September 2026.
- Prequalified supplier to Queensland councils under Local Buy arrangement LB308, ICT Solutions, Products, Services and New Technologies.
- Prequalified supplier under the NSW Government ICT Services Scheme (SCM0020).
- Holder of Victorian Fair Jobs Code pre-assessment certificate FJC-261023-11119, required for Victorian Government threshold and high-value procurement.
- Approved supplier on the Tasmanian Government Technology Services List (TSL) for Application Development Services, Operational Technical Services and Cyber Security.
- Our CISO holds the Exemplar Global ISO/IEC 27001:2022 Lead Auditor credential.
- Professional indemnity, public liability, cyber and workers' compensation insurance, all current.
- More than 65,000 tests across our repositories, counted on 26 October 2026.
- More than 1,500 deploys and releases shipped since 27 April 2026.

> 24/7 incident line: 1800 370 270.

Sources

- Have I Been Pwned, the breaches API, breaches added 1 January to 31 March 2026, read 12 May 2026: https://haveibeenpwned.com/api/v3/breaches
- Have I Been Pwned, API documentation: the breach model, domain search and Pwned Passwords: https://haveibeenpwned.com/API/v3

— Have I Been Pwned, frequently asked questions: sensitive, unverified and subscription-free breaches: https://haveibeenpwned.com/FAQs
— Have I Been Pwned, Pwned Passwords: https://haveibeenpwned.com/Passwords