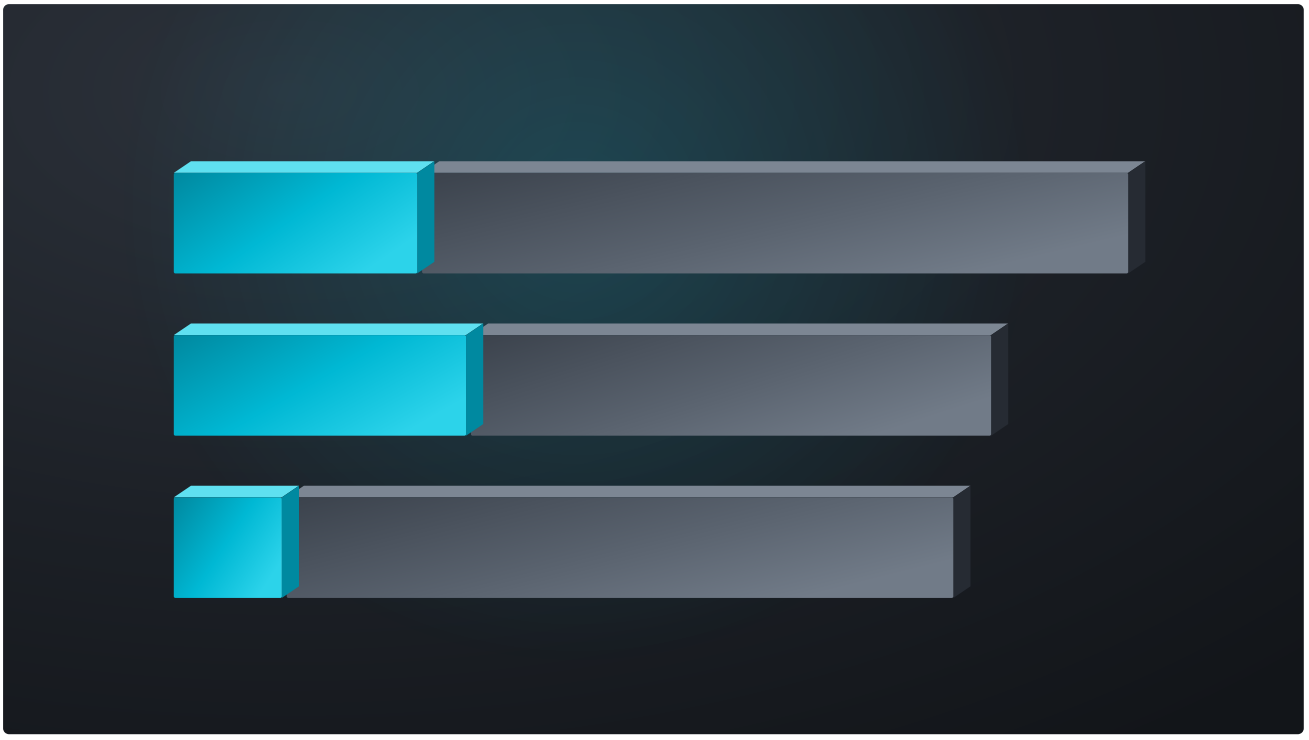
Black Shard

RESEARCH REPORT

Breaches loaded into Have I Been Pwned, July to September 2026

The service loaded fewer breaches from July to September 2026 than in either earlier quarter of the year, and the email addresses in every one of them joined the lists used for phishing and password spraying. Nine months in, the year has already loaded more breaches than the whole of 2025.



Entity	Black Shard Pty Ltd · ABN 66 696 910 773
Document ID	BS-RPT-15
Classification	Public
Version	1.1
First published	11 November 2026
This edition	16 November 2026
Figures	Breaches added 1 Jul to 30 Sep 2026, read 11 Nov 2026

Executive summary

Have I Been Pwned loaded 25 breaches between 1 July and 30 September 2026, covering 162,630,114 accounts, or 162.6 million in round figures. July carried 7 breaches and 89,879,195 accounts, August 11 breaches and 30,199,366 accounts, and September 7 breaches and 42,551,553 accounts.

From 1 January to 30 September 2026 the service loaded 104 breaches covering 531,949,423 accounts; in the whole of 2025 it loaded 91 breaches covering 2,877,214,727 accounts. Nine months of 2026 brought 13 more breaches than the whole of 2025 and 18.5 per cent of that year's accounts.

Every one of the 25 breaches exposed email addresses; 2 of them exposed passwords as well, covering 23,417,285 of the 162,630,114 accounts, and the other 23 exposed no password. Passwords were among the exposed data in 9 of the 32 breaches loaded from January to March 2026, covering 51,475,355 accounts, and in 9 of the 47 loaded from April to June 2026, covering 61,596,500 accounts. A quarter with few password lists still feeds the attacks a small firm meets most often. A list of working email addresses is what a phishing campaign is sent to, and it is the list a password spraying run works through, trying one common password against every address on it.

The largest breach loaded in the quarter held 55,282,226 accounts, 34 per cent of the quarter's total; the average breach held 6.5 million. One large breach can carry a third of a quarter's accounts, and the many small ones carry the addresses of staff who signed up to a supplier portal, a conference or a trial with their work address.

- Search your domain on the service each quarter and read which staff addresses appear in which breaches, and what each breach exposed.
- Put phishing-resistant multi-factor authentication on email and remote access, so a guessed or reused password is no longer enough to sign in.
- Block common and breached passwords at the point they are set, which is what defeats a spraying run.

Method

The figures come from the public breaches feed the service publishes. For each breach it holds, the feed gives the date the breach was added, the number of accounts, the kinds of data exposed (the data classes) and two flags, verified and sensitive. We read the feed on 11 November 2026, when the most recent breach had been added on 3 November 2026, took every breach whose added date falls between 1 July and 30 September 2026, grouped them by month and summed their accounts. The two earlier quarters of 2026 and the whole of 2025 were counted from the same read, the same way.

The added date is the day the service loaded the breach. The breach itself may be months or years older; the load date marks the day the exposure became searchable, and the addresses in it had usually been circulating before then. A breach is counted as exposing passwords when its data classes list passwords, in any form the source held them; a breach that exposed only a hint, a security question or a phone number is not counted that way.

Accounts are counted per breach, as the service counts them: the number of unique email addresses it loaded from that source. An address in two breaches is counted twice. No breach is named, because what matters to a firm is whether its own staff appear, and the domain search answers that directly.

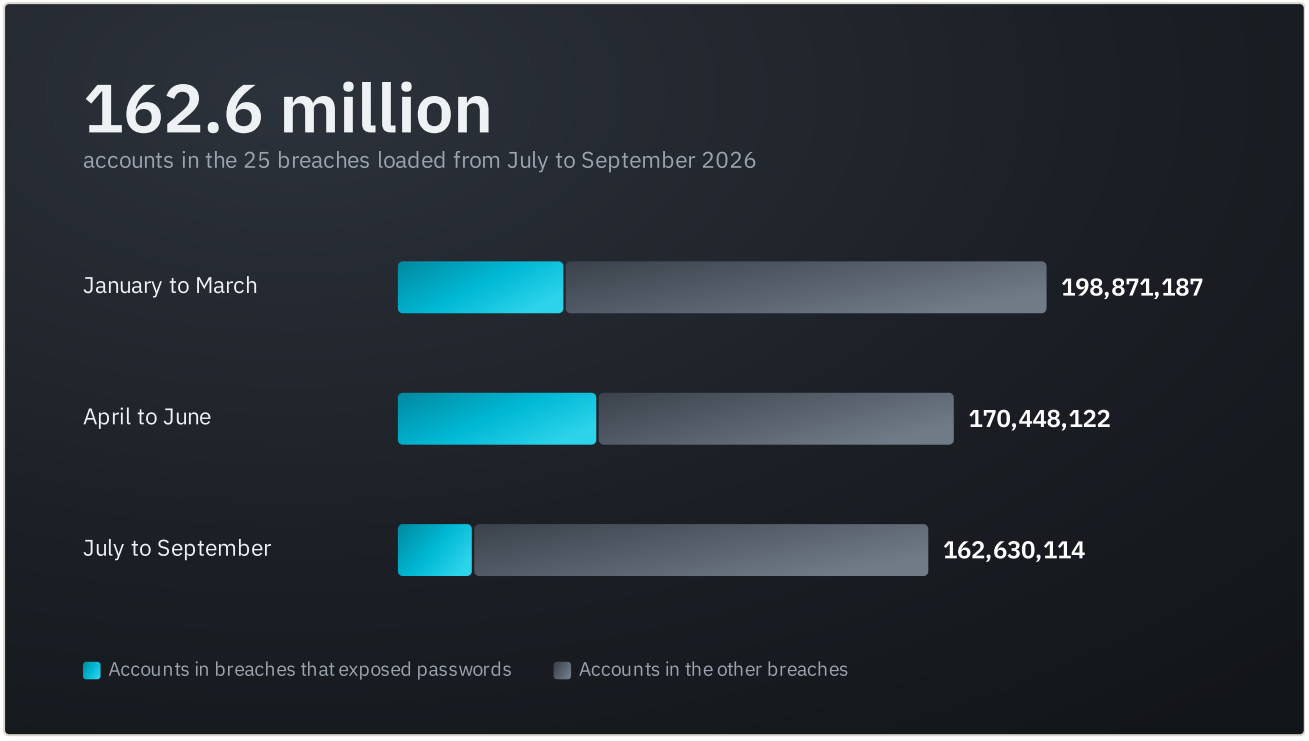
Read the data classes, as well as the count

A verified domain search lists every address on the domain the service has seen, the breaches each appears in and the data classes each breach exposed. Sort the result by data class. An address in a breach that exposed passwords needs the question of reuse asked and answered: was that password, or a variation of it, ever the office password. An address in a breach that exposed only names, addresses and phone numbers needs a different answer, because that data is what makes a phishing message or a call to the helpdesk convincing. Tell the staff member which details are out, so the next message that quotes them is read with suspicion.

The service also notifies a verified domain when one of its addresses appears in a new load. A firm that turns that on, and names the person who reads the notice, hears about each exposure in the week it becomes searchable.

Three quarters of 2026

ACCOUNTS LOADED EACH QUARTER OF 2026, AND THE ACCOUNTS IN BREACHES THAT EXPOSED PASSWORDS



Each quarter of 2026 loaded fewer accounts than the one before, and the accounts in breaches that exposed passwords fell to 23,417,285 in the third. Source: Have I Been Pwned breaches feed, breaches added 1 July to 30 September 2026, read 11 November 2026.

The service loaded 32 breaches covering 198,871,187 accounts between 1 January and 31 March 2026, and 47 breaches covering 170,448,122 accounts between 1 April and 30 June 2026. Have I Been Pwned loaded 25 breaches between 1 July and 30 September 2026, covering 162,630,114 accounts, or 162.6 million in round figures.

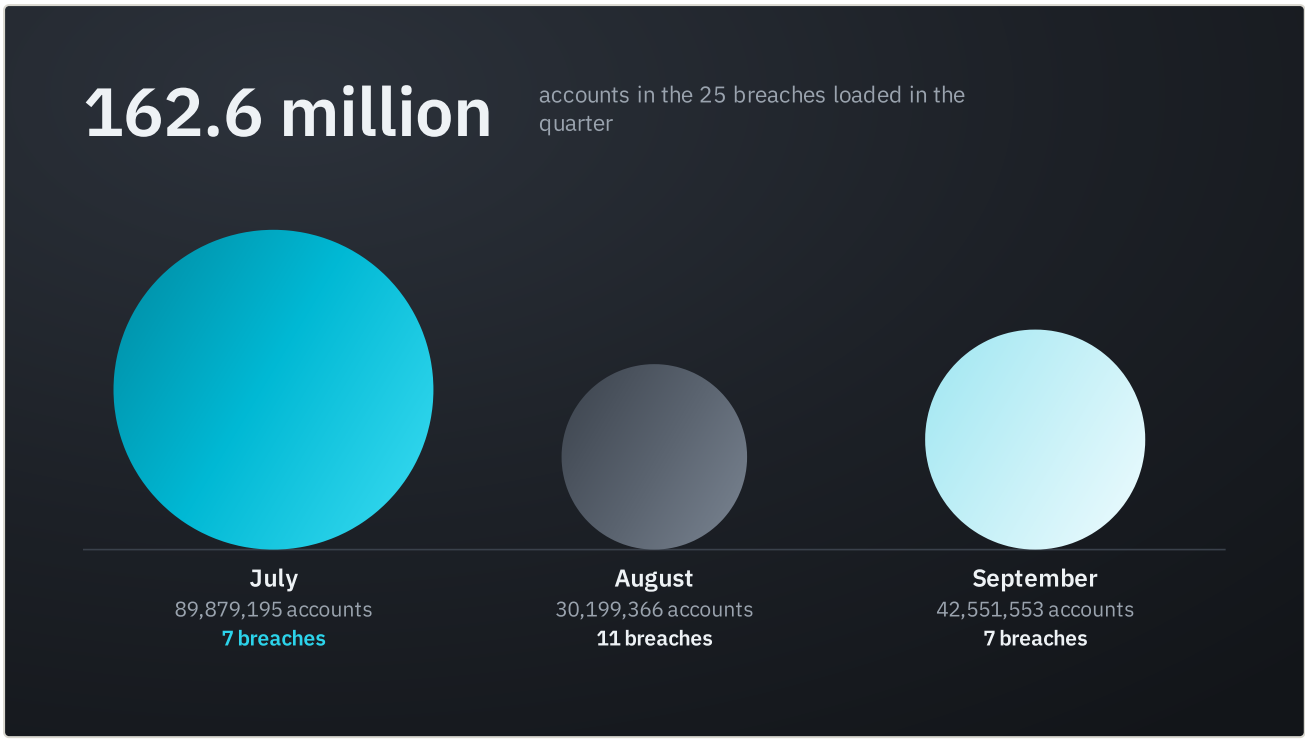
Passwords were among the exposed data in 9 of the 32 breaches loaded from January to March 2026, covering 51,475,355 accounts, and in 9 of the 47 loaded from April to June 2026, covering 61,596,500 accounts. Every one of the 25 breaches exposed email addresses; 2 of them exposed passwords as well, covering 23,417,285 of the 162,630,114 accounts, and the other 23 exposed no password.

Each quarter of 2026 loaded fewer accounts than the one before, and the third quarter's password lists were the smallest of the three. A lighter quarter does not retire the lists loaded earlier in the year. An address and password

pair loaded in March is tested against sign-in pages for as long as the password stays in use, so the firm's exposure is the sum of every load its staff appear in, and the quarter adds to that sum.

The quarter, month by month

ACCOUNTS IN THE BREACHES LOADED EACH MONTH, JULY TO SEPTEMBER 2026



July carried more accounts than August and September together, in as few breaches as September. Source: Have I Been Pwned breaches feed, breaches added 1 July to 30 September 2026, read 11 November 2026.

July carried 7 breaches and 89,879,195 accounts, August 11 breaches and 30,199,366 accounts, and September 7 breaches and 42,551,553 accounts. The largest breach loaded in the quarter held 55,282,226 accounts, 34 per cent of the quarter's total; the average breach held 6.5 million.

The service marked all 25 as verified, its flag for a breach whose data it was able to attribute to the site named. A verified load is one whose data the service could attribute to the site named, so each breach in the quarter had a known source, and a staff member who finds their address in one knows which account to close or change.

The monthly pattern follows what arrives. July's seven breaches carried more accounts than August and September together, and August's eleven carried fewer accounts than either of the other months. For a small firm the breach count is the steadier signal: each breach is another site where a staff member may have used a work address.

What an address list does without a password

A list of addresses with no passwords is the raw material for two attacks. The first is phishing: the list tells an attacker which addresses are live, and the other data in the breach, a name, a phone number, a supplier relationship, makes the message read as genuine. The second is password spraying: software tries a handful of the most common passwords against every address on the list, slowly enough to stay under the lockout threshold, and keeps the sign-ins that work.

Spraying works against accounts whose password is a season and a year, the firm's name with a number, or the default a new starter was given and never changed. Blocking those passwords at the point they are set, and blocking every password in the service's breached password list, takes the attack's whole wordlist away. Phishing-resistant multi-factor authentication on email and remote access closes the rest, because a correct password alone no longer signs in.

The service flagged 4 of the 25 breaches as sensitive, 2 in August and 2 in September; 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. The firm sees those breaches only in a verified domain search. Read them quietly, with the person, and only to the extent of changing the password and checking the account.

What to do

1. Verify your domain with the service, run the domain search and keep the result with the date it was run.
2. Sort the result by data class: ask the reuse question for every address in a breach that exposed passwords, and tell each staff member which of their details are out.
3. Turn on the service's notification for your verified domain, and name the person who reads each notice and acts on it.
4. Block common and breached passwords at the point they are set, through your identity platform or the password manager.
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. Watch sign-in logs for many failed sign-ins spread across many accounts from one source, which is what a spraying run looks like.
7. Close the accounts of departed staff and the shared mailboxes nobody owns; they carry the oldest passwords and appear in the oldest breaches.

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 30 September 2026 and in 2025, read 11 November 2026: https://haveibeenpwned.com/api/v3/breaches
- Have I Been Pwned, API documentation: the breach model, data classes and domain search: https://haveibeenpwned.com/API/v3
- Have I Been Pwned, frequently asked questions: sensitive and unverified breaches: https://haveibeenpwned.com/FAQs
- Have I Been Pwned, Pwned Passwords: https://haveibeenpwned.com/Passwords