Notably, phishing and spear phishing continue to be the most common and highly effective methods by which entities are being compromised—whether large or small—in Australia or internationally.[12] Within the period, a total of 153 data breaches were attributed to this method.

Attackers typically use phishing to elicit credentials—usually a username and password—from a user to gain access to systems. Attacker techniques continue to evolve in this area, making phishing emails increasingly difficult to detect without sustained and focused user education.

After phishing, the second most prevalent cyber incident data breach involved compromised or stolen credentials where the method of compromise was not known by entities reporting to the OAIC. An explanation may be the growing prevalence of 'credential stuffing' attacks using breached user credentials that have been leaked or posted online.

Excluding cyber breaches, social engineering or impersonation and actions taken by a rogue employee or an insider threat were also significant contributors to data breaches, as was theft of paperwork or data storage devices.

Credential compromise

Compromised or stolen credentials underpinned most cyber incidents that led to data breaches in the first year of the NDB scheme.

Phishing provides one explanation for how cyber attackers gain access to credentials. So-called 'credential phishing' typically involves attackers tricking a user into giving up their login details by emailing them a link to a realistic looking login page for a service they trust. Common examples include password reset requests that purport to be from legitimate web-based email providers such as Gmail or Office 365. When the user enters their login details into the fraudulent site, they are handing over their credentials to cyber attackers.

Credentials obtained this way account for 39 per cent of cyber incidents.

However, in 28 per cent of cyber incidents, the notifying entity was not aware of how the credentials were obtained, most likely because they had not detected any phishing-based compromise.

The trend of 'credential stuffing' offers a likely explanation. This involves attackers trying out usernames and passwords obtained from other data breaches on an entity's digital services. In recent years, large troves of credentials have repeatedly been posted online by hackers. These troves typically aggregate credentials from previous data breaches. A recent dump of credentials, dubbed Collection 1-5, totals 100 billion records.[26]

The primary reason credential stuffing works is that many users re-use usernames and passwords across multiple accounts and services. Typically, attackers automate much of the work involved in this technique.

How entities can reduce the risk of credential compromise

- Educating users on how to detect phishing emails.
- Implementing multi-factor authentication.
- Implementing anti-spoofing controls (such as DMARC or SPF).[27]
- Educating users about password re-use and security measures (for example, password managers and services such as 'Have I Been Pwned'[28] to detect compromised accounts).

The OAIC and the ACSC have also developed tips to assist entities to prevent and mitigate data breaches, including how to prevent credential compromise.[13]