

Ecovacs statement to ABC News

11 October 2024

Ecovacs does not provide public comment on individual consumer situations out of respect to the privacy of our consumers.

Ecovacs conducted a thorough internal investigation at the end of May 2024 and found no evidence to suggest that any usernames and passwords were obtained by unauthorised third parties as a result of any breach of Ecovacs' systems. This investigation also identified a credential stuffing event, in which a third party attempted to use email addresses and passwords to try to gain access to Ecovacs' customer accounts. There were significantly more attempts to log-in than the average daily amount, by a factor of 90:1. These all from the same IP address, which was identified as coming from both an unusual device, and an unusual location. This IP address was immediately blocked.

To keep consumers fully updated and stress the importance of changing their security protocols, Ecovacs sent a prompt email to customers on May 31-June 1 to change their account passwords.

Ecovacs takes its responsibility around security and data extremely seriously, it is a process undertaken with both internal and external industry experts, and we have implemented significant measures in this area, including in recent months, and will continue to do so on an ongoing basis. This includes improving the Remote Live Video PIN bypass issue, which is now resolved. To further enhance security, an Over-the-air (OTA) firmware update will be made available in the second week of November 2024 specifically for the X2 series. No other models in Australia are affected.

ECOVACS has always prioritised product and data security, as well as the protection of consumer privacy. We assure customers that our existing products offer a high level of security in daily life, and that consumers can confidently use ECOVACS products.

It is also important for consumers to implement their own steps to improve their level of personal online security, including strong passwords, unique passwords not used for multiple purposes, and to strengthen their Wi-Fi security.

More guidance can be found here:

<https://www.ecovacs.com/au/blog/robot-vacuum-privacy-concerns>

- Strengthen Wi-Fi Security

- Set Strong Passwords
- Regular Software Updates
- Suspicious Activity Notifications
- Factory Reset