byfields
business advisers

UPDATE: WESTNET OR IINET EMAIL DOMAINS

In our September 2024 newsletter, we informed you that we had observed a concerning rise in emails originating from Westnet and iiNet client accounts and that from 30 September 2024, Byfields would no longer accept any emails from the @westnet.com.au, @wn.com.au or @iiNet.net.au domains (Compromised Domains) which would be blocked by its firewall.

Byfields' internal IT manager has undertaken an extensive review of Byfields' IT systems and has confirmed that the receipt of the compromised emails was not due to a breach of Byfield's IT systems.

We have contacted The Messaging Company about the Compromised Domains and after consultation, we have been advised that The Messaging Company has the following security measures in place to maintain the integrity of its IT systems:

a) if it becomes aware that an email account has been compromised, it immediately restricts that email account's functionality, including the ability to send emails. It does not reinstate full functionality until a customer completes the steps outlined on this webpage (https://support.themessaging.co/hc/enau/ articles/10072832384527-I-think-my-account-has-been-compromised) and verifies their identity;

b) its cybersecurity practices are independently audited as part of its ISO 27001 certification and compliance. ISO 27001 is the leading international standard for information security, cybersecurity and privacy protection;

c) it has strict spam filters and offers Two Factor Authentication (2FA), including app-specific passwords. Customers have the option to use or not use 2FA;

d) it has a strict password policy and encourages customers to change old, weak passwords. As part of the recent transition, large numbers of customers have reset the email passwords that they likely held for many years and which previously put them at greater risk of being compromised (on any email platform).

In reliance upon the security measures that The Messaging Company has advised it has in place, we have decided not to block emails received from the Compromised Domains.

Byfields will instead continue to monitor this issue with the assistance of its internal IT manager and an external IT consultant and if necessary, will implement heightened security measures to protect our staff and clients.

If you have any concerns, please feel free to contact your local Byfields office.