

Insurance Companies May Pay Out Unnecessarily - Technology Changes & Government Adoption Means No More Spoofing

Email scams using a domain in an unauthorised manner should be over by now however slow adoption of DMARC has meant insurance companies have possibly been paying out unnecessarily. DMARC covers more than 80% of email users and has done for some years.

Organizations not taking the necessary steps to protect their domain from SPOOF messaging can now be held to account they have not:

- 1.) Implemented the free protection
- 2.) Implemented policies / mechanisms such as an Anti-Spoof Policy to help recipients of email determine the authenticity of the message.

This is not limited to commercial organizations, Government, Schools and NGO's are also potentially liable. To spoof an email and use a domain like bhpbilliton.com harrods.com, police.uk or apple.com is not difficult when left unprotected.

With EU privacy law changes it was a perfect opportunity to close this gap and regulators missed it. We estimate privacy breaches due to phishing emails using SPOOF domains is a primary data breach source.

The awareness of organizations of the technology was tested by a recent survey of top companies on various stock exchanges and in Australia the Local Government Authorities were also surveyed.

Organisation Group	Number Surveyed	Aware / Started	Passed
S&P 500	500	202	NA
FTSE 250	249	11	1
ASX 200	200	45	NA
TSX 60	62	23	0
NZ 35	35	4	0
IBEX 30	30	1	0
Local Government (AU)	570	23	1

The technology has now been mandated in the US, UK, Canada, Mexico, Portugal and Brazil however not one of the surveyed companies has an Anti-Spoof or Phishing policy on their website and email / email domains is often not explicit or referred to in commercial contracts.

Insurance organisations should use the GDPR to review client's domains and ensure the DMARC p=reject policy is part of the cyber insurance audit.

Insurance firms should protect their risk prior to discussing these matters with their clients. Your domain can be checked at <http://emailsendercheck.com>

If this is something you wish discuss further then please contact Zulu eDM and ask for David Barnes david.barnes@au.zululabs.com +61 3 9001 1590 | +61 413 243 423