June 2018

ZuluEDM
Target anyone, anywhere

Technology Changes & Government Adoption Means No More Spoofing Unless Negligent

Organizations can now be held to account if their email domain is spoofed if they have not:

1.) Implemented the free protection
2.) Implemented policies / mechanisms such as an Anti-Spoof Policy to help recipients determine if the email received is authentic.

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 police.vic.gov.au is not difficult.

If you are a victim of a crime that could have easily been prevented by a contributing party and the prevention was free does that give you a right to be compensated OR could / should a criminal charge be laid?

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.

Results as follows:

Organisation Group	Number Surveyed	Aware / Started	Passed
S&P 500	500	243	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.

Law 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