mimecast

The State of Email Security 2021

Key Findings in South Africa
Over the last 12 months.

The Digital Workforce Is Under Attack

84%
said the volume of email at their organisation has increased

65%
expect an email-borne attack will damage their business.
(up from 47% in 2020)

Biggest email security challenges in 2021

50%
of organisations say increasing sophistication of attacks

48%
say growing volume of attacks

52%
say employee naiveté about cybersecurity
(compared with 43% globally)

The Post-COVID Threat Landscape

Organisations saw the volume of email-related attacks increase:

57%
phishing with malicious links or attachments

49%
impersonation fraud or BEC

47%
fraudulent use of their company's brand via spoofed email

47%
internal threats or data leaks by compromised, careless or negligent employees

38%
misuse of their company's brand via spoofed website

Ransomware

47%
experienced business disruption from ransomware
(increase from 45% reported last year)

7 Days
average days of downtime. **For 44% it was a week or more**

53%
paid the ransom

60%
of these recovered their data

40%
didn't get their data back despite paying

Collaboration tools

99%
are using collaboration tools like Slack or Teams

72%
concerned about having an archived business record of conversations from these tools

Is Cyber Resilience Keeping Up with the New Dangers?

41%
have a cyber resilience strategy in place

85%
of companies were hurt by their lack of cyber preparedness
(up from 58% in 2020)

98%
have either deployed, were in the process, or looking to roll out various email security systems

6/10
Fewer than 6 of 10 currently have safeguards in place

12%
have no email security system at all

37%
are using AI and machine learning to bolster their email defences

Microsoft 365

57%
experienced a Microsoft 365 email outage in the last year

87%
of Microsoft 365 users think their companies need additional email security

88%
hold M365 email security in high regard

67%
also agree that there is room for improvement

Cybersecurity Awareness Training: More Critical Than Ever

1/3
provide ongoing cyber awareness training

74%
believe that risky employee behaviour is putting their company at risk

72%
have been hit by an attack that spread from a compromised user to other employees

46%
train once a quarter or even less frequently

A New Urgency for Online Brand Protection

38%
saw an increase in brand impersonation via counterfeit websites

47%
had a rise in malicious email spoofing

99%
concerned if bad actors spoofed their company's email domain
(Versus 78% in 2020)

7
the average number of attempts to clone websites or create lookalike web domains

94%
would be concerned if a counterfeit website misappropriated their company's brand
(Compared to 84% in 2020)

96%
either use or have near-term plans to use a brand protection service

88%
have already deployed such a service

86% of respondents indicated that their companies are:

30%
already making use of DMARC

21%
in the process of implementing the protocol

35%
plan to do so over the next 12 months

Securing the Enterprise in the COVID world

The State of Email Security

GET THE REPORT