mimecast

Confronting the
NEW WAVE OF
CYBERATTACKS

The State of Email Security 2022

KEY
FINDINGS

Over the past 12 months

3 out of 4 companies received an increased number of email-based threats.

Email usage rose at **8 out of 10** companies

To counter brand spoofing, **89%** of companies are making use of DMARC or plan to do so over the next 12 months.

52%

Said cyberattacks are growing increasingly sophisticated.

More than **8 out of 10** respondents believe their company is at risk due to inadvertent data leaks by careless or negligent employees.

96% of companies either have a cyber resilience strategy or are actively planning to put one in place.

80% of companies are bracing for the fallout from an email-borne attack.

When faced with a ransomware attack, **64%** of companies paid the ransom, yet nearly 4 out of 10 of them failed to recover their data.

On average, **14%** of IT budgets are allocated for cyber resilience.

95%

of respondents say their cyber resilience has been impaired by insufficient funding.

Among Microsoft 365 email users, **79%** experienced an outage during the past year.

96% of companies have been the target of an email-related phishing attempt.

Only **23%** of companies provide cyber awareness training to their employees on an ongoing basis, but **87%** offer it at least once a quarter.

75% of companies were hurt by a ransomware attack, up from **61%**

61%
2020

75%
2021

98% of companies are either using or plan to use a brand protection service this year.

Confronting the
NEW WAVE OF
CYBERATTACKS

The State of Email Security 2022

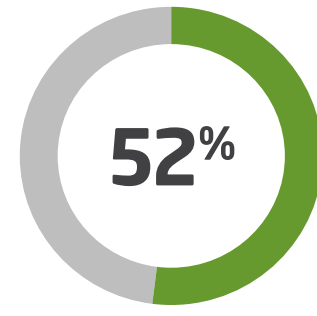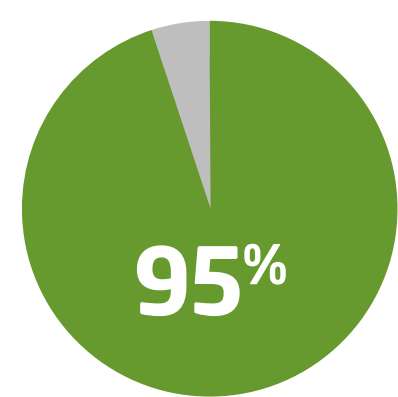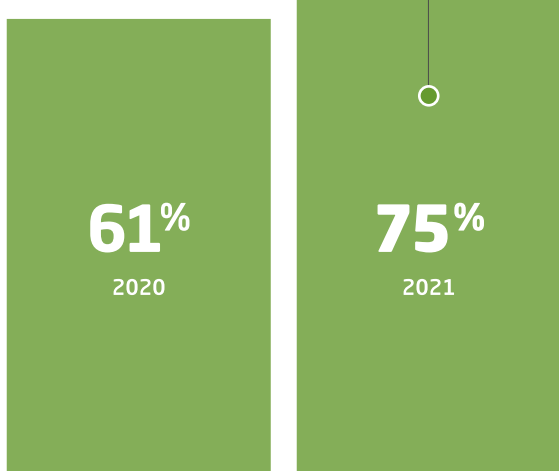PART FIVE:

Security Awareness Training: AN ACHILLES HEEL

Confronting the NEW WAVE OF CYBERATTACKS

GET THE REPORT