UAE respondents are more concerned about various email security challenges, compared to most other countries:

Over the past 12 months

Over two thirds of companies are receiving an increased number of email-based threats.

KEY FINDINGS IN UNITED ARAB EMIRATES

84% of companies have been the target of an email-related phishing attempt.

98% of companies are making use of some combination of artificial intelligence and machine learning.

46% of respondents report a decrease in phishing attacks with 30% saying the decrease was significant. This is possibly because criminals have moved to other, more targeted methods:

- 54% reported an increase in business email compromise
- 50% experienced an increase in internal threats or data leaks initiated by malicious insiders
- 60% cited an increase in spoofed web domains/sites

100% of respondents either have a cyber resilience strategy or are actively planning to put one in place.

84% of companies are using or plan to use a brand protection service this year.

46% are receiving an increased number of email-based threats.

100% of companies either have a system to monitor and protect against email-borne threats or are actively planning to roll one out.

Over two thirds of companies are receiving an increased number of email-based threats.

KEY FINDINGS IN UNITED ARAB EMIRATES

100% of companies expect high levels of changes in their organization from government mandates for cyber resilience:

- Improvements in level of overall cybersecurity in their business - 42%
- Increase in financial cost to their business - 42%
- Decrease in risk of cyberattacks impacting their business - 34%
- Care that business leaders show in relation to improving cybersecurity - 32%

94% of respondents say their cyber resilience has been impaired by insufficient funding, with 50% citing lack of investment in cybersecurity training for existing staff as the biggest setback.

Respondents said the main benefits of implementing AI and ML include:

- 92% feel that additional safeguards are needed for Microsoft 365
- 76% of companies have decreased their exposure to brand spoofing

46% of respondents report a decrease in phishing attacks with 30% saying the decrease was significant. This is possibly because criminals have moved to other, more targeted methods:

- 54% reported an increase in business email compromise
- 50% experienced an increase in internal threats or data leaks initiated by malicious insiders
- 60% cited an increase in spoofed web domains/sites

76% of companies have been the target of an email-related phishing attempt.

84% of companies are using or plan to use a brand protection service this year.

46% are receiving an increased number of email-based threats.

100% of companies either have a cyber resilience strategy or are actively planning to put one in place.

84% of companies are making use of some combination of artificial intelligence and machine learning.

46% of respondents report a decrease in phishing attacks with 30% saying the decrease was significant. This is possibly because criminals have moved to other, more targeted methods:

- 54% reported an increase in business email compromise
- 50% experienced an increase in internal threats or data leaks initiated by malicious insiders
- 60% cited an increase in spoofed web domains/sites

This regular training appears to be translating into some positive behaviour:

- Only 66% were concerned about employees oversharing company information on social media
- 62% were concerned about the use of collaboration tools
- Over 1 in 10 said there was no risk at all to employees using personal email

100% of respondents either have a cyber resilience strategy or are actively planning to put one in place.

84% of companies have been the target of an email-related phishing attempt.

94% of companies are using or plan to use a brand protection service this year.

46% are receiving an increased number of email-based threats.

100% of companies either have a cyber resilience strategy or are actively planning to put one in place.

84% of companies are making use of some combination of artificial intelligence and machine learning.

46% of respondents report a decrease in phishing attacks with 30% saying the decrease was significant. This is possibly because criminals have moved to other, more targeted methods:

- 54% reported an increase in business email compromise
- 50% experienced an increase in internal threats or data leaks initiated by malicious insiders
- 60% cited an increase in spoofed web domains/sites

76% of companies have been the target of an email-related phishing attempt.

84% of companies are using or plan to use a brand protection service this year.

46% are receiving an increased number of email-based threats.

100% of companies either have a cyber resilience strategy or are actively planning to put one in place.

84% of companies are making use of some combination of artificial intelligence and machine learning.

46% of respondents report a decrease in phishing attacks with 30% saying the decrease was significant. This is possibly because criminals have moved to other, more targeted methods:

- 54% reported an increase in business email compromise
- 50% experienced an increase in internal threats or data leaks initiated by malicious insiders
- 60% cited an increase in spoofed web domains/sites

This regular training appears to be translating into some positive behaviour:

- Only 66% were concerned about employees oversharing company information on social media
- 62% were concerned about the use of collaboration tools
- Over 1 in 10 said there was no risk at all to employees using personal email

100% of respondents either have a cyber resilience strategy or are actively planning to put one in place.

84% of companies have been the target of an email-related phishing attempt.

94% of companies are using or plan to use a brand protection service this year.

46% are receiving an increased number of email-based threats.

100% of companies either have a cyber resilience strategy or are actively planning to put one in place.

84% of companies are making use of some combination of artificial intelligence and machine learning.

46% of respondents report a decrease in phishing attacks with 30% saying the decrease was significant. This is possibly because criminals have moved to other, more targeted methods:

- 54% reported an increase in business email compromise
- 50% experienced an increase in internal threats or data leaks initiated by malicious insiders
- 60% cited an increase in spoofed web domains/sites

76% of companies have been the target of an email-related phishing attempt.

84% of companies are using or plan to use a brand protection service this year.

46% are receiving an increased number of email-based threats.

100% of companies either have a cyber resilience strategy or are actively planning to put one in place.

84% of companies are making use of some combination of artificial intelligence and machine learning.

46% of respondents report a decrease in phishing attacks with 30% saying the decrease was significant. This is possibly because criminals have moved to other, more targeted methods:

- 54% reported an increase in business email compromise
- 50% experienced an increase in internal threats or data leaks initiated by malicious insiders
- 60% cited an increase in spoofed web domains/sites

This regular training appears to be translating into some positive behaviour:

- Only 66% were concerned about employees oversharing company information on social media
- 62% were concerned about the use of collaboration tools
- Over 1 in 10 said there was no risk at all to employees using personal email

100% of respondents either have a cyber resilience strategy or are actively planning to put one in place.

84% of companies have been the target of an email-related phishing attempt.

94% of companies are using or plan to use a brand protection service this year.

46% are receiving an increased number of email-based threats.

100% of companies either have a cyber resilience strategy or are actively planning to put one in place.