Email attacks, and why they aren't decreasing

- 67% of organisations believe an email-based attack is likely or likely to happen in the next year
- 62% of organisations have experienced a phishing attack in the past 12 months
- 67% of organisations anticipate an increase in web or email spoofing and brand exploitation as the leading threat

Key findings over the previous 12 months

- Email security is leading to:
  - 48% of organisations have increased resilience preparedness
  - 48% of organisations have increased resilience preparedness
  - 56% of organisations have improved their incident response processes

How Security Awareness Training closes the understanding gap

- 100% of organisations offer some training at varying frequencies and formats:
  - 68% online tests
  - 49% online tests
  - 6% group training
  - 5% printed tips
  - 4% offer training monthly or more
  - 16% offer training monthly or more

The new mandate: online brand protection

- 99% of training was developed in-house
- 37% of organisations have a dedicated budget for online brand protection
- 68% of organisations anticipate an increase in web or email spoofing and brand exploitation as the leading threat

Is cyber resilience improving?

- 79% of organisations have a cyber resilience strategy or actively implement a cyber resilience strategy
- 96% of organisations have a dedicated budget for cyber resilience
- 99% of organisations have a resilience strategy in place

Email Security 2020

The State of

Is cyber resilience improving?

The new mandate: online brand protection

Email attacks, and why they aren't decreasing

Key findings over the previous 12 months

How Security Awareness Training closes the understanding gap

The new mandate: online brand protection

Is cyber resilience improving?

What's included in their cyber resilience strategies?

Email attacks, and why they aren't decreasing

Key findings over the previous 12 months

How Security Awareness Training closes the understanding gap

The new mandate: online brand protection

Is cyber resilience improving?

What's included in their cyber resilience strategies?