The Threat's in the Email

Phishing and other email-borne threats continue to be the major cybersecurity dangers

THE IMPACT OF THREATS

$2.4B

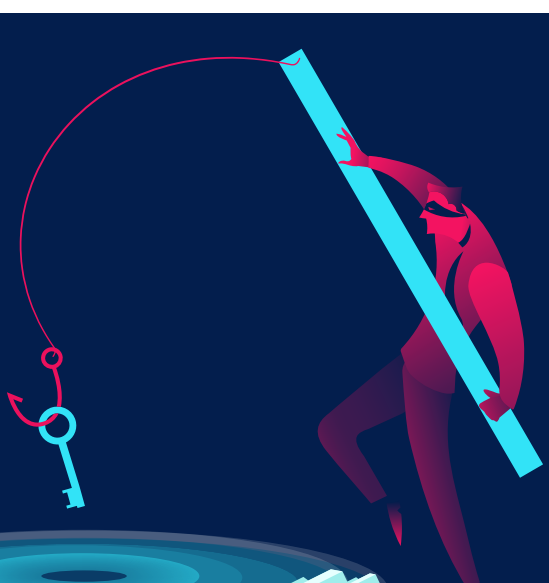
What's the cost of inaction?

The FBI reported that business email compromises (BEC) alone led to losses of $2.4 billion in 2021. Over 320,000 Phishing/Email attacks were reported to the FBI last year.

90%

Nearly all attacks start with an email

Over HALF of all small to midsize businesses (SMBs) fell victim to cyberattack, 90 percent of them began with a phishing email (2020 Verizon DBIR).



150%

A year of living dangerously

Email-based malware attacks surged by over 150% between 2020 and 2021

200+

Detection deceleration

The average time to identify a breach climbed to over 200 days

As the cost and impact of threats continues to grow, organizations of all sizes must find new ways of stopping them before they grow from nuisance to liability

THE PROBLEMS WE FOUND

82 SECONDS

Time is of the essence:

The average time-to-click on a phishing email is only 82 seconds from time of receipt.

Lack of automation strains IT teams

Nearly 3/4 of organizations use ONLY manual processes to review user-reported phishing, limiting IT's capacity to focus on strategic initiatives.

60%

Data breaches are existential threats

60% of businesses fold within six months of data breach or cyberattack.

Secure gateways aren't enough

Millions of malicious messages bypass traditional email defenses such as SEGs every year.

24%

Employee time well-spent?

The amount of their typical 40-hour workweek security analysts spend investigating, detecting, or remediating phishing emails

The security skills shortage is having an impact

Most analysts can handle no more than four phishing threats per day.

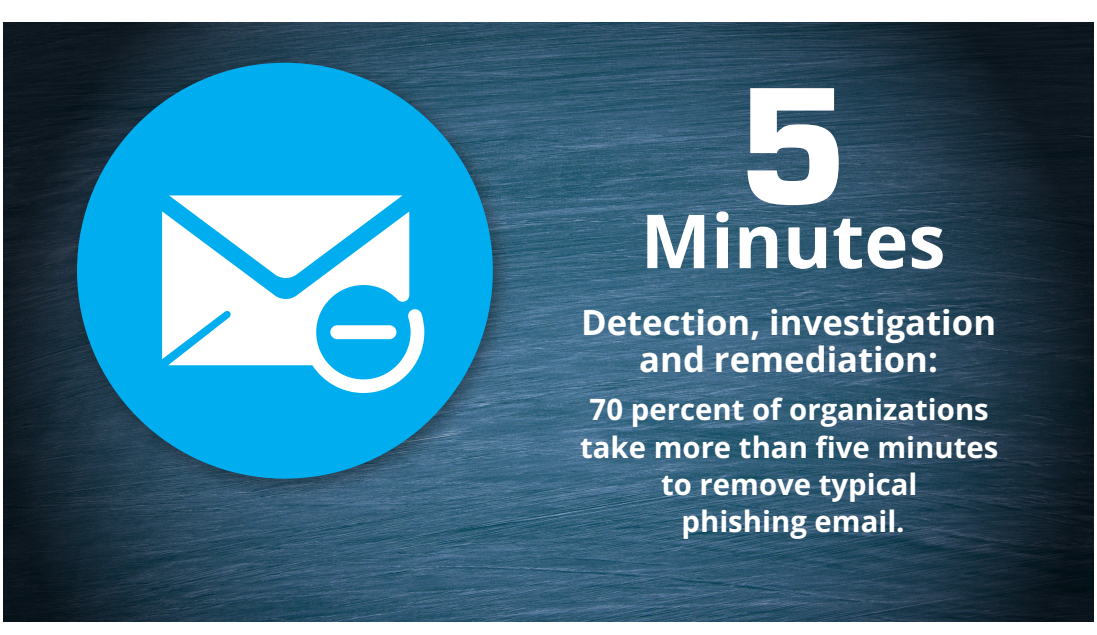
$8900

Bottom line effect of atttacks

The monthly cost of managing phishing attacks for an organization with 5000 users.

What keeps management up at night?

Phishing is the leading concern among decision makers.



As email-based threats grow more sophisticated, no single tool is sufficient to prevent infection and payload detonation on its own. Enterprises must take a multi-faceted approach to preventing data loss or exfiltration.

THE SOLUTION!

How does GoSecure Titan® Inbox Detection & Response Work?

1. Employee notices suspicious email and clicks the GoSecure Titan IDR button to begin the submission process.
2. Email is automatically quarantined and routed through the GoSecure Active Response Center.
3. GoSecure automated machine learning engines investigates the suspicious email.
4. Human security experts conduct a further review on inconclusive messages through a multi-faceted analysis.
5. Within minutes a status message is returned, either the message is verified or removed.
6. Real-time reporting gives the in-house security team clear visibility into the incident and its resolution.

Obtain the full ebook: Stopping Email Attacks with Multi-Layered Security at https://www.gosecure.net

GoSecure is a recognized cybersecurity leader, delivering innovative managed security solutions and expert advisory services. GoSecure Titan® managed security solutions deliver multi-vector protection to counter modern cyber threats through a complete suite of offerings that extend the capabilities of our customers' in-house teams. GoSecure Titan Managed Detection & Response (MDR) offers a best in class mean-time-to-respond, with comprehensive coverage across customers' networks, endpoints and inboxes. For over 10 years, GoSecure has been helping customers better understand their security gaps, improve organizational risk and enhance security posture through advisory services provided by one of the most trusted and skilled teams in the industry. To learn more, please visit: https://www.gosecure.net.

GoSecure gosecure.net | 855-893-5428