The real (and rising) risk of phishing

The causes and costs of phishing attacks, and how to defend your human layer

egress

Inside the report

Executive summary

People are your last line of defense against phishing

It's time to secure your human layer

Phishing continues to dominate the cybersecurity agenda.

Attacks are constantly evolving, and employees and organizations fall victim to sophisticated threats daily.

While organizations have rapidly matured security and controls for their network and application layers, their human layers – their people – urgently require better defenses to detect and mitigate email-borne threats.

This report analyzes the key findings from our recent Insider Data Breach Survey to show the real – and rising – risk of phishing. It also examines the primary causes behind phishing attacks, incident detection and reporting mechanisms, and the human cost this is taking. As successful phishing attacks are never without victims and consequences, we've also featured quotes from IT leaders and employees that share their real-world experiences when falling for and remediating phishing attacks.

With organizations needing to layer their defenses against phishing attacks, we also show how Egress Defend can be deployed directly into your employees' inboxes to ensure they're protected against the most convincing (and therefore damaging) attacks.

What's the risk of phishing?

There's no smoke without fire. The high-level concerns about phishing are driven by the proliferation of breaches taking place and the belief that it's more difficult to prevent these incidents than it ever has been before.

73% of IT leaders report their organization was the victim of a successful phishing attack in the last 12 months, and 53% correlate an increase in phishing-related security incidents with mass remote working.

Half of IT leaders believe ongoing remote and hybrid work will continue to make it more difficult to prevent these incidents in future. The use of mobile devices to facilitate email communication are held partly responsible, with 50% again believing they make it more difficult to effectively prevent security threats.

> Confidential data on a database was compromised after a staff member opened a phishing email and entered personal details. This caused extra strain on the IT department to secure the database and clear the bug from the system.
>
> ANONYMOUS IT LEADER

A phishing pandemic

The COVID-19 pandemic and mass remote work has provided perfect conditions for attackers.

New subject matter: Familiarity with phishing attack templates and topics helps employees recognize and avoid recurring and similar attacks. The pandemic has continually presented a diverse range of new subject matter for cybercriminals to leverage, from coronavirus treatment, testing and vaccines to changing working environments, such as missed deliveries for remote workers and updates to HR policies.

Widespread adoption of new technologies: There have been clear frontrunners in the technologies adopted during the pandemic, meaning attacks based around popular platforms are more likely to resonate with their targets. Additionally, employees using newer systems will also be less likely to detect a well-crafted attack than they would one exploiting a brand or platform they're familiar with.

Workplace disruption and increased email communication: Increased email use means employees are less likely to raise their eyebrows when requests and updates land in their inboxes. Plus, remote work makes it more complicated to query any potential red flags and borderline concerns, whether that's speaking with the Security team directly or simply a quiet sense check with a colleague.

A climate of concern: Socially engineered phishing emails frequently rely on fear to galvanize a response. The increased baseline of anxiety across the general population makes it easier for cybercriminals to manipulate their targets. Added to this, people continue to feel under pressure while working remotely, and distracted and stressed employees are more likely to make mistakes.

Email: An open door for attackers

Email remains the most at-risk vector for data breaches in the eyes of 64% of IT leaders. For phishing attacks specifically, it's one of the easiest ways for cybercriminals to breach your defenses.

Everyone has an email account, and it's not difficult to obtain or correctly predict corporate email addresses. Many organizations display contact details for various team members on their website and follow a similar pattern for all employees (such as firstname.lastname@company.com). Use of corporate email addresses to sign up for social media channels and other online accounts means data dumps from security breaches of these platforms or from screen scraping are available for purchase (and for free!) on the dark web.

It's also far easier to hack a human than it is to find and exploit a technical weakness. Security focus over the last decade has centered on improving technical defenses to the network and application layers, so cybercriminals are now relentlessly targeting the area of greatest vulnerability and, for them, opportunity: the human layer.

> **Phishing emails still comprise a large portion of the world's yearly slate of devastating data breaches.**
>
> ANONYMOUS IT LEADER

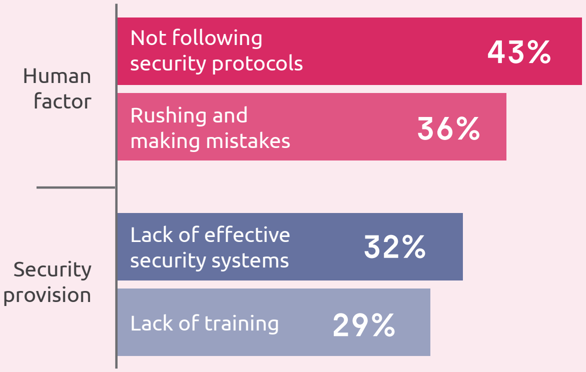
How do organizations perceive and respond to these threats?

What – or who – is to blame for successful phishing attacks?

According to IT leaders, it's people making the wrong choices or not paying enough attention.

Phishing attacks rely on insiders to let them in – and IT leaders know it! 78% believe people are the main contributing factor in phishing-related security incidents, versus 61% who say lack of security systems and training would play a key role.

What are the top ways an employee would fall victim to a phishing attack within your organization?

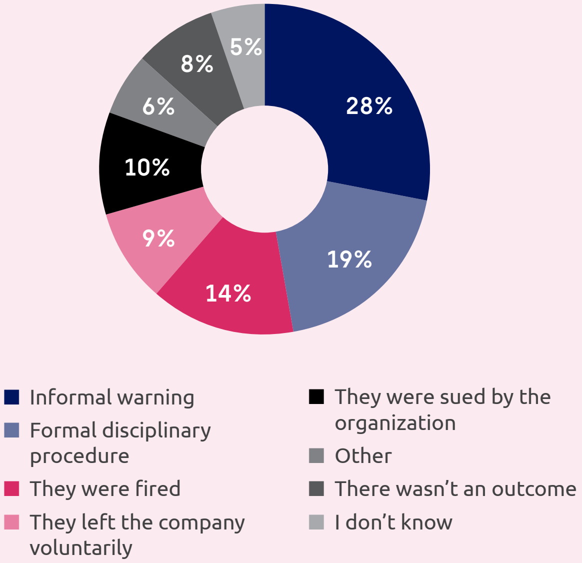


The human cost of phishing

At 87% of organizations, the individual at the center of a phishing attack experienced negative repercussions following a breach.

Phishing attacks are more than just mistakes. They're clever exploitation by cybercriminals whose one job is to deceive their victims. There's a clear perpetrator and victim, yet employees – the victims – are carrying cost for these attacks in almost every organization.

What was the most common outcome for the employee(s) who fell victim to a phishing attack in the last 12 months?

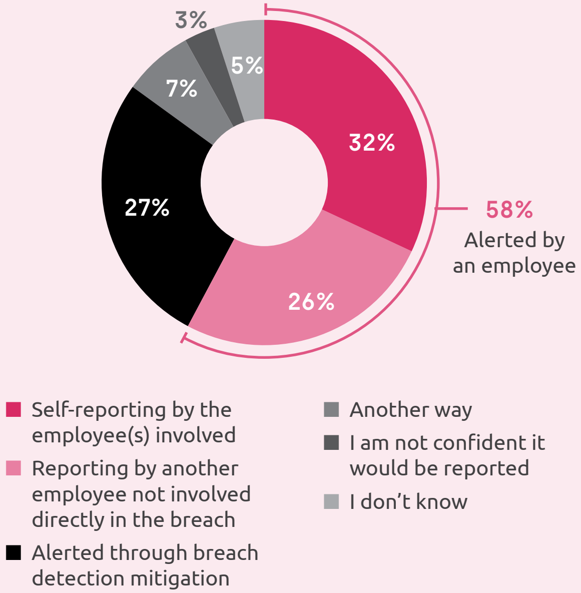


Heavy reliance on self-reporting

Despite the negative outcomes involved, IT leaders primarily rely on employees to report phishing-related security incidents.

However, negative outcomes can act as a strong deterrent for reporting, leaving employees dragging their heels if they choose to report at all.

IT leaders show how they/their teams would be notified about phishing-related security incidents



Defending your human layer from phishing attacks

People are organizations' last line of defense against phishing. They are expected to act as both detection and reporting mechanisms in the face of increasingly sophisticated and relentless targeted attacks. And as the rising tide of breaches shows: it's not working.

It's time to implement intelligent security to defend the human layer where employees need it most: directly in their inboxes.

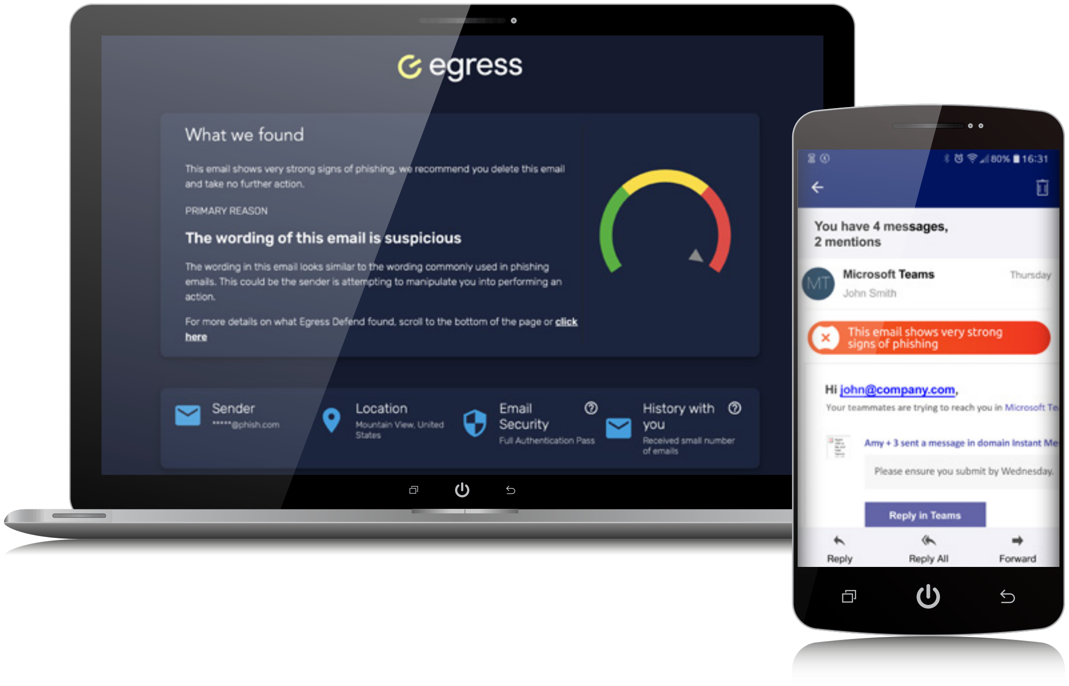
> **Unfortunately, some of the attacks are now so sophisticated that even very experienced and conscientious employees are occasionally duped.**
>
> ANONYMOUS IT LEADER

Egress Defend:
Zero-trust anti-phishing technology

Egress Defend is the only solution globally to operate on a zero-trust model for phishing detection, analyzing the context and content of every inbound email before it is delivered to employees' inboxes.

Deployed directly into Microsoft Outlook, Defend uses the latest in machine learning and natural language processing (NLP) technology to detect all types of phishing attacks, including the most convincing and therefore damaging ones, such as:

- Impersonation attempts and CEO fraud via spoofed domains
- Attacks that originate from compromised accounts on authenticated domains
- Attacks that utilize open-source intelligence (OSINT)
- "Payload-less" attacks that don't contain a malicious attachment or link but request an action be carried out, such a payment transfer
- Hyperlinks that are weaponized by cybercriminals post-delivery



What we found

This email shows very strong signs of phishing, we recommend you delete this email and take no further action.

PRIMARY REASON

The wording of this email is suspicious

The wording in this email looks similar to the wording commonly used in phishing emails. This could be the sender is attempting to manipulate you into performing an action.

For more details on what Egress Defend found, scroll to the bottom of the page or **click here**

Sender: *****@phish.com

Location: Mountain View, United States

Email Security: Full Authentication Pass

History with you: Received small number of emails

You have 4 messages, 2 mentions

Microsoft Teams — John Smith — Thursday

This email shows very strong signs of phishing

Hi john@company.com,

Your teammates are trying to reach you in Microsoft Te

Amy + 3 sent a message in domain Instant Me

Please ensure you submit by Wednesday.

Defend is also designed to partner with end-users for real-time active education. Using a traffic-light warning system and insight summaries, the solution alerts users to risk and provides "tooltip" explanations about phishing detection and why actions (such as clicking on a malicious link) are blocked.

The solution also offers administrators with comprehensive analytics and a real-time threat feed that spans the entire organization, so you can effectively monitor your phishing risk profile in real time.

Book your Defend demo now

Learn more about Defend

About Egress

Our mission is to eliminate the most complex cybersecurity challenge every organization faces: insider risk. We understand that people get hacked, make mistakes, and break the rules. To prevent these human-activated breaches, we have built the only Human Layer Security platform that defends against inbound and outbound threats. Using patented contextual machine learning we detect and prevent abnormal human behavior such as misdirected emails, data exfiltration and targeted spear-phishing attacks.

Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York and Boston.

Methodology

The surveys for the Insider Data Breach Survey 2021 were carried out independently by Arlington Research. 500 IT leaders (defined as someone who has decision-making power over IT solutions within a business) and 3,000 employees were surveyed. Respondents were equally split across the healthcare, finance, legal and 'other' industries, and split 50/50 across the US and the UK.

www.egress.com | info@egress.com | @EgressSoftware

egress