# A New Report Unveils the Most Vulnerable Sectors and Departments to Phishing Attacks

**Wednesday 9 September, 2020**

**Cyber attacks cause great harm to the business world due to their evolving nature and it is expected that cyber attacks will cost businesses 6 trillion dollars worldwide next year. Keepnet Labs reveals its latest research on the most vulnerable sectors and internal departments affected by cyber attacks.**

**PRESS RELEASE** - While cyber attackers chase down system vulnerabilities and valuable data each passing day, the business world has taken the measures against them. The latest trends and cybersecurity statistics reveal that data from various sources, especially mobile and IoT devices, is targeted and attacked. Organizations face the risk of data loss due to unprotected data and weak cyber security practices.

In the first half of last year, $ 4.1 billion of data records were exposed [1], while the average time needed to detect a leak was 206 days [2]. While the average loss caused by a data leak is estimated at $ 3.92 million[3] for businesses, cyberattacks will create $ 6 trillion[4] in losses globally in the next year.

Keepnet Labs, a UK-based cyber security awareness and anti phishing company has revealed the most vulnerable departments and sectors against phishing attacks. The Keepnet Labs 2020 Phishing Trends Report was generated by a data set of 410 thousand phishing emails, covering a period of one year.

Accordingly, 90% of successful cyber attacks occur through email-based attacks. These cyberattacks use deceptive, deceptive and fraudulent social engineering techniques, especially to bypass various security mechanisms / controls.

**1 out of 8 people share the information requested by attackers**

According to the Report, which identifies the sectors and departments that are most vulnerable to phishing attacks:

- 1 out of 2 employees opens and reads phishing emails.
- 1 out of 3 employees clicks links or opens file attachments in phishing emails (which may cause silent installation of malware / ransomware).
- 1 out of every 8 employees shares the information requested in phishing emails.

Moreover, the sectors and departments most vulnerable to cyber attacks are identified in the Report.

**Sectors most vulnerable to cyber attacks**

Top 5 sectors with the highest click rates on malicious links in phishing emails:

- Consulting (63%)
- Clothing and Accessories (48%)
- Education (47%)
- Technology (40%)
- Holdings / Conglomerates (32.37%)

**Sectors with the highest rates of data sharing:**

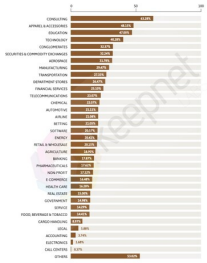
- Clothing and Accessories (43%)
- Consulting (30%)
- Securities and Stock Exchange (23%)
- Education (22%)

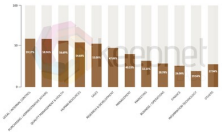
**Corporate departments most affected by cyber attacks**

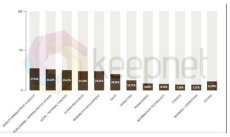
The top three departments with the highest rates of clicking fake links in phishing emails:

- Law / Audit / Internal Control (59%)
- Procurement / Administrative Affairs (58%)

## Media:







## Related Sectors:

Business & Finance :: Computing & Telecoms ::

## Related Keywords:

Keepnet :: Cyber Security :: Cyber Attack :: Phishing :: Report ::

## Scan Me:

- Quality Management / Health (56%)

While the findings reveal that these departments have not changed according to last year's statistics, the Report concludes that most of the sensitive information needed by cybercriminals is accessible via users working in these vulnerable units. This in turn poses a serious threat to their respective organizations, because employees with such privileged access to this prized information are the key people in those organisations who motivate the hackers to infiltrate organizations and execute their intended, malicious campaigns.

**The top three departments with the highest rates of sharing data:**

- Quality Management / Health (27%)
- Procurement / Administrative Affairs (26%)
- Legal / Audit / Internal Control (25%)

These statistics reveal that certain departments are more inclined to share sensitive information compared to others, and considering their position, they should be much more careful against cyber attacks.

The Keepnet Labs 2020 Phishing Trends Report guides organizations in their cyber security and awareness efforts by identifying the most vulnerable departments and sectors.

You can download the Report **here**.

**

Resources**:** [1] RiskBased [2] IBM [3] Security Intelligence [4] C. Ventures

**About Keepnet Labs**

Keepnet Labs protects businesses throughout the full lifecycle of email-based cyber-attacks. Keepnet has developed a full spectrum suite of cyber-security defence, threat monitoring, security management and user awareness products that encapsulate an integrated approach to people, processes and technology thus reducing the threat in all areas of cyber risk.

The company is committed to continuous innovation and expansion of our suite of security products in order to meet the needs of a dynamic and rapidly growing networked population in a constantly evolving cyber-threat environment.

Keepnet’s cyber defence strategy adopts three holistic elements: people, process, and technology:

- People: Keepnet focuses on the "human factor”, using engaging, structured, content to raise cyber awareness and engender “active defence” behaviours.
- Process: Keepnet supports the development and management of user security awareness plans, monitor user compliance and Key Performance Indicators and embed cybersecurity as an intrinsic part of the corporate culture.
- Technology: Keepnet scans and isolates malicious attachments and email content and provides system administrators with “one-click” management across the enterprise.

Keepnet’s internal corporate strategy creates a stimulating and innovative environment where the Keepnet team has the opportunity to continually enhance their skills and creativity while contributing to growth.

Keepnet Labs solution delivers a full-spectrum approach to mitigating phishing risk by:

- Analysis of phishing attacks using Artificial Intelligence and third-party integration for identification, notification and deletion of suspicious emails;
- Safely simulating phishing attacks using a broad range of real-world models;
- Automating malicious email management through “one-click” removal;
- Proving education modules with third-party training platform integration;
- Supporting user training and recording of training outcomes and compliance;
- Delivering integrated cyber-intelligence reporting; and
- Cloud and on-premise implementation options.

Keepnet’s flexible technology implementation model means that it can scale from the smallest SME to the largest corporate organisation using both cloud and on-premise implementations.

The “as a service” model is particularly attractive to smaller organisations without in-house security capability as Keepnet Labs provide both the platform and the operational management of alerting, user training management, phishing simulations and security reporting.

For larger organisations who may choose an on-premise implementation, Keepnet provides a full support capability including heuristic and threat intelligence-based updates to reflect the dynamic nature of the threat perimeter.

Keepnet Labs improves overall organisational security posture and mitigate cyber-risk by;

- Real-time analysis and management of email-borne threats;
- Threat simulation designed to test the organisations' security posture;
- The availability of timely threat intelligence;
- Via realistic, but safe, phishing simulation; and
- Supporting security awareness training programmes.

## Company Contact:

**Keepnet Labs**

E. aytun@linkmedya.com
W. https://keepnetlabs.com

View Online

**Additional Assets:**

**Newsroom:** Visit our Newsroom for all the latest stories:
**https://www.linkmedya.pressat.co.uk**