TitanHQ™

TitanHQ 2023 Automated Phishing Simulation Success Report

Introduction

Cyber-attacks that are human-centered have changed the way that cybercriminals target our businesses and employees. This advancement in activity and scope brought about by manipulating people into doing a cybercriminal's bidding, like clicking a phishing link, has led to massive growth in cybercrime. Cybercrimes are an international, organized, and sophisticated movement expected to cost global businesses around **$10.5 trillion by 2027.**[1]

Hackers don't need to hack if they can walk through the corporate network's digital door using legitimate login credentials. The success of phishing has facilitated the modification of attack techniques from brute force hacking to unauthorized access. In 2022, almost one-third (30%) of adults in the world had encountered phishing, and 35% had experienced an SMS or mobile scam[2].

The 'human in the machine' is the leverage behind these neo-hackers. Human-focused attacks rely on security behaviors that can be manipulated to commit nefarious acts that benefit the attacker unwittingly. The net result is that cybercriminals increasingly target employees for login credentials and other data to make hacking and scamming much easier.

Source[1] - Cybersecurity ventures

Source[2] - Statistica

The Persistent and Evolving Nature of Phishing

Email phishing and SMShing, as attack vectors, have evolved in parallel with the tools that detect phishing attacks. Phishing detection is a complex, multi-layered problem, solved only by the most advanced tools coupled with security awareness rolled out across the organization.

The persistent and evolving nature of phishing has been captured in an EU's ENISA (European Union Agency for Cybersecurity) report. The researchers identify phishing as a persistently popular vector behind many cyber-attacks.[3] However, ENISA cautions, "We see new forms of phishing arising, such as spear-phishing, whaling, smishing, and vishing." This continuous evolution of the phisher's toolkit has created a war of attrition that, in recent years, has seen phishing tactics become ever more sophisticated; new technologies are incorporated into the phisher's portfolio, including generative AI. As a result, IBM has identified phishing as the most used attack type for all types of security incidents.[4]

Phishers and Smishing fraudsters want to gain access to a corporate network as easily as possible and with the chance of detection minimized. As a result, login credentials are a primary focus; almost half (49%) of all phishing involves credential theft, according to the Verizon Data Breach Investigations Report (DBIR)).[5] A simple slip-up by an employee can lead to devastating costs for a business. The IBM Data Breach Investigation report found that the average price of a breach in 2023 is $4.45 million.[6]

This changing phishing landscape leaves organizations on the back foot in this war of attrition. Fighting fire with fire means that organizations must use layers of protection to catch these most sophisticated cyber-attacks. As people are the focus of these hackers, to shift the power balance of employee vs. cybercriminal, an organization must turn to security awareness training and phishing simulations that are powered by automation.

Source[3] - ENISA

Source[4] - IBM research

Source[5] - Verizon

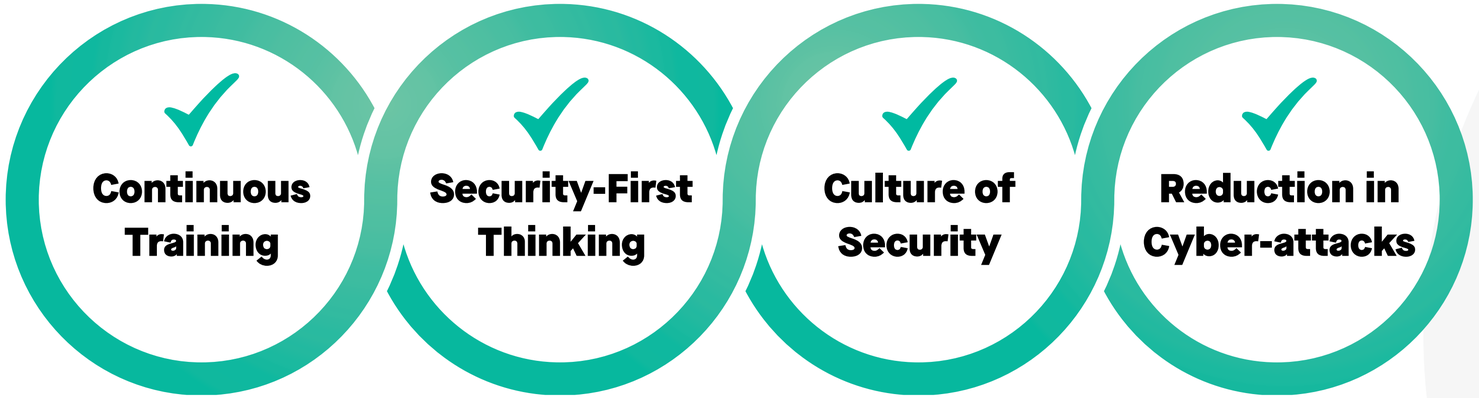
Source[6] - IBM

Source[7] - Cloud Community

Security Training Automation is Essential

Automation of cybersecurity training sessions and phishing simulation campaigns is essential in the cybersecurity strategy of any organization and sector. Humans make mistakes, and cybercriminals manipulate people. With 79% of employees engaging in risky security behaviors, ensuring that security awareness training is carried out regularly is vital to the success of the training.[7]

Security awareness must be designed to work with people and behavior. Automated security awareness training ensures that regular and effective employee training tailored to an individual's interaction with phishing emails is automatically deployed. The automation element is part of a broader design remit of an effective security training platform that also uses behavior-led, AI-driven, simulated phishing campaigns; this powerful combination helps change behavior and empowers employees with the knowledge to prevent social engineering and phishing attacks



Testing Security Awareness and Phishing Vulnerability

Metrics are essential to test the success of automated, behavior-led security awareness training and phishing simulations. If an employee is tricked into clicking a phishing link or downloading an infected attachment, your organization must be aware of this. This employee susceptibility metric indicates the effectiveness of the phishing simulations and training and can provide insight into how to tailor the automated sessions to improve results.

Phish Vulnerable Percentage (PVP) and SMSish Prone Risk (SPR)

The metric is captured as a Phish Vulnerable Percentage (PVP) and SMSish Prone Risk (SPR), the latter being associated with mobile-based phishing attacks. In a recent study, TitanHQ captured and analyzed these metrics to analyze the effectiveness of automated phishing and SMShing training.

This white paper examines how security awareness training was performed during the study based on PVP results by geographic region, organization size, and sector. The data provides an insight into the effect of automated security awareness training and an understanding of the variation across user, industry, and region types.

97%

of organizations around the world have experienced an increase in email phishing attacks.

Source: www.cybertalk.org

Phishing Vulnerability and Industry Risk

All industry sectors face cyber-attacks, and all have phishing campaigns waged against their industry. For example, financial services were the most targeted sector by phishing in Q4 2022[8]. Knowing the **Phish Vulnerable Percentage (PVP)** and **SMSish Prone Risk (SPR)** for your sector provides intelligence on the susceptibility of an organization's employees to phishing against its peer group. The value of PVP or SPR equates directly to an organization's risk level. A high PVP or SPR means an organization has a higher risk of a successful cyber-attack, such as phishing, focusing on human factors. This information can provide important data for management and at the board level. If your score is lower than the average for your sector, this can provide the evidence needed to request a security budget. **If the score exceeds the sector average, you can show management how well the training is progressing and how this relates to reduced cyber-attack risk.**

PVP and SPR are direct indicators of how effective your security awareness training is and if a security culture is forming in the organization. A culture and ethos where employees across the organization put security first is an essential element when building a 'human firewall.'[9] If cybercriminals attack an organization by targeting its staff, then employees must be aware of how they do this. Using industry PVP and SPR scores as a benchmark can help your organization improve its security culture. A robust security culture leads to a reduced risk of a successful cyber-attack.

This study will look at the PVP and SPR baselines across sectors, sizes, and geographies; with this knowledge, you can look at your baseline using metrics from automated phishing and SMShing simulations to see how you score against this average. To improve your score, you can look at methods and strategies, such as automation, to create tailored and effective phishing simulation campaigns.

79%

of employees engage in risky security behaviors.

PVP & SPR

Phish Vulnerable Percentage (PVP) and SMSish Prone Risk (SPR)

Source[8] - Statisita

Source[9] - TitanHQ blog post

TitanHQ 2023 Automated Phishing Simulation Success Report

Main findings:

- There is a **92%** drop in phishing susceptibility when employees are trained using the automated security awareness training solution SafeTitan.
- Some industries are more prone to phishing than others, with biotechnology at the most significant risk of phishing-related attacks.
- Europe is the most prone, and Australasia is the least prone to phishing.
- Companies under 500 employees are the most susceptible to phishing.
- Focused training is more effective, and automated training platforms that focus attention on the most susceptible employees work best.

Methodology and Data Analysis

Insight into how an organization compares to industry peers regarding security risk is a good indicator of security posture. This foundation stone provides a starting point for building a robust, security-first-minded organization and reducing the threat of cyber-attacks. However, to build up a complete picture of phishing risk levels requires data. This data provides the basis for risk remediation, as the metrics are used to measure the effectiveness of a security awareness strategy. The metrics give the baseline from which you can assess your position and security posture and develop an effective security-first strategy.

For this study, TitanHQ aggregated the baseline PVP of over 500 organizations using metrics generated using the SafeTitan platform. This baseline showed an organization's risk level before security awareness training and automated phishing simulations had begun. One year later, after regular phishing simulations and training, PVP data was collected and analyzed to compare against the baseline; this demonstrated if progress or regression had occurred post-security awareness training.

The training program was automated to ensure that regular training was carried out. The SafeTitan solution also ensures that the training is targeted and behavior-driven. **All company data was anonymized before this research was conducted.**

Study Methodology: 2023

Each participant organization used SafeTitan to generate and deploy automated simulated phishing campaigns. These campaigns were targeted and tailored to test out an employee's response to receiving phishing emails or SMShing messages. Metrics were generated by capturing data if an employee clicked on a phishing link or downloaded an infected attachment. The study was split into two parts:

Part one: Baseline Generation

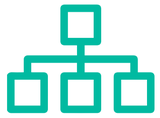
Metrics for employee interaction with simulated phishing messages were captured on day 0 of using an automated phishing simulation platform. This acted as a baseline reading of PVP or SRP.

Part two: PVP Captured After one year of Ongoing Automated Phishing Simulations

A year after the baseline metrics were captured, automated phishing simulations were again deployed as part of the regular and ongoing training. At day 365, any interactions with phishing links, responding to a phishing email/message, or downloading infected attachments were recorded. This gave a second PVP or SRP reading that could be compared to the baseline.

Adjunct Study: PVP by Sector

A further adjunct study was carried out to look at specific industry sectors. This adjunct captured the PVP in 2021 and 2022 to see if an organization's PVP changed over time if they continued to use automated security awareness training and phishing simulations. Once the data was collected, an analysis was performed, and the results were split into the following areas:



Organization size

Geographic region

Sector

$10.5T

Cybercrimes are an international, organized, and sophisticated movement expected to cost global businesses around $10.5 trillion by 2027.

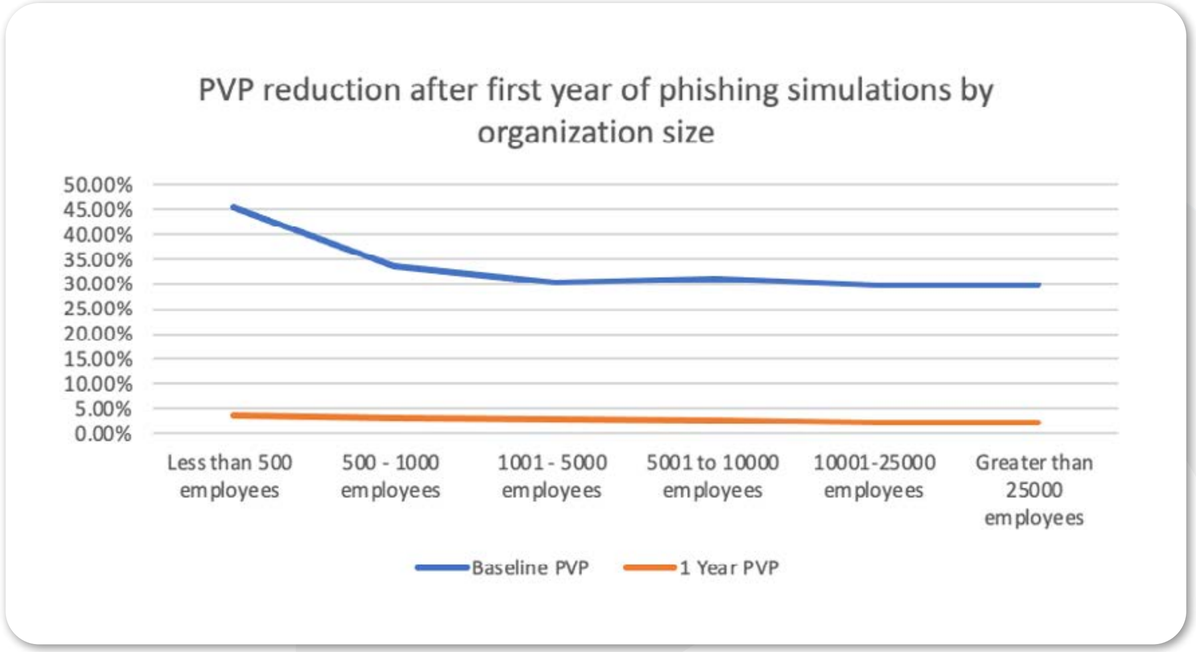
By Organization Size

Phishing knows no bounds when it comes to organization size. Organizations of all sizes are at risk. However, according to research, phishing occurs highest in smaller organizations of less than 250 employees[10]. TitanHQ's results show that the smaller organizations of <500 employees began with a higher baseline, PVP, i.e., employees are more susceptible to phishing before automated phishing simulation exercises were carried out.

Other sized organizations, i.e., >500 employees, all had similar starting points before beginning to test employees using automated simulated phishing campaigns.

Results

Organization Size	Baseline PVP	1 Year PVP	PVP Reduction
Less than 500 employees	45.50%	3.60%	92% ∇
500 - 1000 employees	33.60%	3.20%	90% ∇
1001 - 5000 employees	30.20%	3.00%	90% ∇
5001 to 10,000 employees	31.20%	2.60%	92% ∇
10001-25000 employees	29.90%	2.20%	93% ∇
Greater than 25000 employees	29.80%	2.10%	93% ∇



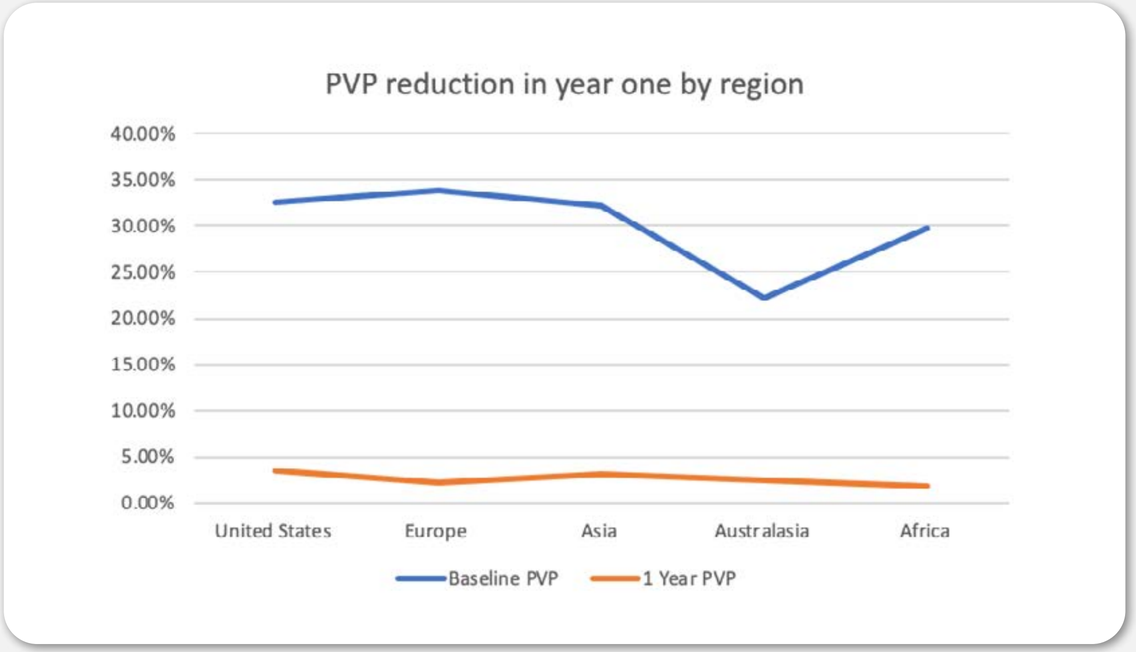
The results graph shows a significant drop in risk related to phishing susceptibility for all sized organizations using the SafeTitan automated phishing simulation platform. **Overall, the average decrease in phishing susceptibility across all sizes of organizations was 92%. This figure is heartening as it strongly indicates that regular, automated phishing simulations work.**

Source[8] - Cybersecurity ventures

By Region

Just as cybercriminals target organizations of all sizes, they also target all geographies. TitanHQ collected data worldwide to determine how effective automated phishing simulations were by region.

Organization Size	Baseline PVP	1 Year PVP	PVP Reduction
United States	32.50%	3.50%	89% ∇
Europe	33.80%	2.20%	93% ∇
Asia	32.20%	3.10%	90% ∇
Australasia	22.20%	2.50%	92% ∇
Africa	29.70%	1.90%	94% ∇



All regions showed a significant drop in susceptibility to phishing after one year of using the SafeTitan automated phishing simulation platform. The results correlated with the percentage decrease in phishing susceptibility by organization size. The best-performing region was Europe, with the worst being the United States. However, all regions vastly improved phishing responses and de-risked the likelihood of a successful phishing attack. The average PPP reduction worldwide was **92%**, which aligns with the average based on organization size.

Worst and Best Phishing Response Rates by Sector

A sector analysis always shines a light on the different risk levels and types of risk in every industry. TitanHQ's research looked at the following industry types:

- Real Estate
- Employment
- Manufacturing
- Transportation
- Air Transportation
- Biotechnology
- Aerospace
- Accommodations
- Auto
- Government

Cybercriminals target all industry sectors. However, some sectors experience specific types of phishing. The Verizon DBIR looks at some industry sectors, including **manufacturing, public administration (Government), and accommodation.**

The manufacturing sector, for example, suffers from social engineering attacks, including phishing. Personal (60%) and Credentials (38%) are the primary data compromised in the sector. Similarly, public administration is plagued by social engineering, with Personal (38%), Other (35%), and Credentials (33%) being compromised. Even the accommodation sector is threatened by phishing and social engineering, with data compromised, including Payment (41%) and Credentials (38%).

IBM

IBM has identified phishing as the most used attack type for all types of security incidents.

Source[11] - FBI

Source[12] - TitanHQ blog post

Source[13] - IBM Research

Source[14] - IC3 Report

Source[15] - Computer Weekly

Phishing is the number one vector, but the implications to an industry vary and include:

Business Email Compromise (BEC)

The FBI calls BEC scams a $50 billion scam, as that is how much these cyber-attacks cost companies annually[11]. BEC and similar extortion-related scams are the basis for over one-quarter of all cyber-attacks. BEC relies on the social engineering of specific staff in a company, typically using spear phishing[12]. Particular sectors are experiencing more BEC scams than others, with 30% of extortion targeting **manufacturing** and 44% of extortion targeting **European companies**[13].

Ransomware

Ransomware attacks and phishing are intrinsically linked. According to a 2022 FBI IC3 report, the topmost targeted sectors for ransomware are **healthcare, government, and manufacturing**[14]**.** The report also identified phishing as one of the top vectors associated with ransomware infection.

Data theft

According to the Verizon Data Breach Investigation Report 2023, phishing causes around 36% of data breaches. Data is an essential element of all cyber-attacks; stolen login credentials, for example, provide the mechanism to walk into a corporate network undetected. Credential theft often involves highly targeted forms of phishing, such as Clone and spear-phishing.

The supply chain and phishing

Compromised supply chains have become a successful part of the cyber-attack chain, with phishing emails targeting vital suppliers, including Salesforce and Microsoft. Research has shown that 92% of organizations have succumbed to a phishing attack via a Microsoft 365 environment.

The Most and Least Phishing-Prone Companies

From 2021 to 2022, TitanHQ continued to find positive reductions in overall PVP across all sectors and regions. Evidence from the data shows that clients are more security aware, with the average overall phishing response falling from **11.03% to 8.78%**. TitanHQ continues to explore how to continue this trend further.

Exploring the data for the organizations across the ten industry sectors was interesting, as it showed apparent differences between organizations with the most minor and most risky phishing behavior. The PVP data, taken over two years, shows that the organization's size may influence specific sectors; smaller companies, for example, may not have a dedicated IT or security team to oversee training. As we found in comparing the baseline PVP versus one-year PVP results, there are dramatic reductions by organizations that implement an automated security awareness strategy. A star sector was **manufacturing**, with a 26% decrease in PVP rates. Again, however, the smaller organization may need help to run effective awareness training. However, automation and delivery via an MSP can counteract this issue.

The **biotechnology** sector has one of the worst PVP scores at 32.33% in 2021. The lowest-scoring sectors include **aerospace, accommodations, auto, and government.** These sectors are the most likely to experience a successful phishing lure. **Accommodations and auto** experienced further increases in their PVP risk scores over the year.

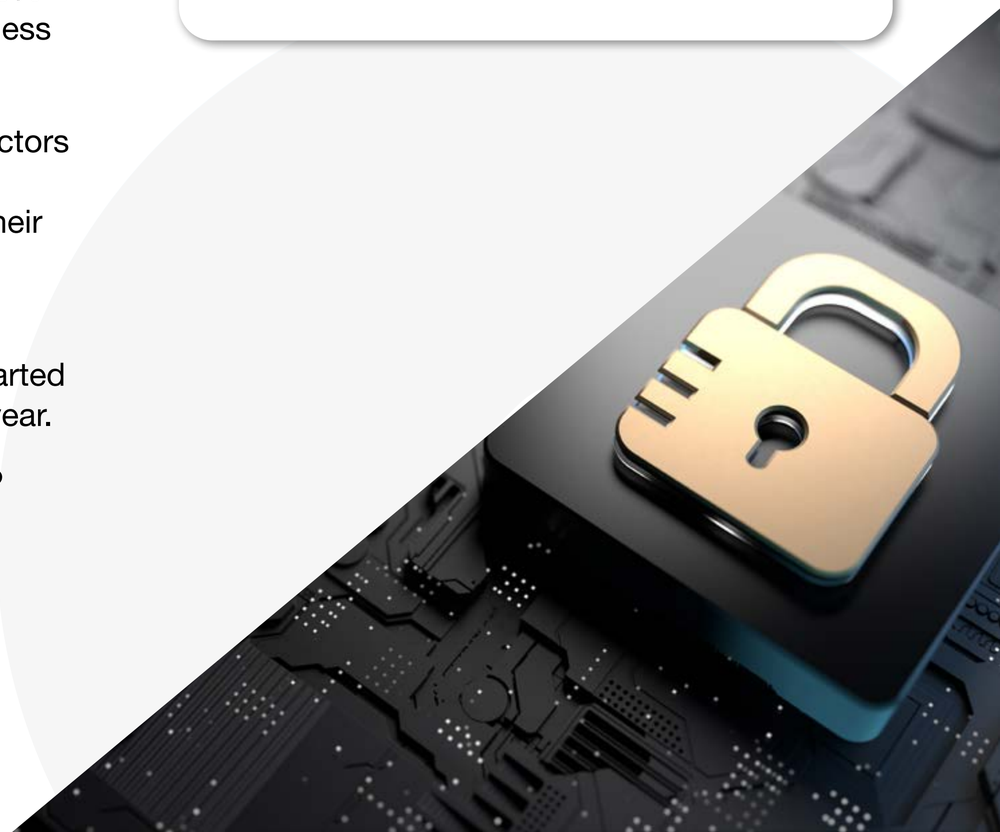
The industries with the lowest PVP scores and lower risk of a successful phishing attack were **manufacturing, transportation, real estate, air transportation, and employment**. Manufacturing started with one of the group's lower scores at 5.42% but saw a 26% improvement in its PVP score over the year.

Who and what industries, by size, region, and type, are most phishing prone?

- Smaller organizations (less than 1000 employees)
- In Europe
- Biotech, aerospace, government, accommodations, auto

30%

In 2022, almost one-third (30%) of adults in the world had encountered phishing, and 35% had experienced an SMS or mobile scam.



Who and What Industries, by Size, Region, and Type, are the Least Phishing-Prone?

- Large companies, over 25,000
- In Australasia
- Manufacturing, real estate, employment, transportation, air transportation

Industries with the Lowest Risk Phish Response

No industry is safe from cyber-attacks and phishing. However, some fare better than others regarding how employees deal with and respond to a phishing attack. As the data shows, the most minor phishing-prone companies offer exceptional PVP rates, and some continue improving as simulated phishing exercises are regularly run. Amongst the stars of PVP are manufacturing and real estate, delivering significant and continuous improvement on already excellent PVP scores.

Results

Industry	2021	2022	PVP Change
Real Estate	4.43%	3.62%	18.28% ∇
Employment	3.98%	4%	0.5%
Manufacturing	5.42%	4.01%	26.01% ∇
Transportation	4.44%	4.38%	1.35%∇
Air Transportation	5.63%	4.67%	17.05%∇

Industries with the Highest Risk, Phish Response

Industries with a high-risk response are prone to phishing-based cyber-attacks. This puts them at high risk of various attack types, including data breaches, business email compromise scams, and ransomware attacks. An organization must take control of this risk using an automated security awareness training program.

Results

Industry	2021	2022	PVP Change
Biotechnology	32.33%	32.26%	0.22% ∇
Aerospace	25.21%	25.00%	0.83% ∇
Accommodations	21.38%	23.38%	9.35%
Auto	23.33%	23.34%	0.04%
Government	22.34%	21.74%	2.69% ∇

Biotechnology was found to be at significant risk of a phishing-initiated cyber-attack with an initial PVP in 2021 of **32.33%**; even after one year, there was a slight improvement. The Government sector, with a PVP score that is still high at **21.74%** in 2022, shows the best improvement.

Conclusion

The data indicates that an effective Phishing and SMShing awareness strategy works. The 92%, on average, reduction in phishing susceptibility is strong evidence for the use of automated, regular phishing simulations, no matter what size organization or where it is based.

However, deeply intrinsic within the data was that some organizations, particularly smaller companies, need more resources to carry out an effective security awareness strategy, thus reducing the effectiveness of a security awareness platform. For these companies, deploying an automated training package, either in-house or by a managed service provider (MSP), is the best option. Automation takes the strain away from busy IT teams.

SafeTitan's automated Phishing and SMShing awareness solution reduces overhead to MSPs and an organization's security department, making implementing an effective Security Awareness Strategy possible.

SafeTitan's reactive targeted training only enrolls susceptible people in training campaigns, thus reducing staff time and cost overhead to MSPs and organizations.

SafeTitan Automated Campaigns

Automation and focused training are the two pivots upon which practical simulated phishing sessions turn. This is why SafeTitan has released comprehensive support for automated testing and training campaigns. With automation, organizations can run an effective annual security awareness strategy, reducing the cost and time needed to set up, manage, and deploy training. This significantly reduces the overheads for an MSP or in-house IT or security administrator.

Automation provides control: by planning and scheduling, the MSP or organization can:

- Select the number of campaigns they wish to run each quarter.
- Select response training messages that give immediate training to the responder.
- Deliver further reactive training in video or interactive training formats.

$4.45 m

Average cost of a breach in 2023 is $4.45 million

(The IBM Data Breach Investigation report)

92%

of organizations have succumbed to a phishing attack via a Microsoft 365 environment.

Phishing occurs highest in smaller organizations of less than 250 employees.[18]

Source[18] - Cybersecurity ventures

TitanHQ
SafeTitan

Time and cost overhead is reduced for the administrator and staff as only those who respond to the simulations will be engaged in training, thus reducing the training overhead to the organization. SafeTitan is powered by automation, but the platform has a full range of advanced features needed to make security awareness training effective. Some of these features include:

Automated Phishing Campaigns

A simulated phishing platform delivers spoof emails and text messages to employees to test their responses. The administrator of the simulated phishing campaign configures this platform. This task typically involves choosing the elements of a phishing message, such as:

Which employees will be targeted by spoof phishing messages?

- What type of phishing message will be sent out?
- The content of the phishing message, including phishing links and spoofed malicious attachments.
- During training, feedback for an employee who clicks a malicious element teaches the employee what could go wrong.

All these elements are typically available from a rich source of preconfigured phishing templates. However, automation of these campaigns takes this process to new optimization levels by generating repeated simulated phishing campaigns with no user intervention. An automated scheduling calendar is used to send out pre-configured campaigns at regular intervals; the process is streamlined, saving time and money and ensuring regular training happens to improve the effectiveness of awareness programs. The campaigns are adjusted using AI to ensure that the simulated phishing program improves effectiveness over time.

Automated Reporting and Reminders

Reporting is integral to security awareness training; reports are used to evidence compliance and offer meaningful insights into awareness training. Also, reminders about training can take lots of time if done manually. An at-a-glance dashboard provides the tool to configure and auto-generate reports, alerts, and reminders. These reports contain information about how campaigns are progressing and can evidence the effectiveness of a training session, demonstrating improved security awareness.

Automated Enrollment

“Risky clickers” are those employees who click on a malicious link or open a dangerous attachment. Identifying these users and adjusting their training sessions would take a long time and create lags in training. Instead, a process known as ‘Auto-enrolment ‘for risky clickers is used to automatically assign a training simulation that fits the needs of that employee. The ability to automatically recognize risky behavior is an inherent aspect of behavior-driven security awareness training. Using a behavioral event to trigger an automated process to improve a training campaign on a per-user basis is a powerful way to save time and money.

More SafeTitan Features

- A vast set of simulated phishing templates: Access to over 1.8K phishing templates that can be used to generate automated simulated phishing campaigns.
- Mass campaigns and training. There is no need to spend hours selecting customers and assigning one-by-one. Select multiple and spin up a training.
- Automate scheduling: Create a campaign or training and schedule execution N times per week/month/year.
- Auto-enrolment for risky clickers: If a predefined action is performed (i.e., the user clicked a link in a training phishing email), the user is automatically assigned to a training simulation.
- Scheduled client reporting: Configure reports in a couple of clicks and enjoy new data weekly, bi-weekly, quarterly, bi-annually, or annually.

TitanHQ
SafeTitan

SafeTitan for MSPs

SafeTitan is an award-winning security awareness training solution designed for delivery by an MSP. Some of the features that make SafeTitan a great choice to add to an MSP's security stack include the following:

- **Reduce security risk for your clients.**
- **Fully re-brandable solution for your customers.**
- **MSP Dashboard: allows for the setup of manual or automated simulated phishing campaigns. Automated simulated [phishing is AI-driven to adjust to changes in user behavior over time.**
- **Automated phishing simulation, training, quizzes, videos, smishing, and phishing reporting in a matter of minutes.**
- **Access to over 18,000 phishing templates, 80+ Videos, trainings sessions & webinars.**
- **Auto Campaigns that provide MSPs with always-on SAT campaigns.**
- **Easy to understand training content in manageable pieces..**
- **Seamless integration with TitanHQ's email security and web security solutions.**
- **Dynamic User Management, easily add users.**

Mass campaigns & Training.

Designed to fit an MSP security stack seamlessly.

Auto-enrolment for risky clickers

Scheduled client reporting

Automated scheduling of campaigns

Security Culture Supporting the Front-Line Human Defender

Cyber-attacks that are human-centered have changed the way cybercriminals target businesses and employees. This advancement in activity and scope by manipulating people into actions like clicking a phishing link has led to massive growth in cybercrime. Cybercrimes are an international, organized, and sophisticated movement expected to cost global businesses around $10.5 trillion by 2027. [1]

Security awareness training increases security and helps transform user behavior to decrease the likelihood of issues with compliance, lawsuits, breaches, and attacks. An MSP should look to align any solution they offer with the client's business situation. For example, the training solution should be able to deliver automated simulated phishing to employees that match the most likely cybersecurity threats and employee profiles.

When choosing an SAT solution, look for a comprehensive offering that covers all aspects of training needs, from phishing simulations to engaging exercises that empower your employees against cyber-attacks and accidents. The only way to overcome this growing threat is through awareness and education. Over time, automated security training, phishing simulations, and reactive behavior-triggered training teach your employees how to handle every threat.

About the Author

Susan Morrow Bio

With over 20 years of experience in tech, Susan has domain expertise in cybersecurity and digital identity. Susan has held several advisory board posts, including the EU's Next Generation Internet initiative; she is an advisor for Think Digital Partners. Susan was listed as one of the most influential women in technology in the UK in 2020, 2021, 2022, and 2023 by Computer Weekly. She was also shortlisted in thetop "100 Women in Tech" in 2021. Susan also writes on identity and security in publications such as CSOOnline and CyberNews.

About TitanHQ

TitanHQ is a 25-year-old multi-award-winning SaaS cybersecurity platform delivering a layered security solution to businesses globally. TitanHQ offers cutting-edge technologies and robust solutions to protect SMBs and MSPs against phishing attacks, malware, ransomware, and other cyberattacks that can compromise data and disrupt operations.

References :

1. TitanHQ 2023 Automated Phishing Simulation Success Report
2. TitanHQ Adjunct study: PVP by sector
3. Cybersecurity ventures: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
4. Statistica: https://www.statista.com/statistics/1389306/cyber-crime-encounter-worldwide-by-type/
5. ENISA: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends
6. IBM research: https://www.ibm.com/reports/threat-intelligence
7. Verizon https://www.verizon.com/business/en-gb/resources/reports/dbir/
8. IBM: https://www.ibm.com/reports/data-breach
9. https://www.thecloudcommunity.net/media/mdjmn3dh/delinea-whitepaper-balancing-productivity-and-security.pdf
10. https://www.statista.com/statistics/266161/websites-most-affected-by-phishing/
11. TitanHQ blog post: https://www.titanhq.com/blog/employees-firewall-cybercrime/
12. Cybersecurity ventures: https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/
13. FBI: https://www.ic3.gov/Media/Y2023/PSA230609
14. TitanHQ blog post: https://www.spamtitan.com/blog/bec-attacks-businesses-improve-defenses/
15. IBM research: https://www.ibm.com/reports/threat-intelligence
16. IC3 report https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
17. Computer Weekly: https://www.computerweekly.com/news/365532100/Nine-in-10-enterprises-fell-victim-to-successful-phishing-in-2022