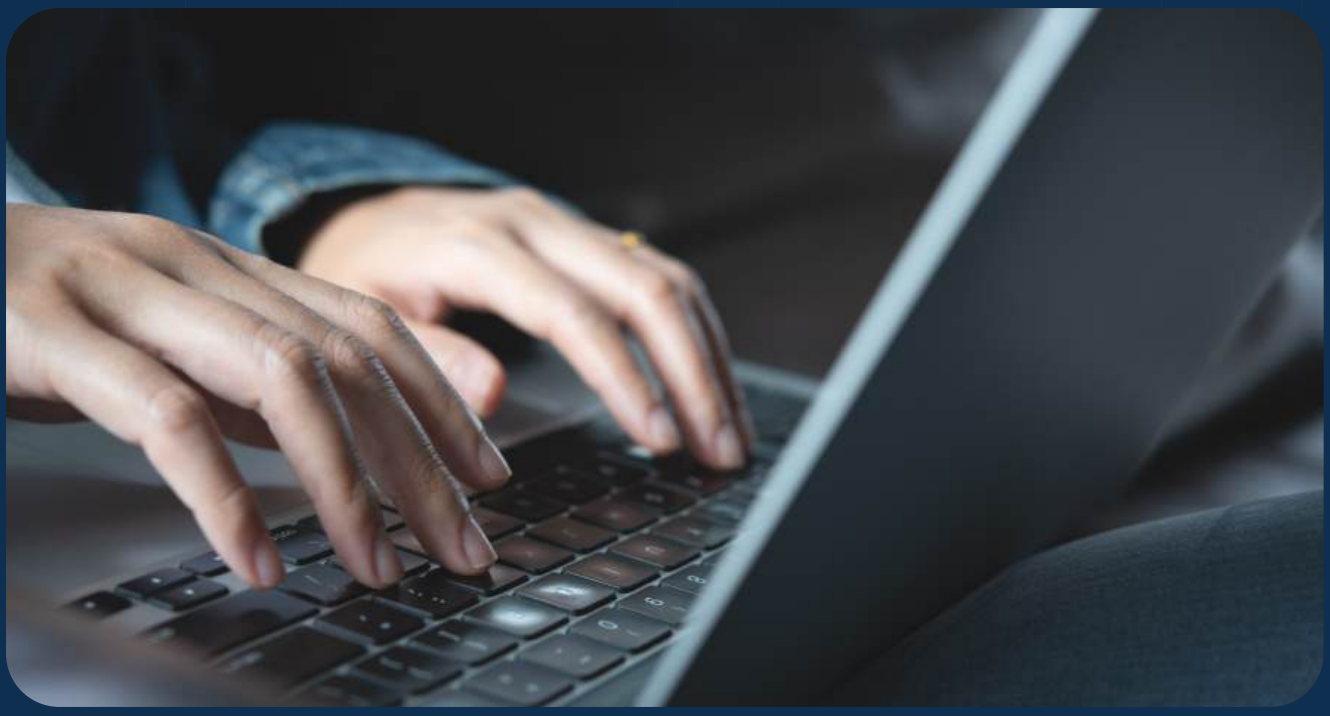
PHISHING TACKLE

Comparison between Phishing Tackle's Managed and Self-Managed Services



Contents

Introduction, including aims and objectives

The research aims to shed light on the journey to improved security awareness an organisation experiences within their first twelve months of signing up with Phishing Tackle.

Objectives:

- Investigate differences in progress between Self-Managed and Managed Service
- Identify key selling points of both service types
- Outline trends in risk by industry and organisation size

Methodology:

Each organisation's progress across both service types was recorded, along with information on their industry and size in terms of employee count. Size groups were determined as follows:

SMB:
1-999

Enterprise:
1000+

Industry groups:

- Agriculture and Mining
- Business Services
- Computers and Electronics
- Consumer Services
- Education
- Energy and Utilities
- Financial Services
- Government
- Healthcare, Pharmaceuticals, & Biotech
- Legal
- Manufacturing
- Media and Entertainment
- Non-Profit
- Other
- Real Estate and Construction
- Retail
- Software & Internet
- Telecommunications
- Transport and Storage
- Travel, Recreation & Leisure
- Wholesale & Distributors

Click-Prone % (CP%) data was then recorded for each to measure risk, where a higher score indicates a higher level of risk.

Due to Self-Managed organisations choosing to use the platform in varying ways, data could not be gathered using the same method between the Self-Managed and Managed Service:

Managed Service

To start, an initial test was carried out before providing any training for each organisation in order to assess the starting level of risk across all recipients within the organisation, known as a baseline.

The CP% was then calculated on a month-by-month basis from the baseline, testing all recipients within an organisation each time, from the 1st month of phishing and training up to the 12th month of simulated phishing campaigns, along with a score for their most recent campaign. A percentage of change in CP% was then calculated, comparing the CP% after three, six, nine and twelve months against their baseline CP%.

In some instances, organisations requested that their frequent campaigns be separated into groups, such as by department. In this case, the mean CP% was calculated depending on the frequency and timeframes requested.

Where an organisation requested to run their separate campaigns on the same day, a mean score was calculated between all campaigns occurring on that day.

Where an organisation requested to stagger their separate campaigns over a specified period, a mean score was calculated from all campaigns until the last group's campaign ran. The mean score was timestamped with the month in which the last campaign was carried out within each period.

To align with the Self-Managed groups overleaf, all Managed Service organisations are classed as frequently tests and frequently trains.

Self-Managed

As usage trends of the platform vary in this service type, the following five categories were created and allocated accordingly:

As usage trends of the platform vary in this service type, the following five categories were created and allocated accordingly:

- **Frequently tests and frequently trains**
- **Frequently tests and infrequently trains**
- **Frequently tests and never trains**
- **Infrequently tests and infrequently trains**
- **Infrequently tests and never trains**

To determine whether an organisation frequently uses simulated phishing, they must have scheduled more than one campaign with a frequency of no more than six months, or scheduled at least one recurring campaign with a repeat timer of less than one year. Any organisations that created a recurring campaign that has only run one time were classed as infrequent.

To determine whether an organisation's training is qualified as infrequent, they must have used at least one course from the media library under the theme of security awareness, and the course must not have 0.00% completion. To determine whether an organisation frequently uses training, they must have consistently scheduled a training course containing differing content at a frequency of no larger than quarterly. No assessed Self-Managed organisations qualified as using frequent training.

To assess an organisation's initial risk, the results of the first campaign created to send to all recipients were treated as the baseline test. If an organisation had only run ad-hoc campaigns targeted to select departments, groups, or individuals, a mean CP% was calculated between all applicable campaigns. Where an organisation had not tested all recipients across multiple campaigns, the results for the missing recipients were counted as a non-failure.

The Current CP% was then recorded as a representation of their current risk by recording the results of the last campaign created to go to all recipients.

For organisations that ran ad-hoc campaigns targeted to select departments, groups, or individuals, or staggered or split their campaigns into groups, a mean score was calculated from all most recent campaigns until the total number of recipients phished matched the number of recipients within their address book.

If the number of recipients phished within this period did not match the total number of recipients, the results from the un-phished recipients' most recent test were used, or if they had never been tested, were counted as a non-failure.

A percentage of change in CP% was then calculated between the baseline and current CP%.

Findings / Results

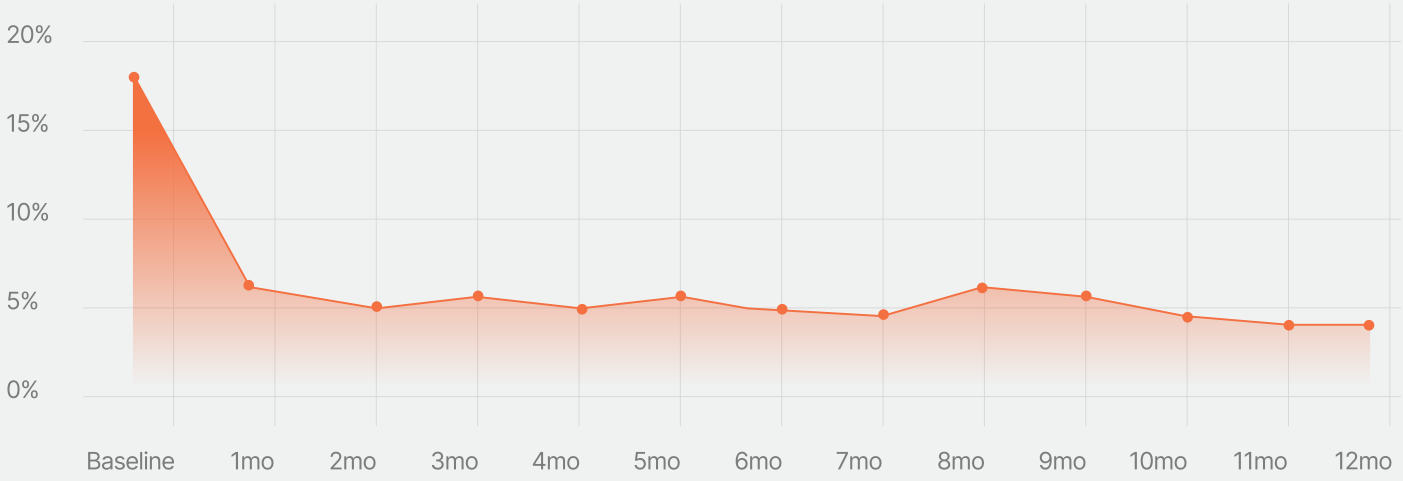
Managed Service

The average baseline CP% for all Managed Service organisations came to 17.17%, and the average 12th-month score came to 4.07%: an improvement in score of 76.31%.

an improvement in score

76.31%

Click-Prone % Over Time



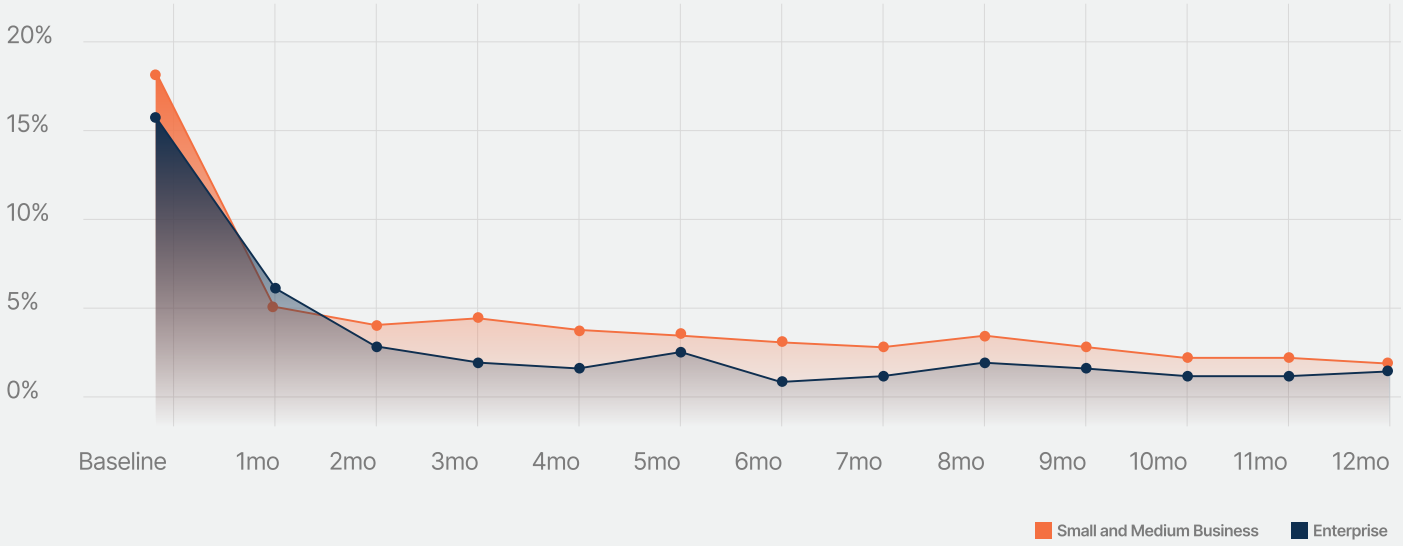
SMBs scored the highest average of

17.43%

Enterprises scored the lowest average of

15.41%

Click-Prone % Over Time by Organisation Size

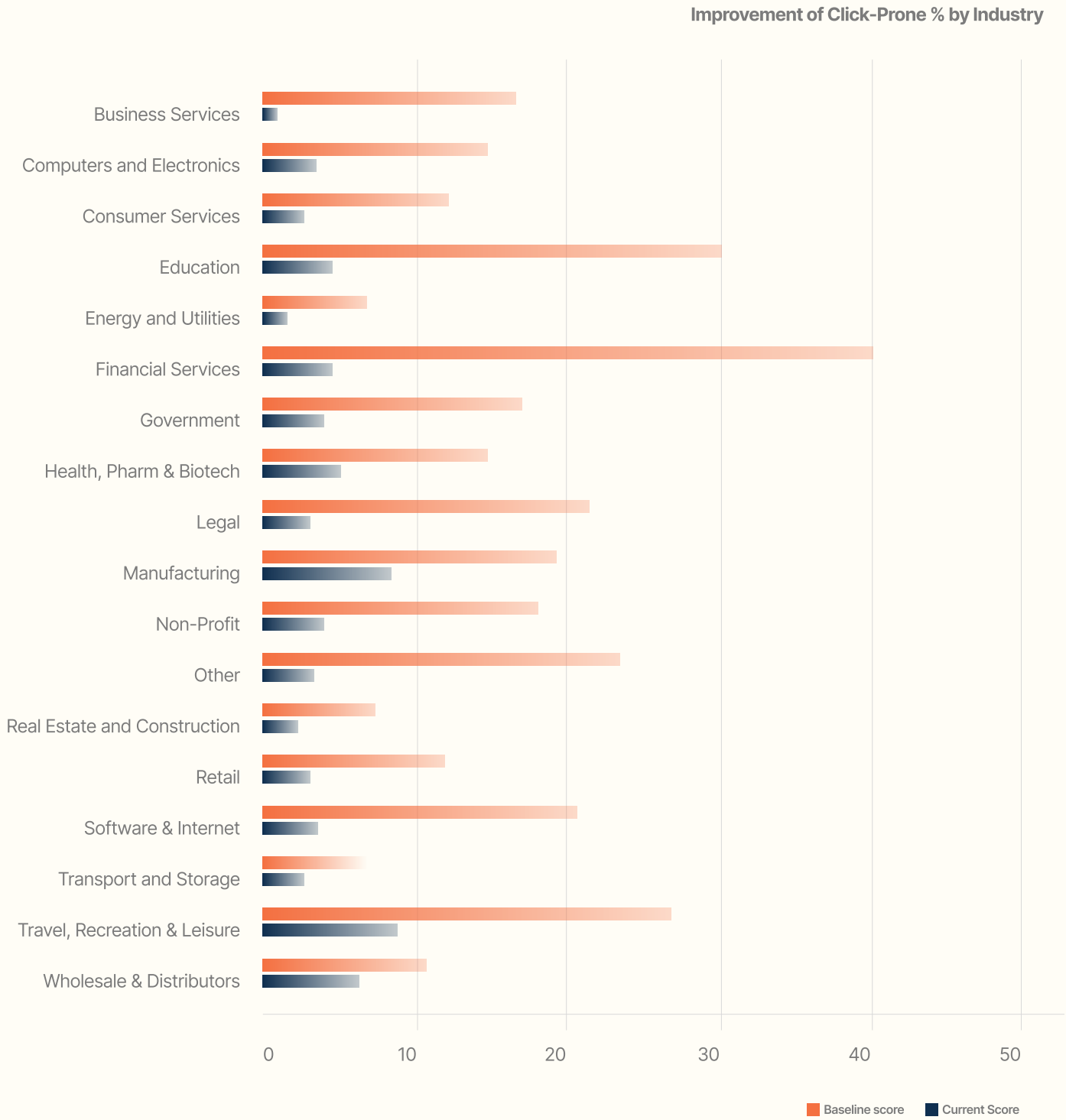


When grouped by industry, the three cohorts with the highest risk were:

Financial Services
40.25%

Education
30.28%

Travel, Recreation, and Leisure
25.40%



Self-Managed

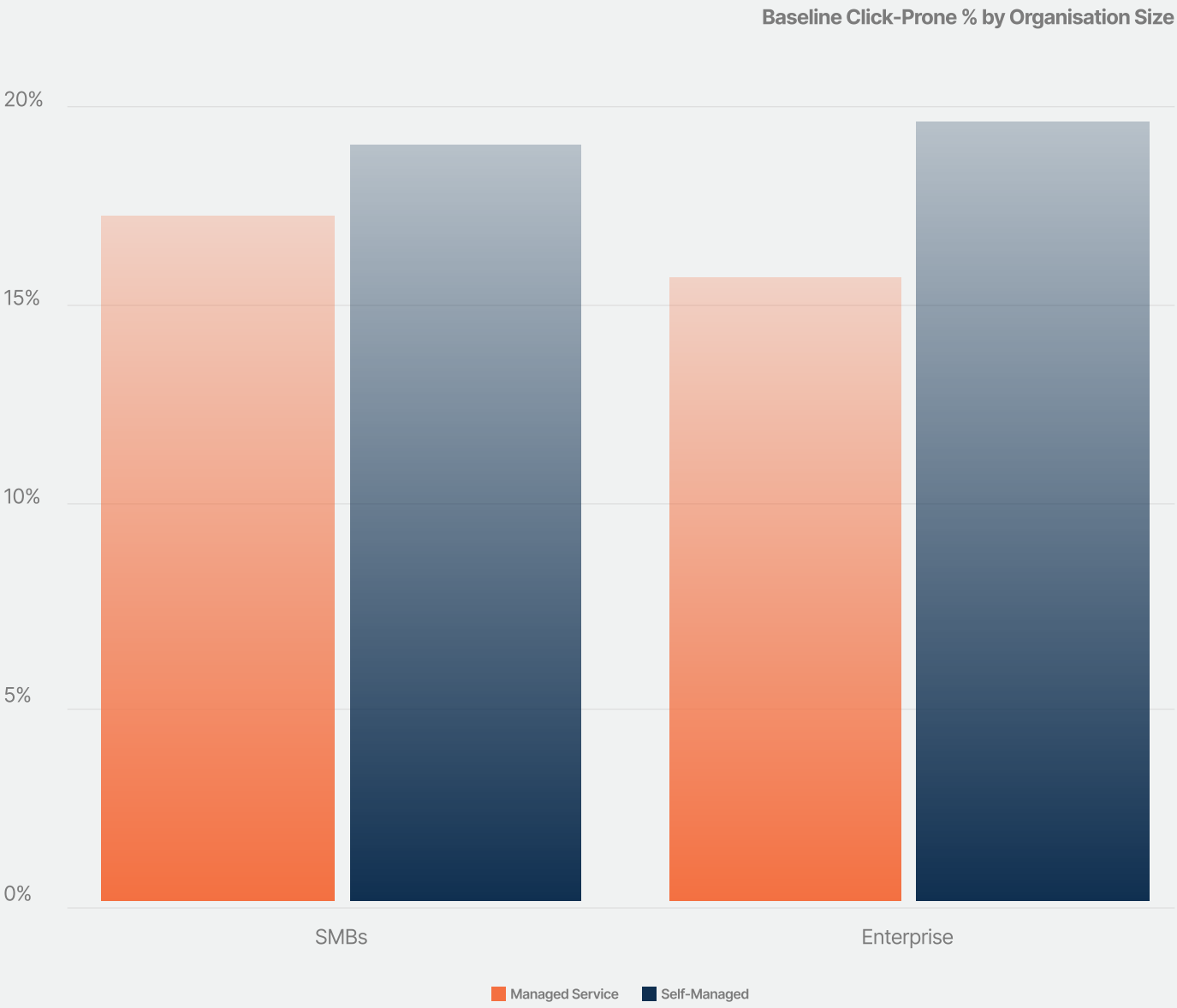
The average baseline CP% for all Self-Managed organisations came to 19.76% and a current CP% of 11.93%, improving by an average of 60.37% since the baseline test.

an improvement in score

60.37%

After running a baseline test:

- **SMBs** scored the lowest with 18.70% and a current score of 10.57%: an improvement of **43.50%**
- **Enterprises** scored the highest with 22.89% and a current score of 19.74%: an improvement of **13.76%**



When grouped by usage, 68% frequently used phishing campaigns, and 43% used training. Compared to the total number of Self-Managed Organisations surveyed:

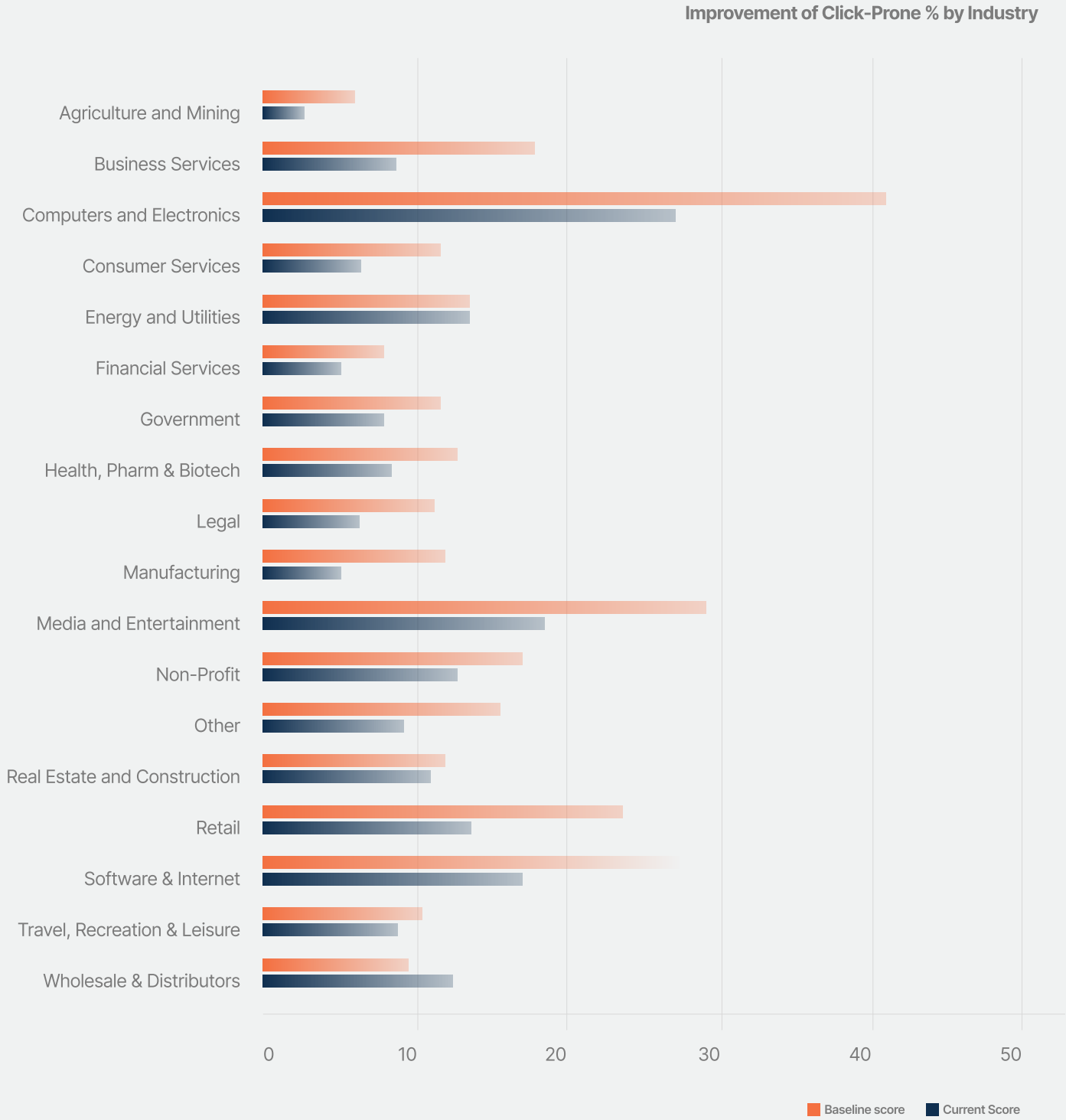
+ **Frequently tests and infrequently trains** accounted for 33%
+ **Frequently tests and never trains** accounted for 33%
+ **Infrequently tests and infrequently trains** accounted for 10%
+ **Infrequently tests and never trains** accounted for 22%

Comparing the baseline to current CP% of these groups:

+ **Frequently tests and infrequently trains** scored a baseline of 21.44% and a current score of 8.42%: an improvement of **60.71%.**
+ **Frequently tests and never trains** scored a baseline of 15.72% and a current score of 7.32%: an improvement of **53.41%.**
+ **Infrequently tests and infrequently trains** scored a baseline of 17.43% and a current score of 15.17%: an improvement of **12.94%.**
+ **Infrequently tests and never trains** scored a baseline of 25.90% and a current score of 26.72%: an increase in risk of **3.17%.**

When grouped by industry, the three cohorts with the highest risk were:

Computers and Electronics	Media and Entertainment	Software & Internet
40.68%	**29.41%**	**27.17%**

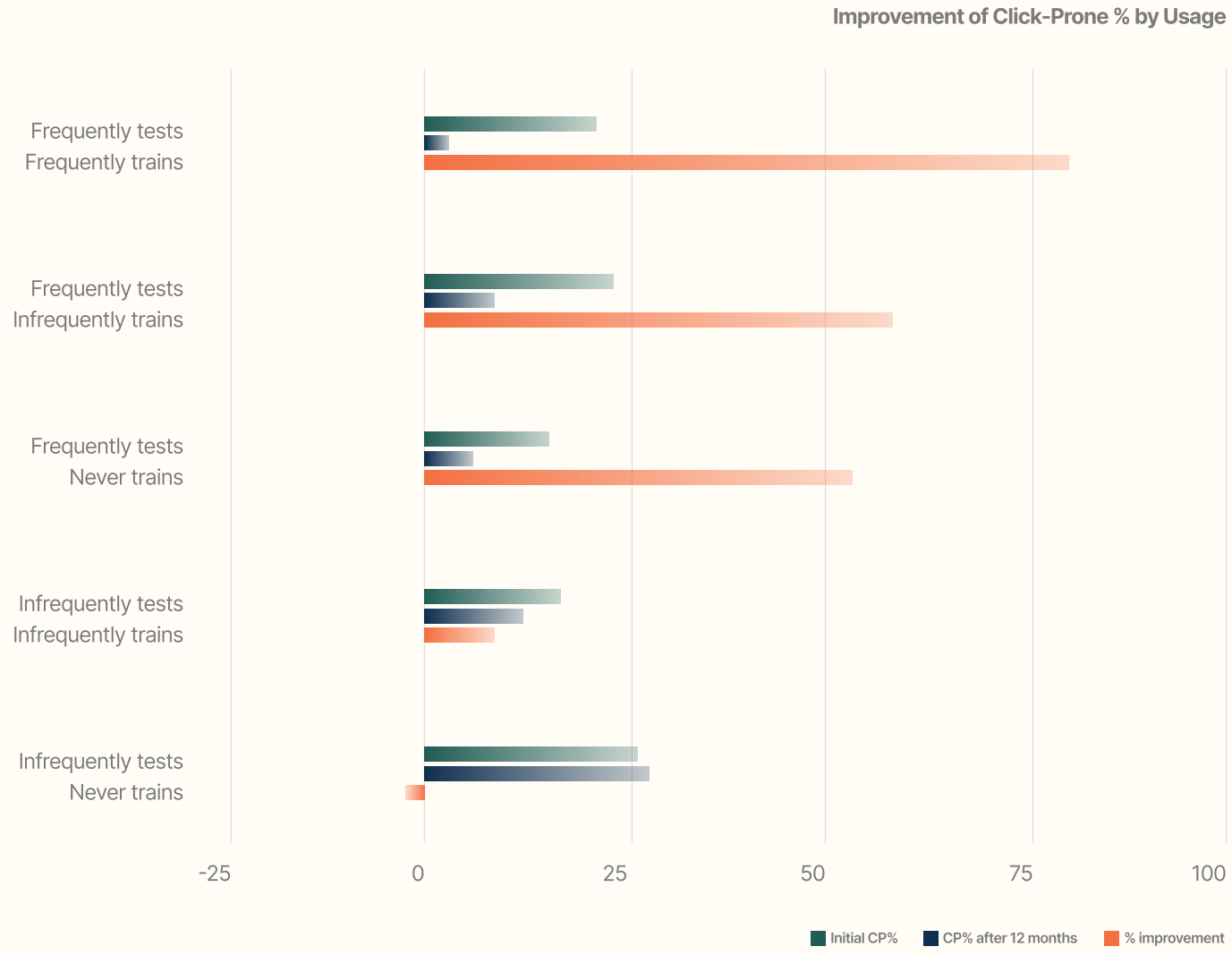


Discussion

Looking at percentage change since the baseline test, data suggests that frequently testing and training provides the highest level of improvement, with an improvement score of 81.60%. Frequently testing but infrequently training (60.71%) demonstrates a 7.40% difference in improvement when compared to frequently testing and never training (53.41%), suggesting that a higher frequency of training is a key factor in boosting awareness and reducing risk.

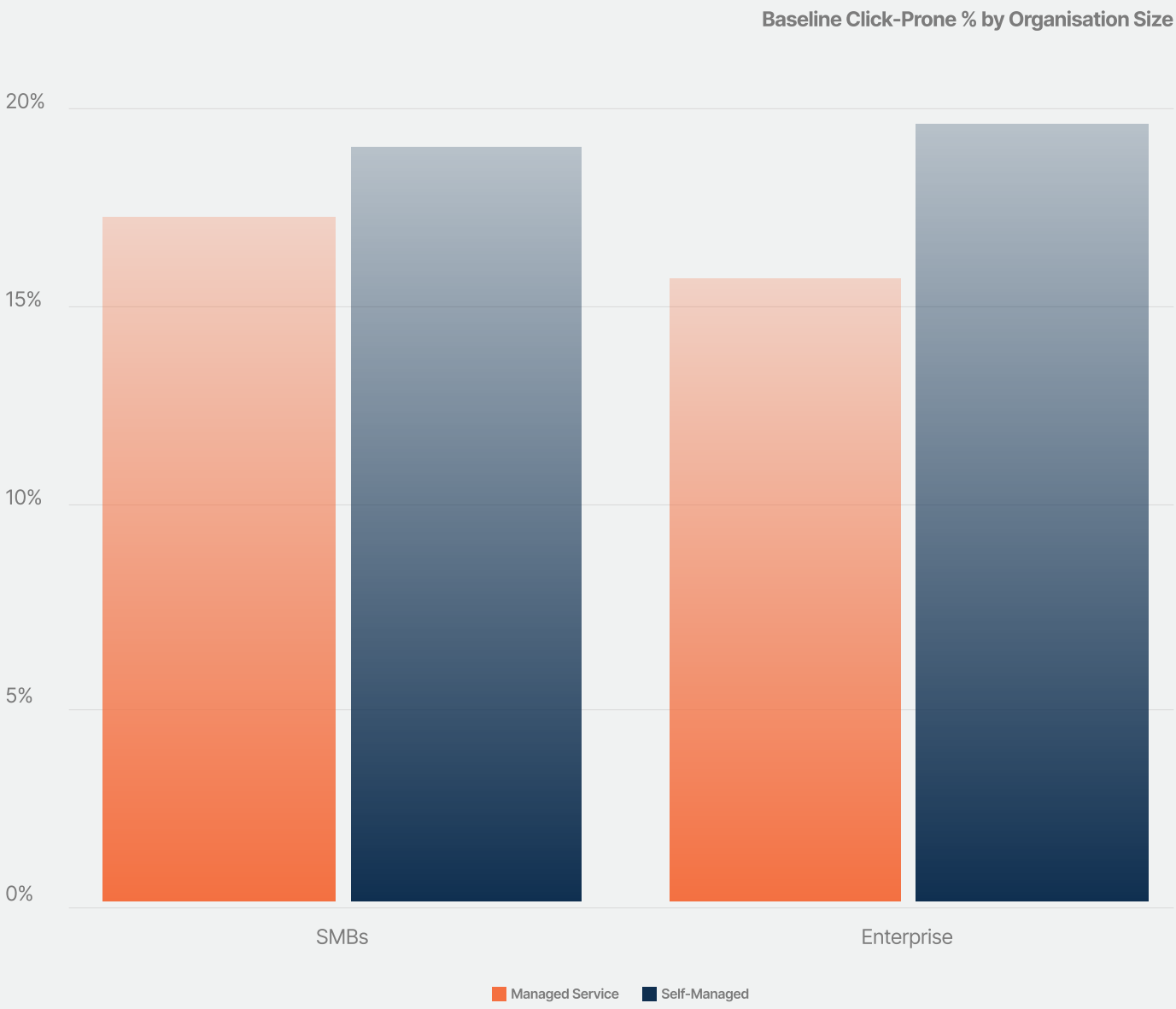
Those who train without testing regularly, or at all, see a much lower improvement of **12.94%**

Suggesting that testing is essential to highlighting areas of weakness over time, allowing for targeted training material.



For those who do not regularly test or use any training, an increase in risk of 3.17% suggests that over time, with no insight into the posture of the human firewall, an organisation continues to become more likely to suffer from a cyber-attack.

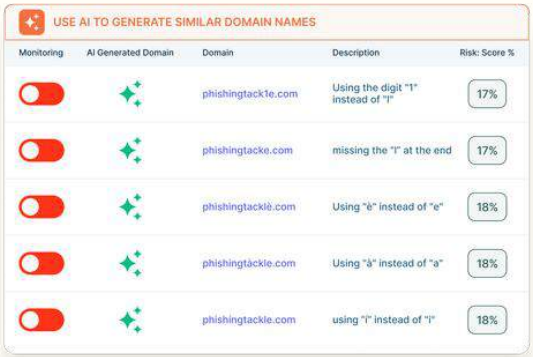
On average, organisations of all sizes appear to start with a similar level of risk. However, larger organisations see the smallest levels of improvement when comparing baseline CP% to their most recent results, and of these organisations, those running a Self-Managed service see a much lower improvement (13.76%), when compared to Managed Service (91.97%). This suggests that time and resources are a heavily limiting factor in creating positive changes in security awareness.



New Tools That Turbocharge Your Security Strategy

PhishNet: Phishing response supercharged

Automate threat triage with real-time SOAR-powered email analysis. Investigate suspicious messages instantly, scan for malware via VirusTotal, and route threats with zero manual effort.

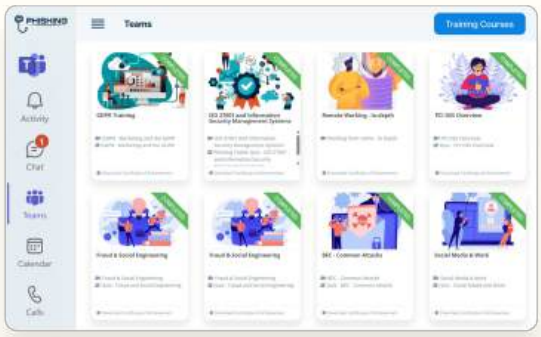


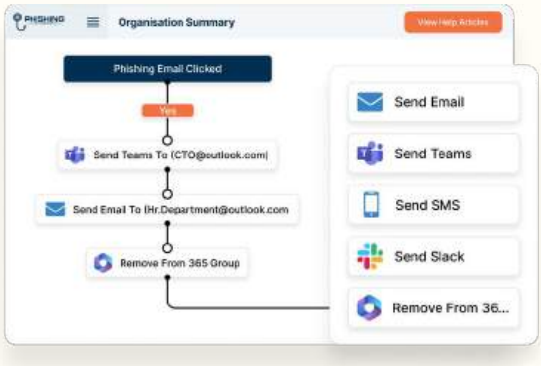
CatPhish: Brand protection on autopilot

Stop lookalike domains in their tracks. CatPhish uses AI to spot and monitor spoofed domains, surface high-risk threats, and launch takedown actions before they're weaponised.

PhishTAIL: Training delivered where your people already are

Plug security awareness training, policy updates & alerts right into Microsoft Teams. No logins, no platform switching, just faster engagement and better adoption.





StarPhish: Next-level automation for instant response

When someone clicks a phishing link, StarPhish takes action, triggering training, access controls, and alerts automatically. Build workflows with drag-and-drop ease and turn incidents into learning opportunities, instantly.

Conclusion

This research clearly shows that regular phishing simulations combined with consistent training deliver the strongest improvements in security awareness. Managed Service customers, who benefit from both, achieve the most significant risk reduction, while Self-Managed organisations often see smaller gains due to resource and time constraints.

For organisations looking to strengthen their “human firewall,” the path is clear: frequent, targeted testing, timely training, and tools that streamline the process are essential to reducing click-prone risk and building long-term resilience against phishing threats.

Book a demo

PHISHING TACKLE