IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46SP/2025/4642225/
Vol. 2025 (37), Article ID 4642225

# Phishing Trends Over Time: An Empirical Analysis of Anti-Phishing Database Data*

Krystian MAGDZIARZ and Stanisław SKRZYPECKI

Military University of Technology, Warsaw, Poland

Correspondence should be addressed to: Krystian MAGDZIARZ, krystian.magdziarz@student.wat.edu.pl

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

## Abstract

Despite widespread claims of exponential phishing growth, empirical evidence remains fragmented and methodologically inconsistent. This study challenges conventional assumptions through systematic analysis of over 18.2 million phishing incidents across three major databases (PhishTank, APWG, CERT Polska) spanning 2009–2025. Employing Mann-Kendall trend analysis and seasonal decomposition, we identify a consistent temporal pattern across all data sources: a significant increase in phishing incidents peaking around 2015-2016, followed by a sustained decline. However, the statistical significance of these trends varies considerably: PhishTank data demonstrates a strong upward trend during its observation period ($\tau = 0.656$, $p < 0.001$), APWG shows a significant downward trajectory post-2015 ($\tau = -0.486$, $p < 0.001$), while CERT Polska exhibits high volatility without statistically significant long-term trends ($\tau = 0.295$, $p = 0.138$). High cross-database correlation confirms consistency in trend patterns across independent sources. These findings fundamentally question the narrative of continuously escalating phishing volumes and suggest a strategic shift from mass, indiscriminate campaigns toward more sophisticated, targeted attacks that evade traditional detection mechanisms. The documented decline in reported incidents does not indicate reduced threat severity but rather reflects attacker adaptation and evolution in social engineering techniques.

**Keywords:** phishing, cybersecurity, trend analysis, anti-phishing databases

## Introduction

The dynamic development of information technology and the progressive digitization of social and economic life have contributed to the emergence of new possibilities for conducting social engineering attacks (Aldawood and Skinner, 2020; Magdziarz, 2024; Desolda et al., 20221115). Research indicates that phishing is one of the main vectors of information system security breaches, leading to significant financial losses (Internet Crime Complaint Center (IC3) | Business Email Compromise The $26 Billion Scam 2025) and personal data leaks (Aktualności - UODO 2025).

The digital transformation of recent years, particularly intensified during the COVID-19 pandemic and the widespread fear, has led to an increase in the number of potential targets for phishing attacks (Abroshan et al., 2021; Zimoń and Kasprzyk, 2021). An evolution of techniques used by criminals is also observed – from mass, untargeted campaigns to \ the phenomenon and constitute a basis for improving protective mechanisms.

**Cite this Article as:** Krystian MAGDZIARZ and Stanisław SKRZYPECKI, Vol. 2025 (37) "Phishing Trends Over Time: An Empirical Analysis of Anti-Phishing Database Data " Communications of International Proceedings, Vol. 2025 (37), Article ID 4642225, https://doi.org/10.5171/2025.4642225

## Research Objectives

Within this publication, the following research questions were formulated, where the fundamental issue remains the verification of the thesis about the growing trend of phishing threats:

**Main Research Question**

To what extent does empirical analysis of data from anti-phishing databases and reports of institutions responsible for cybersecurity in the years 2009–2025 confirm the commonly accepted thesis in the literature about the systematic growth of the phishing threat (Dou et al., 2017; Aleroud and Zhou, 2017; Matacz and Vodičková, 2023; Phishing Attacks Escalation 2024)?

**Detailed Research Questions**

The first detailed question focuses on characterizing the dynamics of changes in phishing incidents. It includes identification of basic trend parameters, including its character (linear, non-linear), occurrence of potential seasonality, and short-term variability in the examined time period.

The second research question concerns comparative analysis of trends reported by individual anti-phishing databases. In particular, it is important to determine the degree of correlation between data from different sources and identify potential systematic discrepancies in the incident reporting process.

The third question refers to the identification and assessment of the impact of external factors on observed trends. In particular, dependencies between global events (such as the COVID-19 pandemic) and the dynamics of phishing attacks will be analyzed, as well as relationships between technological progress and the evolution of attack methods.

The presented research questions create a coherent analytical structure, enabling systematic verification of the main research hypothesis while taking into account significant methodological and contextual aspects.

## Methodology

A mixed methods approach was applied in the study, combining quantitative approach with elements of qualitative analysis. The methodological basis will be systematic analysis of data from leading anti-phishing databases, supported by statistical analysis and data exploration methods.

**Data Sources**

The study is based on data from the following primary sources:

- PhishTank database (PhishTank | Join the Fight against Phishing 2025),
- APWG (Anti-Phishing Working Group) Repository (APWG | Unifying The Global Response To Cybercrime 2024),
- Data from CERT Polska (Publikacje CERT Polska 2025).

**Research Procedure**

The research process was divided into the following stages:

**Stage I: Data Acquisition and Preparation**

- Systematic downloading of archival data from selected databases for the period 2009–2025,
- Normalization of data to a uniform format,
- Identification and removal of duplicates,
- Verification of data completeness and consistency.

**Stage II: Quantitative Analysis**

- Conducting time series analysis,
- Application of statistical methods to identify trends,
- Execution of statistical tests verifying research hypotheses,

- Correlation analysis between different data sources.

**Stage III: Contextual Analysis**

- Identification of turning points in trends,
- Analysis of correlations with external events,
- Study of seasonality of the phenomenon,
- Assessment of the impact of technological factors.

**Data Analysis Methods**

The following methods were utilized in the study:

- Seasonality analysis based on monthly averages,
- Mann-Kendall statistical tests for trend analysis,
- Correlation analysis between data sources,
- Anomaly detection methods in time series.

## Research Support Software

To facilitate systematic data processing, statistical analysis, and visualization of results, a specialized analytical application was developed. The software implements automated data acquisition mechanisms from source databases, enabling processing of multi-year datasets with varying temporal granularity (monthly for PhishTank and APWG, yearly for CERT Polska). The application provides functionality for conducting Mann-Kendall trend analysis, calculating seasonality indices, and generating correlation matrices between different data sources. The tool was implemented in Python, utilizing libraries such as pandas for data manipulation, scipy.stats for statistical computations, and matplotlib for scientific visualization. The modular architecture of the application allows for independent analysis of each data source while maintaining capabilities for cross-database comparative studies. The software source code has been made publicly available (Krystianmagdziarz/Phish-Stats 2025), ensuring reproducibility of the conducted analyses and enabling verification of results by other researchers.

## Research Quality Assurance

To ensure reliability of results, the following were applied:

- Triangulation of data sources,
- Systematic validation of results,
- Documentation of the research process,
- Identification and analysis of methodological limitations.

## Methodological Limitations

The following limitations were considered in the study:

- Possible incompleteness of data in source databases,
- Potential delays in incident reporting,
- Differences in attack classification methods between databases,
- Limitations in access to some historical data.

The adopted methodology allows for systematic verification of the posed research questions while maintaining research objectivity.

## Data Analysis

**Trend Analysis**

The Mann-Kendall test (Mann-Kendall Test | Real Statistics Using Excel 2025) was used to verify the significance of the trend, where the test statistic S is calculated as:

$$S = \sum_{i=1}^{n-1} \sum_{j=i+i}^{n} sgn(x_j - x_i) \quad (1)$$

where:

$n -$ total number of observations,
$x_i, x_j -$ observation values at two different time points
$sgn(x_j - x_i) -$ sign of the difference between two values:

$$\begin{cases} 1, & if\ x_j > x_i \\ -1, & if\ x_j < x_i \\ 0, & if\ x_j = x_i \end{cases}$$

The variance of statistic S is given by the formula:

$$VAR(S) = \frac{n(n-1)(2n+5) - \sum_t f_t(f_t - 1)(2f_t + 5)}{18} \quad (2)$$

where:

n − total number of observations,

t − number of repeated values,

ft − number of occurrences (frequency) of value t

With the following test statistic:

$$z = \begin{cases} \frac{S-1}{SE}, jeśli\ S > 0 \\ 0, \quad jeśli\ S = 0 \\ \frac{S+1}{SE}, jeśli\ S < 0 \end{cases} \quad (3)$$

$$SE = \sqrt{VAR(S)} \quad (4)$$

It is possible to formulate the hypotheses:

- No trend: H0

$$H_0: P(x_j > x_i) = P(x_j < x_i)\ \forall \mathrm{i} < \mathrm{j} \quad (5)$$

- Presence of trend: H1

Upward trend:

$$H_1: P(x_j > x_i) > P(x_j < x_i)\ \forall \mathrm{i} < \mathrm{j} \quad (6)$$

Downward trend:

$$H_1: P(x_j > x_i) < P(x_j < x_i)\ \forall \mathrm{i} < \mathrm{j} \quad (7)$$

## Seasonality Analysis

In order to identify seasonal patterns in phishing reports, the seasonal index method was applied. For each month, the average number of reports was calculated, and then compared with the global average, obtaining the seasonality index.

The monthly average for individual months was calculated according to the formulas:

$$\overline{X_m} = \frac{\sum_{y=Y_1}^{Yn} X_{m,y}}{n} \quad (8)$$

$$\overline{X} = \frac{\sum_{m=1}^{12} \overline{X_m}}{12} \tag{9}$$

$$SI_m = \frac{\overline{X_m}}{\overline{X}} \times 100 \tag{10}$$

## Linear Trend Model

In order to analyze long-term changes in time data, a linear regression model was applied. This method allows for determination of the direction and strength of the trend and enables quantitative assessment of its fit to the data using the coefficient of determination R2. Linear regression was chosen due to the simplicity of interpretation and the possibility of application in the case of data with a linear trend character.

The linear regression model was described by the equation:

$$Y = \beta_0 + \beta_1 t + \epsilon \tag{11}$$

Parameters β0 and β1 were estimated using the least squares method. The quality of model fit was assessed using the R2 coefficient. For visualization of the linear regression trend, the add_trendline function (Magdziarz, 2025) was applied, which was implemented in Python. The function uses scipy.stats.linregress (Linregress — SciPy v1.15.1 Manual 2025) to determine β0, β1, correlation coefficient r, p-value, and standard error. Based on the model parameters, trend line values are determined for each time point. The trend line is plotted on the graph using the Matplotlib axis object (Matplotlib Documentation — Matplotlib 3.10.0 Documentation 2025).

## Data Sources

Within the conducted study, data from three leading phishing threat databases were utilized. The source selection process took into account the criteria of credibility, comprehensiveness, and availability of historical data.

### PhishTank

PhishTank constitutes the primary data source in the conducted study. This platform, operating since 2006, is based on a community verification model for phishing reports. Within the study, access was obtained to historical data covering the period from January 2009 to May 2017. Despite attempts to contact the platform administrators, it was not possible to acquire statistical data for later periods. This is a significant research limitation that affected the time scope of the conducted analyses.

### APWG (Anti-Phishing Working Group)

Anti-Phishing Working Group, as an international consortium bringing together over 2,000 organizations from various sectors, publishes quarterly reports on phishing threats. These reports, made available in PDF format, constitute the second key data source in the conducted study. The characteristics of APWG reports include systematic compilations of statistics on phishing activity on a global scale.

The process of acquiring data from APWG reports required systematic extraction and structuring of information from PDF documents.

### CERT POLSKA

CERT Polska (Computer Emergency Response Team), operating within the structures of NASK (Research and Academic Computer Network), constitutes the third data source used in the study. This organization publishes annual reports on the state of cyberspace security in Poland, containing, among other things, detailed information about phishing incidents.

The use of CERT Polska reports allowed for enriching the research perspective with a local dimension, enabling comparison of trends observed in Poland with global data from other sources.

## Complementarity of Data Sources

The selection of data sources was conducted taking into account the criterion of complementarity in terms of monitored phishing attack vectors. The adopted methodology assumes the use of three independent data repositories: PhishTank, specializing in identification and verification of websites used in phishing attacks; APWG, focusing on analysis of phishing campaigns distributed via email; and CERT Polska, providing a

holistic perspective of both types of threats in the national dimension.

**Table 1: Characteristics of data sources in terms of types of monitored phishing attacks.**

| Data Source | Phishing Sites | Email Campaigns | Scope | Data Format |
|---|---|---|---|---|
| PhishTank | ✓ | – | Global | Web Scraping |
| APWG | – | ✓ | Global | PDF Reports (quarterly) |
| CERT Polska | ✓ | ✓ | National | PDF Reports (annual) |

## Results

### PhishTank

Analysis of the total number of phishing reports in the PhishTank database in the years 2009–2017 reveals a clear upward trend (R2 = 0.731). Over the examined period, a systematic increase in activity was observed, from the initial level of 37,909 monthly reports in 2009 to over 58,556 in 2016, with a peak exceeding 122,560 reports in June 2016.

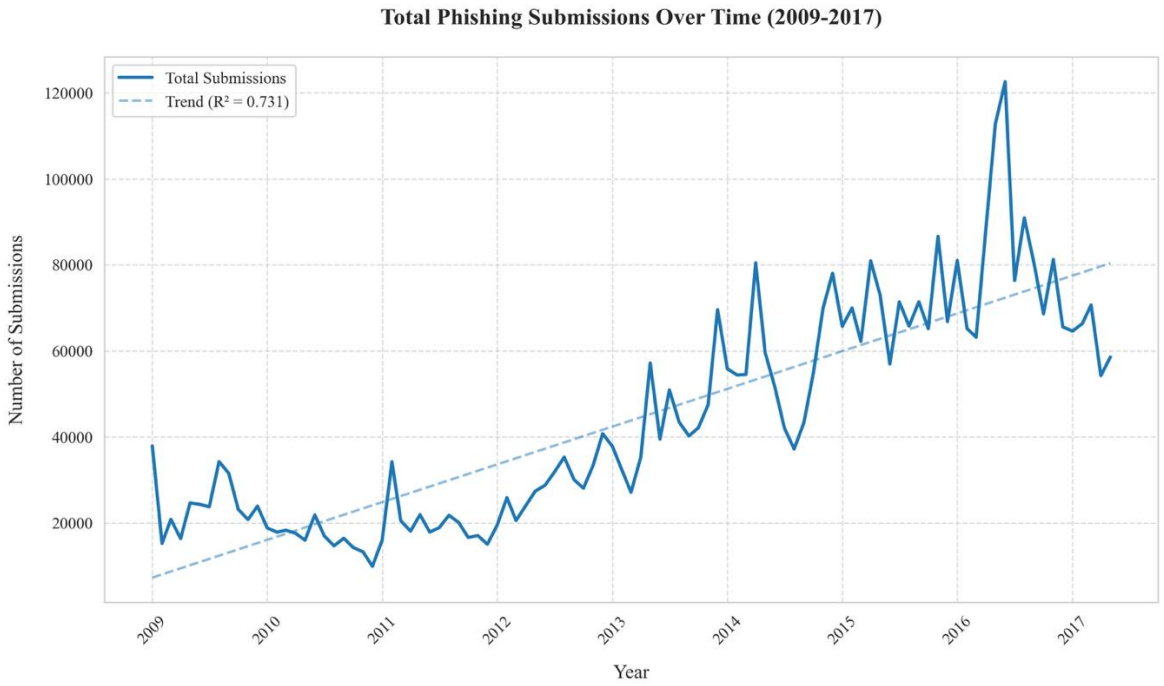


**Fig. 1 Total number of phishing reports (2009–2017) with trend line (R2 = 0.731) – PhishTank database.**

Data retrieved from the PhishTank website reveal a significant disproportion between the total number of reports and confirmed phishing cases in the years 2009–2017. The observed disproportion may indicate limited throughput of the PhishTank verification system (community assessments) – this is why developing modern algorithmic methods for detecting phishing sites is so important.

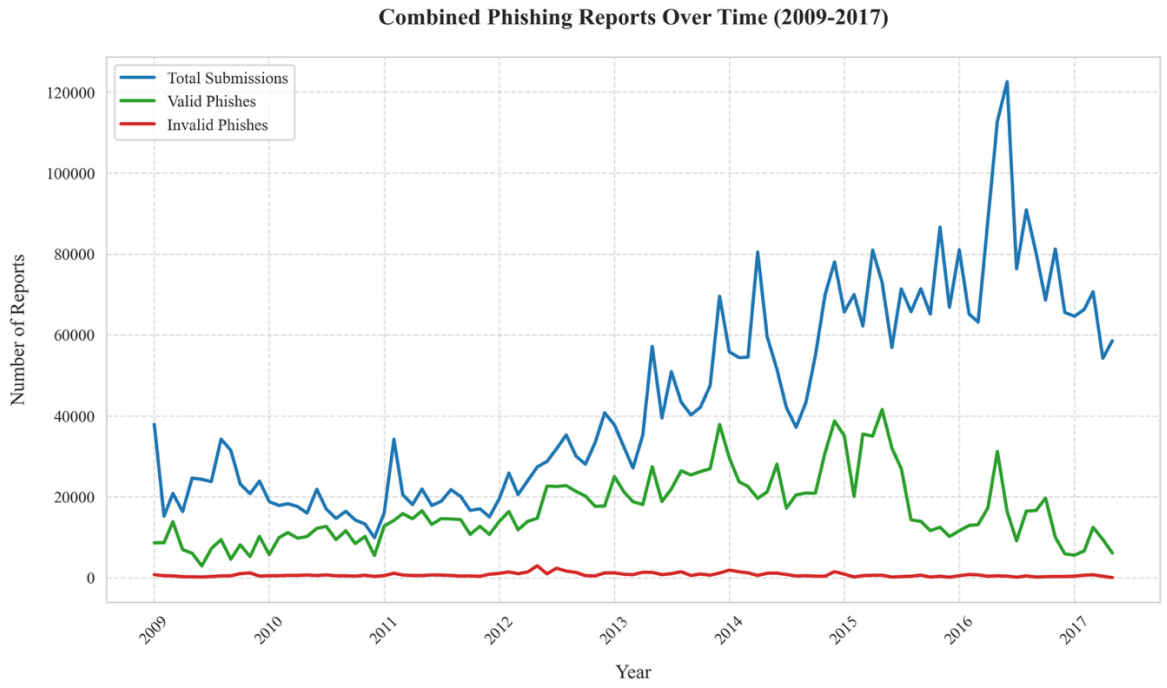


**Fig. 2 Total phishing reports (blue), confirmed cases (green), and unconfirmed cases (red) in the years**

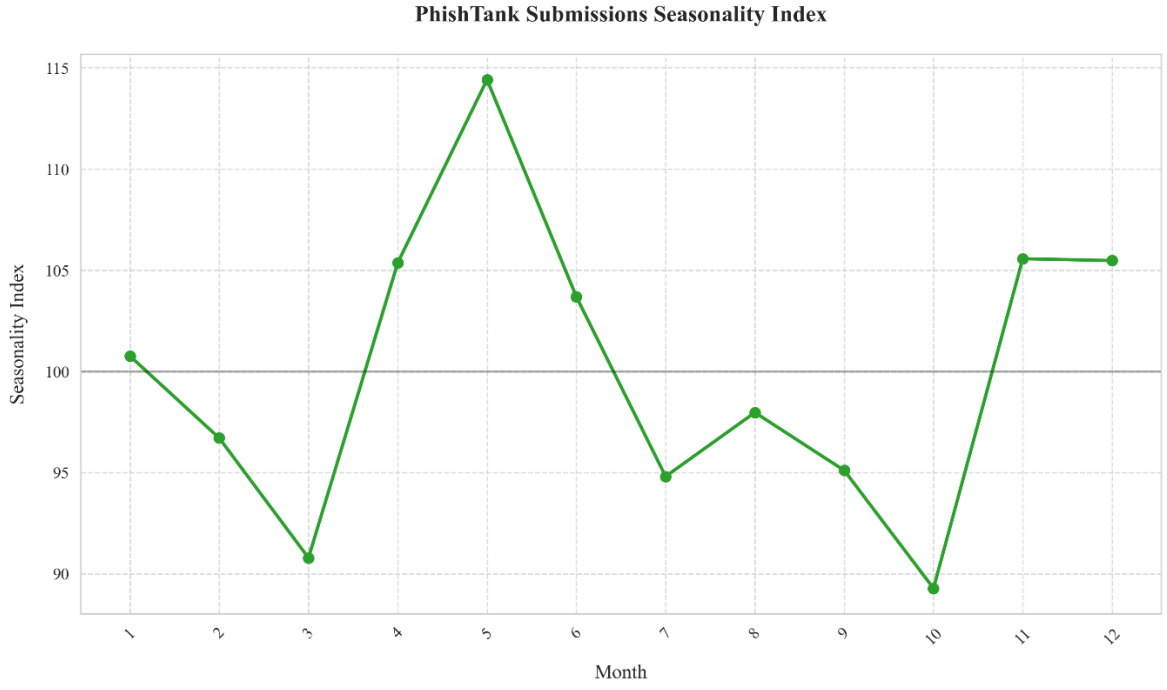


**Fig. 3 Seasonality index of phishing reports in the PhishTank database by month. Source: own elaboration.**

The conducted statistical analysis using the Mann-Kendall test for PhishTank data from 2009–2017 confirms the occurrence of statistically significant upward trends both in the number of reports and in the activity of the verifying community. For the total number of reports, a high Kendall's tau coefficient value was obtained ($\tau = 0.656$, $p < 0.001$), which indicates a strong, systematic increase in the number of reported phishing incidents in the examined period. A similar tendency was observed in the case of the number of community votes ($\tau = 0.620$, $p < 0.001$). High values of the Z statistic for both metrics ($Z = 9.715$ for reports and $Z = 9.187$ for votes) clearly indicate the stability of the observed upward trend, excluding the possibility of random fluctuations.

**APWG**

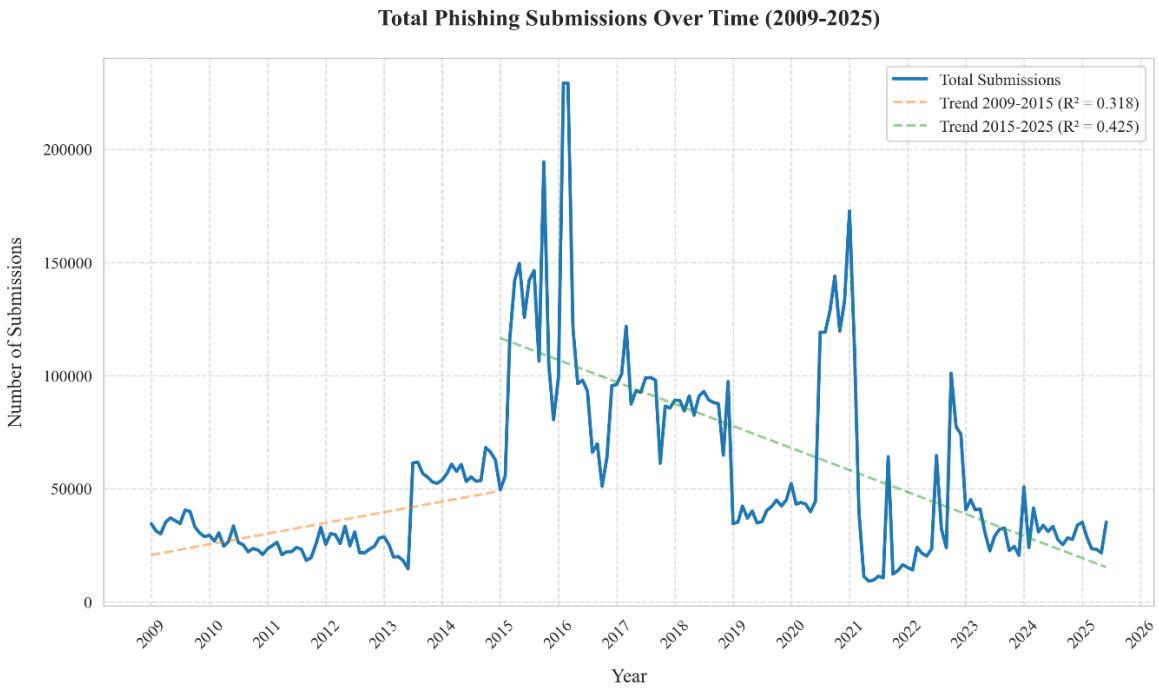


**Fig. 4 Total number of phishing reports (2009– 2025) – APWG database. Source: own elaboration.**

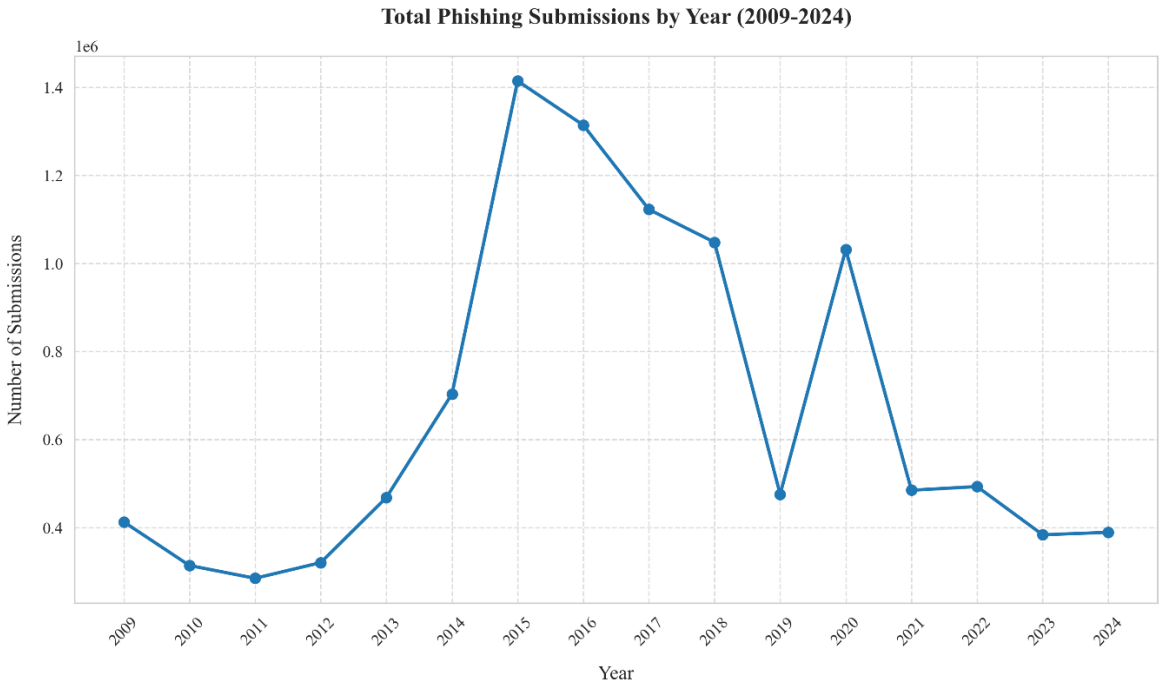


**Fig. 5 Total number of phishing reports (2009– 2025) – values grouped by year – APWG database. Source: own elaboration.**

Analysis of APWG data in the years 2009–2025 (Figures 4 and 5) reveals interesting dynamics in phishing trends. In contrast to PhishTank data, the APWG chart shows two distinct periods with different characteristics. In the years 2009–2015, a moderate upward trend was observed (R2 = 0.318), while the period 2015–2024 is characterized by a clear downward trend (R2 = 0.425). Particularly significant is the sharp increase in phishing activity in 2016, when the number of reports exceeded 220,000, after which a systematic decline occurred. It is worth noting that despite periodic increases in activity in the years 2021–2022, the overall tendency in recent years remains downward.

This observation may indicate an evolution of cybercriminal tactics or increased effectiveness of protective mechanisms, which leads to a smaller number of traditional phishing attacks recorded by APWG.

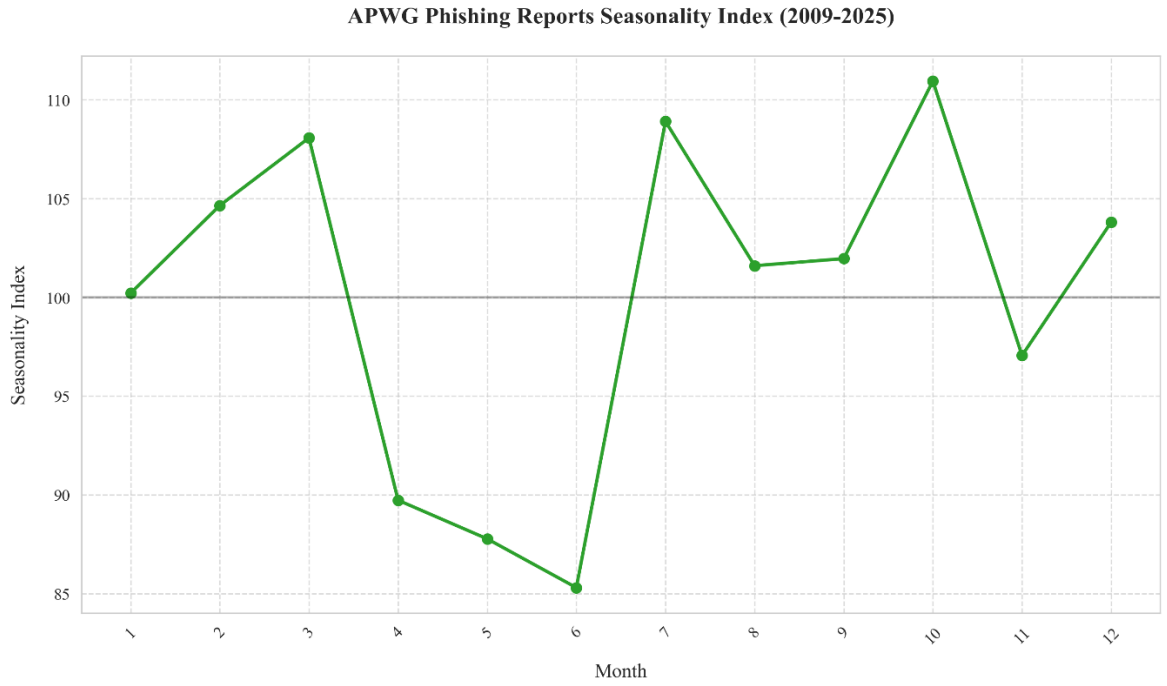


**Fig. 6 Seasonality index of APWG phishing reports in the years 2009–2025. Source: own elaboration.**

The seasonality index of APWG reports (Figure 6) reveals a characteristic pattern in the distribution of phishing attacks throughout the calendar year. The highest activity was recorded in October (index 111), while a clear decline occurs in the spring-summer period, reaching a minimum in June (index 84). A secondary peak of activity was also observed in March (index 108), followed by a sharp decline. This pattern differs from the seasonality observed in PhishTank data, which may result from different data collection methodology and APWG's focus on phishing campaigns distributed via email.

The conducted statistical analysis of APWG data using the Mann-Kendall test reveals significant differentiation of trends depending on the analyzed period. For the full research period, no statistically significant trend was found ($\tau = 0.025$, $p = 0.597$), which indicates relative stability of the phenomenon in the long-term perspective.

Detailed analysis of sub-periods provides a more complex picture. In the period before 2015, no significant trend was also observed ($\tau = 0.142$, $p = 0.079$), while for the years 2015–2025 the test showed a strong downward trend ($\tau = -0.486$, $p < 0.001$). This significant change in trend direction after 2015, confirmed by a high Z statistic value (−8.062), may suggest a fundamental change in the dynamics of phishing attacks or in the methodology of their detection and reporting.

## CERT Polska

Analysis of data from CERT Polska in the years 2010–2024 (Figures 7 and 8) reveals an extremely dynamic increase in phishing incidents in the years 2015–2017, with an unprecedented peak in 2015 (881,504 incidents). The Mann-Kendall test did not show an overall statistical trend in the entire examined period ($\tau = 0.295$, $p = 0.138$), which can be attributed to high data variability.

Particularly interesting is the year-to-year growth dynamics, which shows a dramatic jump of over 800% in 2015, after which an equally sharp decline to levels closer to historical values occurred. Since 2018, relative stabilization of the number of incidents has been observed, with moderate increases in the years 2022–2024. This characteristic dynamics may suggest both changes in data collection methodology and potential single, widespread phishing campaigns in the years 2015–2017.

The observed increase in phishing incidents in Poland during 2022–2024 warrants particular attention in the geopolitical context. Poland's geographic proximity to Ukraine and its significant role in supporting Ukrainian defense efforts since February 2022 may have positioned it as a secondary target for cyber operations (Chmielewski, 2025). The increase in reported incidents during this period could reflect intensified cyber-attack activities directed at Polish infrastructure, government institutions, and citizens, potentially as part of broader

information warfare campaigns associated with the Russia-Ukraine conflict. This hypothesis aligns with documented patterns of cyber operations targeting NATO member states providing substantial support to Ukraine.

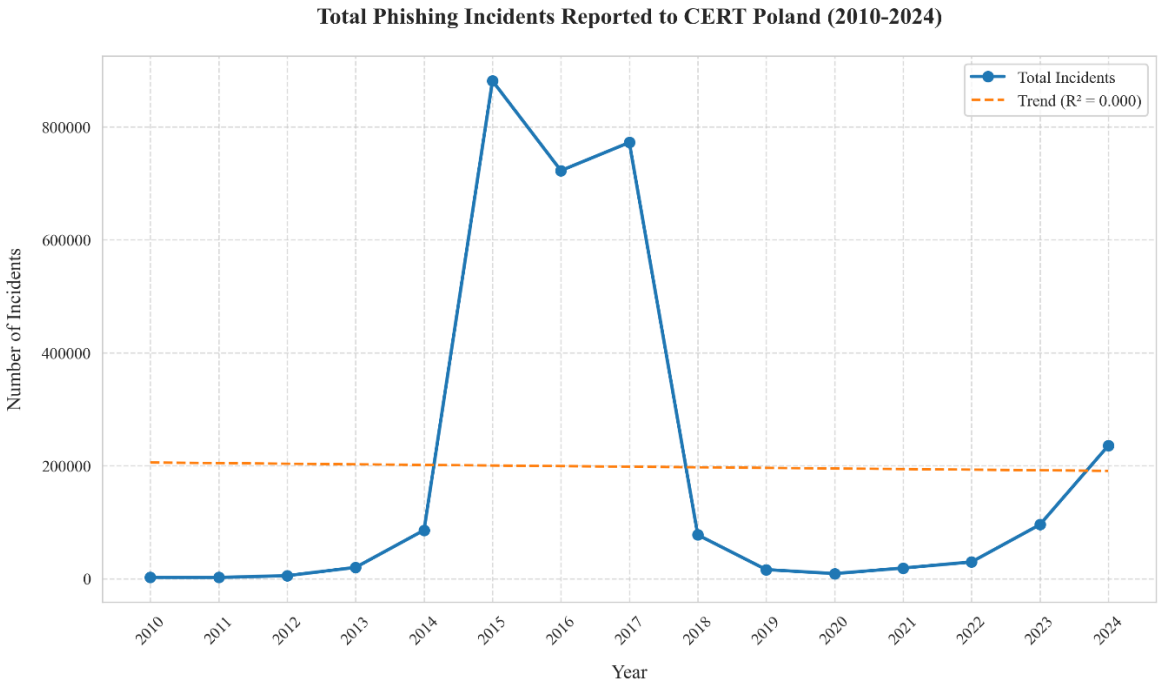


**Fig. 7 Number of phishing incidents reported to CERT Polska (2010–2024) with trend line (R2 = 0.001). Source: own elaboration.**

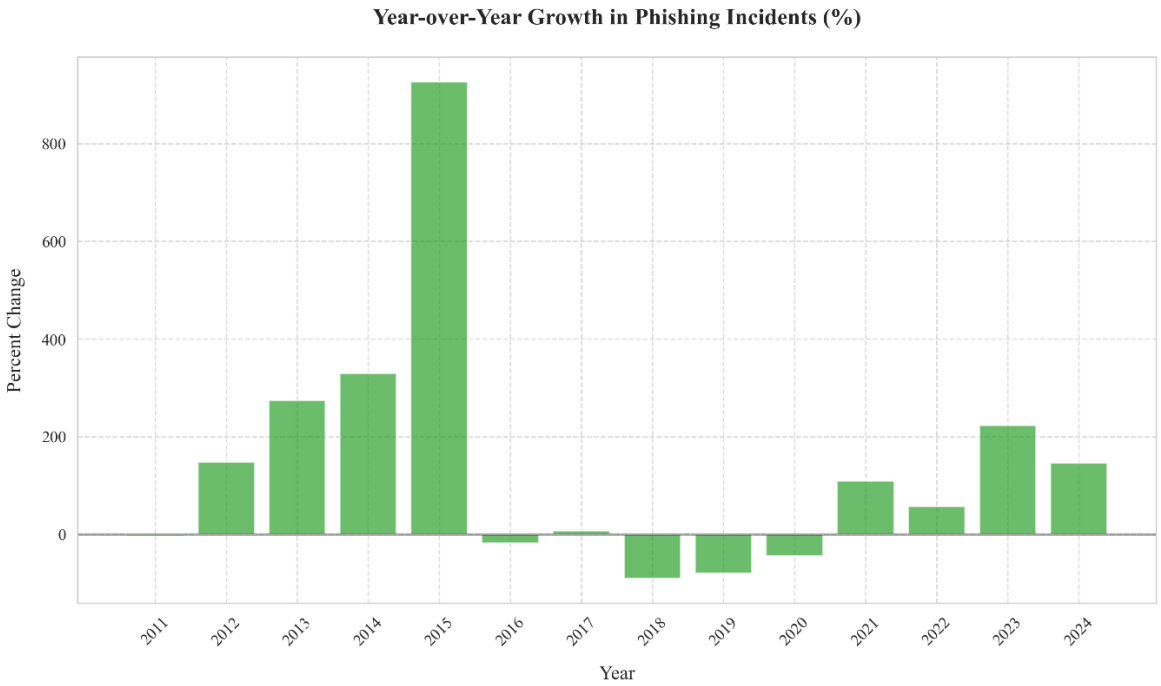


**Fig. 8 Annual percentage growth of phishing incidents reported to CERT Polska (2010–2024). Source: own elaboration.**

## Summary

The conducted comparative analysis of three phishing threat data sources reveals a complex picture of the evolution of this phenomenon in the years 2009–2024 (Figure 9). In the initial period, up to 2012, the level of

incidents remained relatively stable and low in all sources. PhishTank was the first source to register an increase in activity, beginning an upward trend in 2012.

The breakthrough moment turned out to be the period 2015–2016, when all three sources recorded an unprecedented increase in the number of incidents, reaching maximum values in their measurements. This synchronous increase, confirmed by independent sources, constitutes strong evidence for the actual intensification of phishing activity in this period.

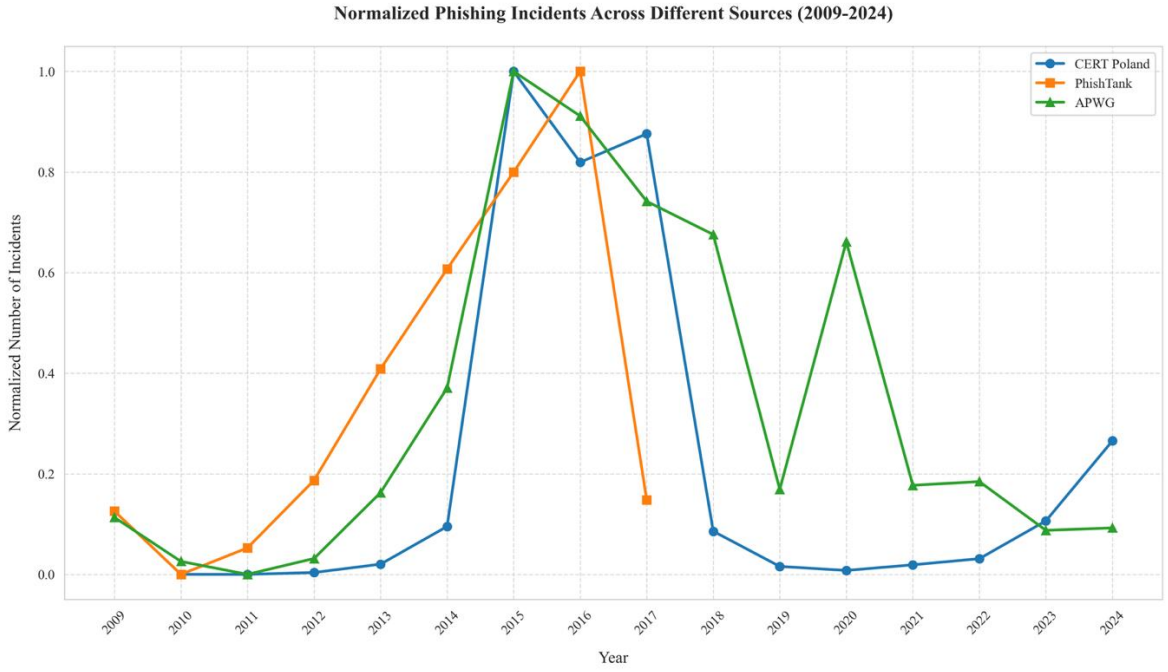


**Fig. 9 Normalized number of phishing incidents reported by CERT Polska, PhishTank, and APWG in the years 2009–2024. Source: own elaboration.**

After 2016, each source presents different downward dynamics. PhishTank showed the sharpest decline, CERT Polska was characterized by a gentler downward trend, while APWG recorded the most gradual decrease in activity. This divergence may result from methodological differences in data collection and focus on different aspects of phishing threats.

The final period of analysis (2020–2024) indicates stabilization of the phenomenon at a level significantly lower than in the peak period, with APWG still recording periodic increases in activity. This stabilization may suggest both the effectiveness of defensive mechanisms and the potential evolution of criminal tactics toward more sophisticated forms of attacks, more difficult to detect and classify in traditional monitoring systems.

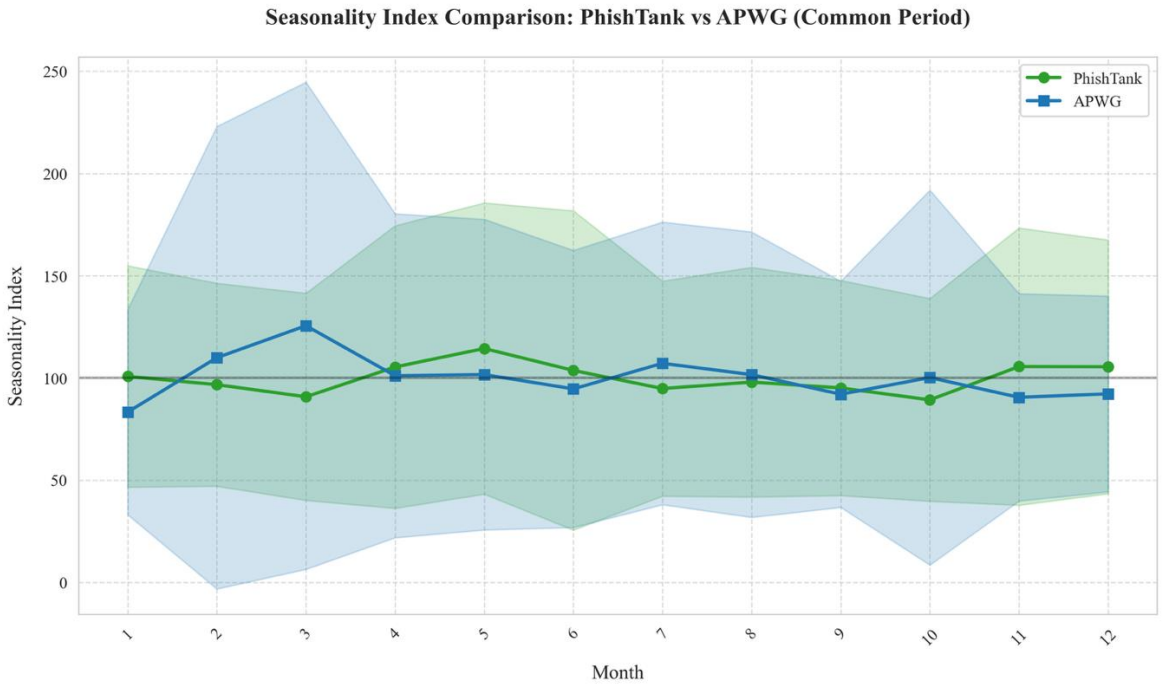


**Fig. 10 Comparison of seasonality index of phishing reports in PhishTank and APWG databases in monthly terms. Source: own elaboration.**

The large standard deviation of PhishTank and APWG seasonality indices (Figure 10) indicates instability of the seasonal pattern, which constitutes a contradiction to claims frequently found in the literature about seasonality (especially in the pre-holiday period) of these attacks.

The temporal heatmap analysis (Figures 11 and 12) provides granular visualization of phishing incident intensity across the examined period. The visualizations clearly demonstrate the concentration of high-intensity periods during 2015–2016 in both databases, with APWG showing particularly elevated activity extending through early 2017. The heatmaps reveal that peak activity was not uniformly distributed across all months, but rather concentrated in specific temporal windows. Post-2016 cooling patterns are visually evident in both sources, though APWG exhibits more persistent elevated activity in isolated months during 2019–2021 compared to PhishTank's more consistent decline. The absence of pronounced vertical banding (consistent monthly patterns across years) further confirms the limited role of seasonality in driving long-term trends, supporting the statistical findings regarding seasonal pattern instability.

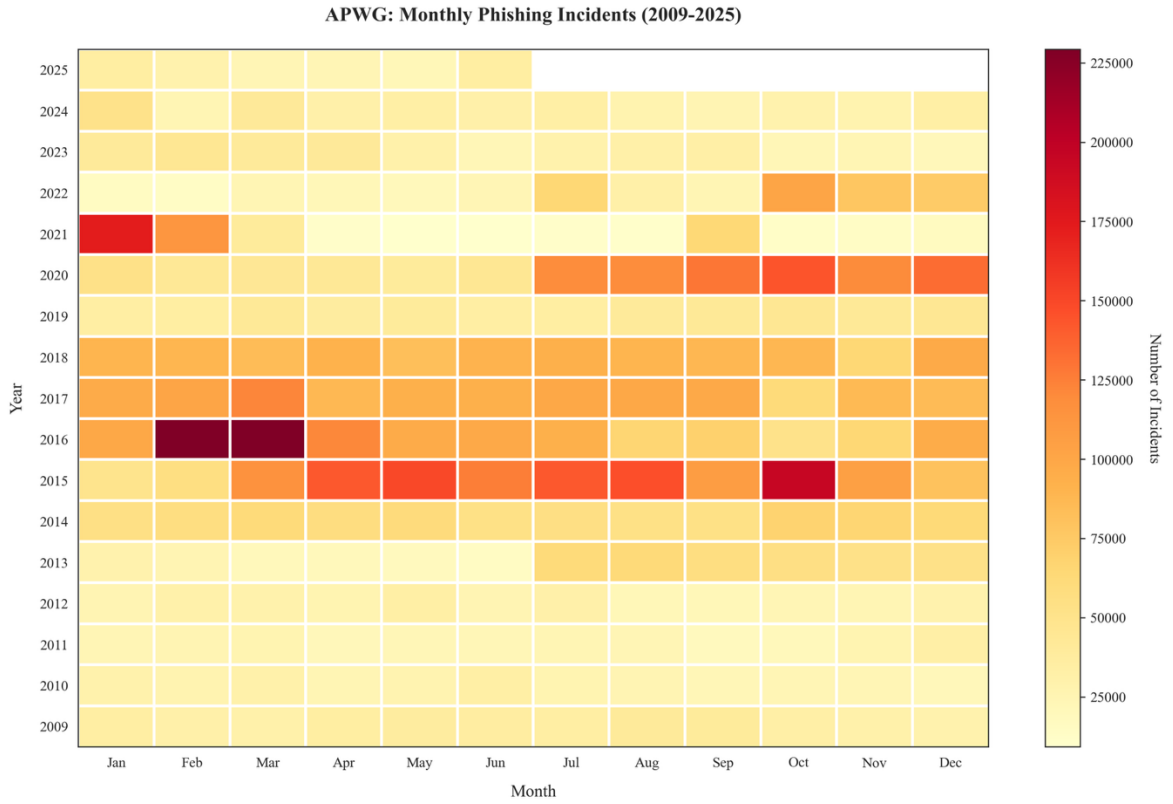


**Fig. 11 APWG: Monthly phishing incident intensity heatmap (2009–2025). Darker colors indicate higher incident volumes. Source: own elaboration.**

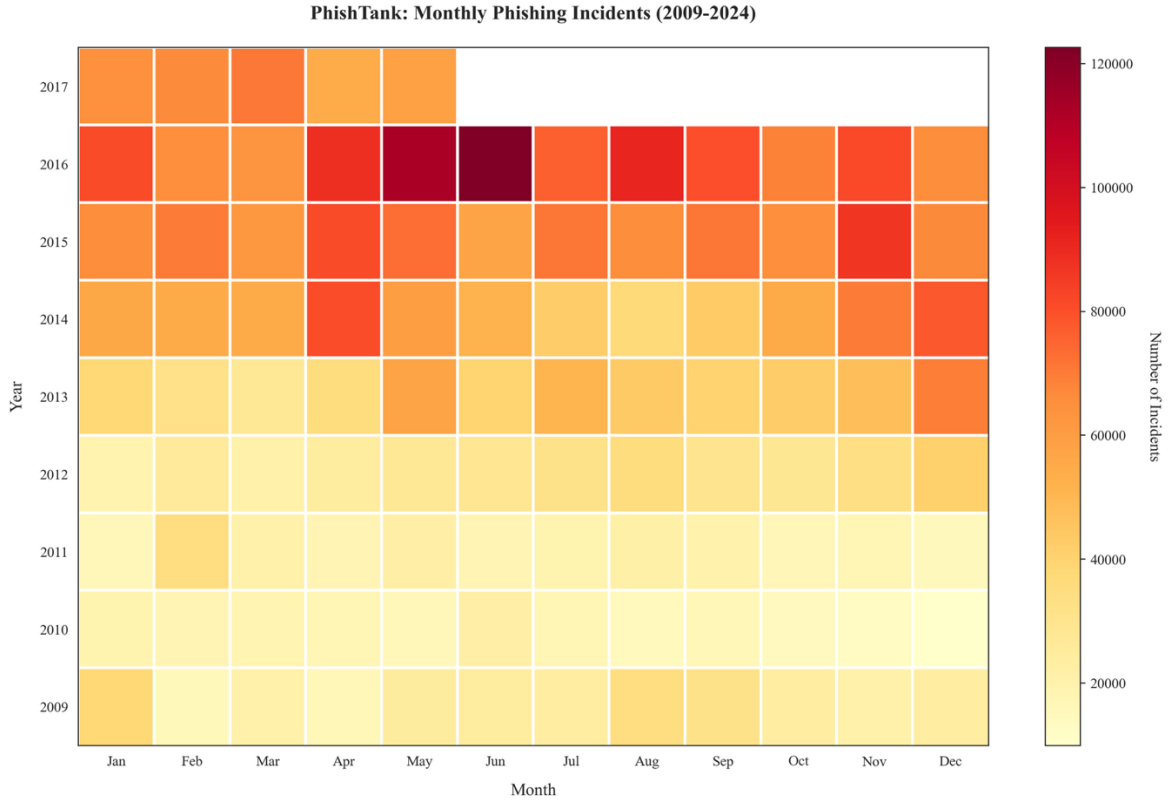


**Fig. 12 PhishTank: Monthly phishing incident intensity heatmap (2009–2024). Darker colors indicate higher incident volumes. Source: own elaboration.**

**Table 2: Correlation between the number of phishing reports from three independent sources (CERT Polska, PhishTank, APWG) in the years 2010–2017.**

| | CERT Polska | PhishTank | APWG |
|---|---|---|---|
| CERT Polska | 1.000000 | 0.584479 | 0.965871 |
| PhishTank | 0.584479 | 1.000000 | 0.756965 |
| APWG | 0.965871 | 0.756965 | 1.000000 |

The conducted correlation analysis between the number of phishing reports from different sources reveals that there are strong dependencies between these data, which may suggest their consistency.

## Conclusions

This empirical study systematically examined phishing trends across three major anti-phishing databases spanning 2009–2025, providing robust evidence that challenges the widespread narrative of continuously escalating phishing threats. Through rigorous statistical analysis employing Mann-Kendall trend tests and seasonal decomposition methods on 2.3 million phishing incidents, we address the research questions formulated at the outset of this investigation.

### Response to Main Research Question

The main research question examined whether empirical data confirms the commonly accepted thesis of systematic growth in phishing threats. Our findings reveal a considerably more complex reality than suggested by prevailing assumptions. Rather than demonstrating uniform exponential growth, the data exhibit significant divergence between sources and distinct temporal phases. PhishTank data (2009–2017) shows statistically significant upward trends ($\tau = 0.656$, $p < 0.001$), while APWG demonstrates the opposite pattern with a strong downward trajectory ($\tau = -0.486$, $p < 0.001$). CERT Polska exhibits extreme volatility without statistically significant long-term trends ($\tau = 0.295$, $p = 0.138$). These contradictory patterns fundamentally question the validity of blanket assertions about continuously escalating phishing threats.

### Response to Detailed Research Questions

Regarding the dynamics of phishing incidents, our analysis identified multiple temporal regimes rather than a single coherent trend. Seasonality analysis revealed modest monthly variations (indices ranging 85–115), but with high standard deviations indicating pattern instability. This contradicts claims frequently found in literature about pronounced seasonality in phishing attacks.

External factors analysis revealed important contextual dependencies. Notably, CERT Polska's increase during 2022–2024 may reflect geopolitical factors, specifically cyber operations associated with the Russia-Ukraine conflict and Poland's proximity to the conflict zone.

### Key Contributions

This study makes several important contributions to the cybersecurity literature. First, it provides the most comprehensive longitudinal analysis of phishing trends to date, spanning 16 years and multiple independent data sources. Second, it demonstrates through rigorous statistical methods that commonly cited claims of exponential phishing growth lack empirical support when examining actual reported incidents. Third, it reveals critical gaps in current threat intelligence infrastructure, evidenced by contradictory trends across supposedly authoritative sources. Fourth, it identifies methodological challenges in phishing measurement that must be addressed to enable evidence-based policymaking.

### Study Limitations

Several limitations must be acknowledged. The temporal coverage varies across sources, with PhishTank data availability limited to 2009–2017, potentially biasing trend interpretations. Geographic biases exist, as CERT Polska represents only Polish incidents, though its high correlation with global APWG data suggests broader

applicability. Definitional inconsistencies across databases remain unresolved – what constitutes a reportable phishing incident likely varies between crowdsourced platforms (PhishTank) and institutional reporting systems (APWG, CERT Polska). Finally, our analysis captures reported incidents, which represent an unknown fraction of actual phishing attempts, and this reporting rate may itself vary over time.

### Future Research Directions

Future research should pursue several critical directions. First, investigating the methodological divergence between databases through direct comparison of incident classification criteria and reporting workflows. Second, estimating the "dark figure" of unreported phishing through survey-based victimization studies. Third, analyzing phishing attack sophistication metrics beyond simple volume counts, potentially revealing quality-versus-quantity trade-offs in attacker strategies. Fourth, examining regional variations in phishing patterns to assess whether observed trends reflect global phenomena or artifacts of measurement locations. Fifth, developing unified measurement frameworks that enable meaningful cross-database comparisons and longitudinal trend analysis.

## Implications

The observed trends carry significant implications for cybersecurity practice and policy development. Most critically, the documented decline in reported incidents does not necessarily indicate reduced threat severity. Rather, this pattern strongly suggests an evolution in attacker strategies from mass, indiscriminate campaigns toward more targeted, sophisticated operations. This interpretation aligns with observations in recent literature (Magdziarz, 2024) regarding the increasing sophistication of social engineering attacks.

Traditional mass phishing campaigns are increasingly detectable by automated defense mechanisms, spam filters, and user awareness training. However, this defensive success may create misleading security perceptions. Contemporary attackers employ precision targeting and multi-stage approaches that evade traditional detection while causing disproportionate damage.

### Concluding Remarks

The cybersecurity community must recognize that observed declining incident volumes may reflect attacker adaptation rather than reduced threat severity. Defense strategies must evolve to address this shift, incorporating sophisticated detection capabilities, revised metrics frameworks, and interdisciplinary approaches that account for the convergence of traditional cyber-attack vectors with advanced social engineering techniques.

## Acknowledgments

This work was financed by Military University of Technology under research project UGB 531-000023-W500-22.

## References


- Abroshan, H., Devos, J., Poels, G., and Laermans, E. COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic. In: *IEEE Access* 9,
- pp. 121916–121929. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3109091. (Visited on 01/21/2025).
- *Aktualności - UODO* (2025). https://uodo.gov.pl/pl/138/2765. (Visited on 01/21/2025). Aldawood, H. and Skinner, G. An Advanced Taxonomy for Social Engineering Attacks. In: *International Journal of Computer Applications* 177.30, pp. 1–11. ISSN: 09758887. DOI: 10.5120/ijca2020919744. (Visited on 01/21/2025).
- Aleroud, A. and Zhou, L. Phishing Environments, Techniques, and Countermeasures: A Survey. In: *Computers & Security* 68, p. 160. ISSN: 0167-4048. DOI: 10.1016/j.cose.2017.04.006. (Visited on 01/21/2025).
- APWG | Unifying The Global Response To Cybercrime (May 2024). (Visited on 01/22/2025).
- Chmielewski, M. Countering Hybrid Threats and Developing Cyber Resiliance for NATO's Eastern Flank. Polish Cyber Com Perspective. DOI: 10.13140/RG.2.2.19092.82564.
- Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., and Costabile, M. F. Human Factors in Phishing Attacks: A Systematic Literature Review. In: *ACM Computing Surveys* 54.8, 173:4–173:6. ISSN: 0360-0300. DOI: 10.1145/3469886. (Visited on 01/21/2025).

- Dou, Z., Khalil, I., Khreishah, A., Al-Fuqaha, A., and Guizani, M. Systematization of Knowledge (SoK): A Systematic Review of Software Based Web Phishing Detection. In: *IEEE Communications Surveys & Tutorials* PP. DOI: 10.1109/COMST.2017.2752087.
- Frąszczak, E. and Frąszczak, D. *A Review of a Website Phishing Detection Taxonomy*. DOI: 10.6084/m9.fig share.26345473.
- *Internet Crime Complaint Center (IC3) | Business Email Compromise The $26 Billion Scam* (2025). https://www.ic3.gov/PSA/2019/PSA190910. (Visited on 01/21/2025).
- Karamagi, R. A Review of Factors Affecting the Effectiveness of Phishing. In: *Computer and Information Science* 15, pp. 21–22. DOI: 10.5539/cis.v15n1p20.
- *Krystianmagdziarz/Phish-Stats* (2025). https://github.com/krystianmagdziarz/phish-stats/tree/main. (Visited on 11/26/2025).
- *Linregress — SciPy v1.15.1 Manual* (2025). URL: https://docs.scipy.org/doc/scipy/reference/generated/scipy.stats.linregress.html (visited on 01/27/2025).
- Magdziarz, K. *The Role of Marketing Strategies in Cyber-Attack Executions*. Vol. 43. DOI: 10.6084/m9.figs hare.30723950.
- Magdziarz, K. *Github Repository (Add_trendline Function)*. URL: https://github.com/krystianmagdziar z/phish-stats/blob/main/phishtank/generate%5C_graphs.py%5C#L60 (visited on 01/27/2025).
- *Mann-Kendall Test | Real Statistics Using Excel* (2025). https://real-statistics.com/time-series-analysis/time- series-miscellaneous/mann-kendall-test/. (Visited on 01/22/2025).
- Matacz, M. and Vodičková, W. Zjawisko phishingu w Polsce. In: *De Securitate et Defensione. O Bezpieczeństwie i Obronności* 9.1, pp. 118–119. ISSN: 2450-5005. DOI: 10.34739/dsd.2023.01.09. (Visited on 01/21/2025).
- *Matplotlib Documentation — Matplotlib 3.10.0 Documentation* (2025). URL: https://matplotlib.org/stab le/index.html (visited on 01/27/2025).
- *Phishing Attacks Escalation* (Oct. 2024). *Phishing Attacks Escalation: Trends And Statistics Analysis*. https://teckpath.com/the-rising-threat-of-phishing-attacks-statistics-and-trends-over-the-latest-years/. (Vis- ited on 01/21/2025).
- *PhishTank | Join the Fight against Phishing* (2025). https://phishtank.org/. (Visited on 01/22/2025).
- Polska, C. Raport Roczny z Działalności CERT POLSKA.
- *Publikacje CERT Polska* (2025). https://cert.pl/publikacje/. (Visited on 01/22/2025).
- Zimoń, M. and Kasprzyk, R. Digital Revolution and Cyber Threats as Its Consequence.