appgate

PROACTIVE PHISHING NEUTRALIZATION AND BEST PRACTICES FOR FRAUD PREVENTION IN 2024

The battle against phishing scams is intensifying, with attackers leveraging AI to create increasingly sophisticated threats. Appgate's Security Operations Center (SOC) is at the forefront of this fight, continuously monitoring and responding to cyberattacks, and here's an overview of the top fraud attack types in the first half of 2024, as well as how we're achieving record-breaking phishing neutralization times.

The cyberthreat landscape is rapidly evolving, fueled by the increasing use of artificial intelligence (AI) by attackers. This technology enables them to expand their attack surface and create sophisticated phishing scams that mimic legitimate websites with alarming accuracy. Phishing remains a primary tool for cybercriminals seeking to harvest sensitive information for fraud and identity theft. Staying informed and proactive is critical in this escalating threat environment.

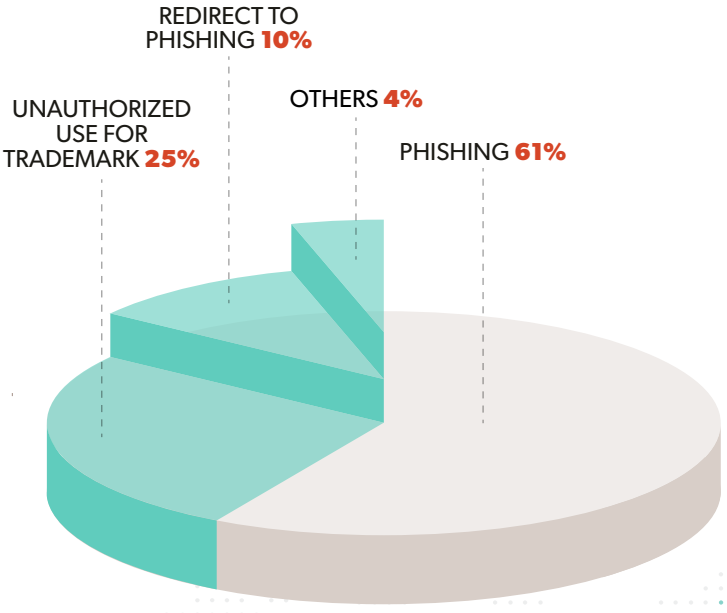
Our Security Operations Center (SOC) team is on the front lines, constantly monitoring and analyzing both cutting-edge and traditional cyberattacks. We rely on these key metrics to measure our performance and prioritize our efforts. In our most recent report, we uncovered and explored the most common types of attacks in 2023, as well as the year-over-year attack trends. This blog will provide an overview and analysis of our attack response, proactive measures and incident deactivation times for the first half of 2024.

FRAUD ATTACK TYPES IN H1 2024

During the first half of 2024, we surpassed **20,000 fraud deactivations,** underscoring our commitment to protecting our customers. We achieved this by implementing automated solutions that significantly enhanced our operational efficiency.

Top Fraud Attack Types:

- Phishing 61%
- Unauthorized use of trademarks 25%
- Redirect to Phishing Pages 10%
- Others 4%



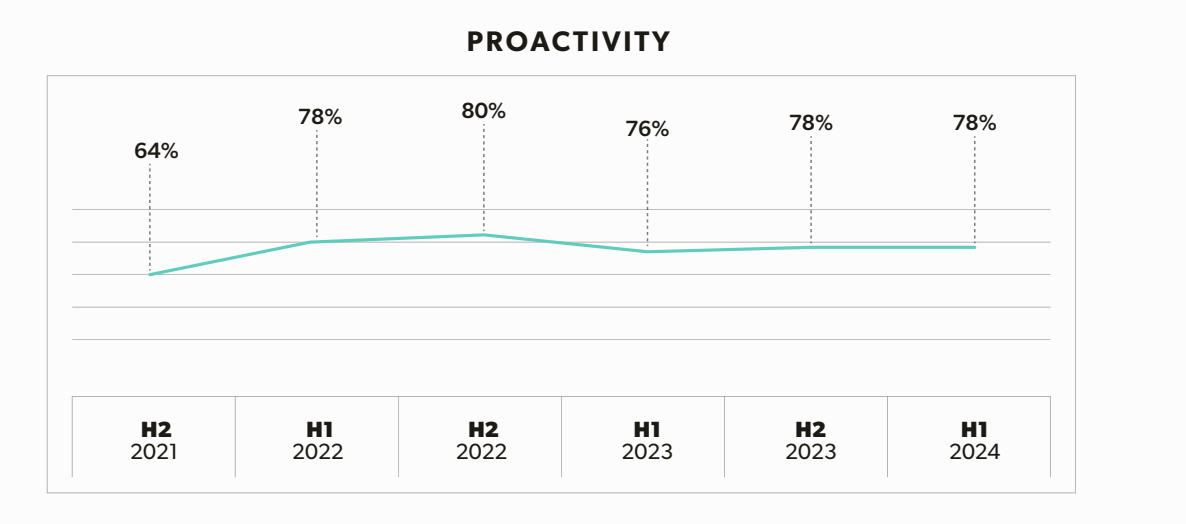
ENHANCING PROACTIVE PHISHING DETECTION CAPABILITIES

The Appgate SOC has significantly enhanced its proactive detection capabilities for phishing and fake profiles, **achieving an average proactivity rate exceeding 78%** in recent years. These improvements have resulted in greater efficiency and accuracy in identifying and mitigating threats.

Key enhancements include:

- **Vendor collaboration:** We actively collaborate with multiple vendors to rigorously test and refine our detection capabilities, ensuring we remain at the forefront of phishing prevention.
- **Automated phishing analysis:** By significantly improving our automated phishing analysis capabilities, we can now enable a faster and more effective response to reactive phishing incidents.
- **Optimized monitoring automation:** We have optimized our monitoring automation processes, leading to a substantial increase in the accuracy of phishing detection and identification of fake social media profiles.

These ongoing efforts demonstrate our commitment to proactively safeguarding our environment from the evolving threat of phishing attacks. Let's examine the growth of our proactive detection capabilities over time:



RAPID PHISHING NEUTRALIZATION: A TESTAMENT TO PROACTIVE CYBERSECURITY

In the first half of 2024, **we achieved a remarkable 70% success rate in disabling phishing attempts within 0 to 5 days**. This rapid response time significantly mitigates the potential damage of these attacks, safeguarding sensitive data and operational integrity. This advance not only demonstrates our technical capacity but is also a testament to the dedication of our cybersecurity experts and the effectiveness of our collaborative approach, which enables us to proactively adapt to the ever-evolving digital fraud landscape.

As the global costs of data breaches continue to escalate, with an average cost approaching $5 million according to the recent IBM and Ponemon Institute report, it is clear that adopting advanced technologies such as artificial intelligence and automation is crucial. Phishing remains a major vector for initiating these breaches, underscoring the importance of proactive defense mechanisms. At Appgate, we integrate these technologies into our 360 Fraud Protection suite to reduce breach costs and enhance real-time detection, ensuring that our clients not only respond swiftly to threats but also prevent incidents before they escalate into major issues.

OUR COMMITMENT TO CONTINUOUS IMPROVEMENT

The first half of 2024 reaffirmed the importance of maintaining proactive and efficient cyber threat detection. Through automation enhancements and strong vendor partnerships, we have achieved a significant reduction in response times, enabling our SOC team to identify and neutralize attacks with greater accuracy.

As threats continue to evolve, we remain committed to strengthening our defenses, focusing on the most vulnerable regions and attack techniques. We will continue to refine our strategies to exceed customer expectations, ensuring their data is protected and their confidence in our cyber risk management capabilities remains strong.

Appgate remains steadast in its commitment to innovation and security, and we encourage organizations to join us in the fight against fraud to ensure a secure future for all.

To learn more about Appgate's threat advisory, secure access and anti-fraud solutions, visit our Demo Hub. (https://www.appgate.com/resources/fraud-protection)