SOLUTION BRIEF

HYAS **PROTECT**

How to Stop Phishing Attacks with Protective DNS

Phishing Threats Are Increasing In Scale and Sophistication

Phishing remains one of the most dangerous and widespread cybersecurity threats. This brief examines the escalating phishing landscape, shortcomings of common anti-phishing approaches, and why implementing a Protective DNS service as part of a layered defense provides the most effective solution.

Phishing is now the most common initial attack vector, overtaking stolen or compromised credentials.[1] Stolen or compromised credentials was the leading attack vector in the prior year's report.

According to recent research, the number of phishing attacks vastly outpaces all other cyber threats. Business Email Compromise (BEC), a type of phishing attack, results in the greatest financial losses of any cybercrime.

In 2021 alone, estimated adjusted losses from BEC totaled $2.4 billion USD globally.[2] This staggering figure represents more than 59 percent of the losses from the top five most costly internet crimes worldwide. These statistics highlight the immense threat posed by phishing, especially BEC attacks, to organizations across industries.

Phishing continues to dominate the Social Engineering incident classification pattern, ensuring that email remains one of the most common and easiest means of influencing individuals in an organization. These trends demonstrate how phishing remains one of the most pervasive and costly cyber threats facing businesses today.

> **According to recent research, the number of phishing attacks vastly outpaces all other cyber threats.**

Sources: [1]IBM Security: Cost of a Data Breach Report 2023, [2]Microsoft Digital Defense Report 2022, [3]2023 Verizon Data Breach Investigations Report

Phishing Attacks are Evolving, Improving and Automating

Phishing attacks are becoming more targeted. Phishing attackers are increasingly using social engineering techniques to personalize their attacks and target specific individuals or organizations. For example, attackers may research their victims on social media or other online sources to gather personal information that can be used to make their phishing emails more believable.

> **Phishing attackers are using increasingly sophisticated techniques to evade detection by traditional security solutions.**

Phishing attacks are becoming more difficult to detect. Phishing attackers are using increasingly sophisticated techniques to evade detection by traditional security solutions. For example, attackers may use domain spoofing techniques to create websites that look like legitimate websites, or they may use malware to inject malicious code into legitimate websites.

Phishing attacks are becoming more automated. Phishing attackers are increasingly using automation tools to scale their attacks. This allows them to send millions of phishing emails per day, making it difficult for organizations to keep up.

These trends make it clear that phishing attacks are becoming increasingly threatening to businesses of all sizes. Organizations need to implement a layered security approach that includes Protective DNS to effectively protect themselves from phishing attacks.

Why Existing Anti-Phishing Measures Fall Short

Organizations employ various methods to combat phishing, but limitations remain:

1. **Email Filtering** relies on signatures, display names, and content inspection.
2. **Blacklisting URLs** fail to keep pace as phishers exploit typosquatting and generate new fraudulent domains rapidly.
3. **User Education** is unreliable when faced with highly-refined psychological manipulation tailored to override caution.
4. **Multi-Factor Authentication (MFA)** blocks unauthorized access by requiring an additional factor, but does not stop the phishing attempt itself. Users still access harmful links or attachments.
5. **Business Email Compromise (BEC)** filters focus solely on email while phishing also occurs via web, social media, search, and apps. Other vectors are missed.

These examples demonstrate the need for advanced solutions that reliably block phishing proactively at the lower level before attacks reach end users.

An Evolving Threat Requires Adaptive Defenses

While phishing methods are constantly evolving, common attack vectors include:

Spear Phishing – Highly targeted emails personalized with researched details to appear authentic. Often used to compromise executive and privileged accounts.

Deceptive Domains – Phony websites designed to impersonate and trick visitors into entering login credentials or sensitive data. URL spoofing and typosquatting techniques bypass casual inspection.

Malware Payloads – Malicious attachments or links that install info-stealing malware, ransomware, or remote access Trojans via phishing messages.

Social Engineering – Psychological manipulation triggers emotions like fear, curiosity, or a sense of urgency that override caution.

This combination of highly-tailored social engineering, stealthy technical deception, and harmful payloads allow phishing attacks to circumvent many current defenses. This is where HYAS Protect comes in.

HYAS Protective DNS Provides Superior Phishing Protection

HYAS Protect Protective DNS solution preemptively blocks known phishing sites and domains before requests reach them by focusing on the DNS layer which is a common thread required in most internet interactions. This prevents connections to phishing content at the source, stopping attacks earlier in the kill chain.

Real-Time Blocking – Newly identified phishing sites and emails are blocked instantly across the protected network as they are added to the DNS filter database. No reliance on match lists, signatures, or patterns.

Identifies Emerging Threats Faster – By leveraging our unique adversary infrastructure platform's data lake, Protective DNS services continuously analyze the web to rapidly detect phishing sites as they emerge.

Universal Coverage – Blocks phishing sites regardless of vector—email links, web pages, documents, apps, search engine results, etc.

Difficult to Evade – Blocking based on domain reputation prevents circumvention via display name spoofing, content changes, or social engineering.

For example, a phishing email slips past the corporate email gateway defenses. But when the embedded link is clicked, HYAS Protect recognizes the destination domain as fraudulent based on real-time threat intelligence and blocks access. The user's device never connects to the phishing site.

This unique ability to reliably stop phishing attacks prior to interaction establishes HYAS Protect as an essential anti-phishing technical control.

HYAS Protective DNS Provides Proactive Defense

As phishing threats accelerate, organizations can no longer rely solely on reactive methods like email filtering, URL blacklisting, or end user discretion. Businesses need proactive Protective DNS solutions to reliably block phishing at the source before attacks reach and fool users.

Anchoring your anti-phishing defenses with HYAS Protect Protective DNS and layered security provides comprehensive protection against this dangerous and constantly evolving threat.

A Layered Defense-in-Depth Strategy

While Protective DNS serves as the foundation for blocking phishing proactively, incorporating additional safeguards provides defense-in-depth. This blend of human and technical measures provides overlapping protection across potential phishing vectors, including:

Email Security – Safelisting, impersonation analysis, attachment sandboxing

Access Controls – Multi-factor authentication, single sign-on, identity management

Endpoint Protection – Antivirus, endpoint detection and response (EDR)

User Education – Ongoing security awareness training and testing

Incident Response – Rapid containment, investigation and remediation

Penetration Testing – Uncover configuration gaps that may enable phishing

CONTACT US
hyas.com/contact

IDENTIFY AND BLOCK
ATTACKS BEFORE THEY HAPPEN

HYAS PROTECT

HYAS Protect enforces security and blocks command and control (C2) communication used by malware, ransomware, phishing, and supply chain attacks. All the while, it delivers on-demand intelligence to enhance your existing security and IT governance stack.

HYAS

PROTECTING BUSINESSES AND SOLVING INTELLIGENCE PROBLEMS
THROUGH DETECTION OF ADVERSARY INFRASTRUCTURE AND ANOMALOUS COMMUNICATION PATTERNS

HYAS is a world-leading authority on cyber adversary infrastructure and communication to that infrastructure. We help businesses see more, do more, and understand more about the nature of the threats they face in real time. HYAS turns meta-data into actionable threat intelligence, actual adversary visibility, and protective DNS that renders malware inoperable. HYAS's foundational cybersecurity solutions and personalized service provide the confidence and enhanced risk mitigation that today's businesses need to move forward in an ever-changing data environment. Visit for more details.