LayerX

THE DARK SIDE OF PHISHING PROTECTION

Are You as Protected as You Should Be?

THE PHISHING PROTECTION CHALLENGE

The recent years have witnessed a steep rise in the volume and sophistication of phishing attacks, making their part within the overall threat landscape more prominent than ever.

There are two main contributing factors to this rise. The first is the rapidly increasing transition of enterprise applications and workloads to the cloud, placing them just a username and password away from malicious access. That fact, in conjunction with the extreme prevalence of password reuse, significantly increases the potential value of compromised credentials, leading adversaries to target them even more intensively than before.

The second factor is the rapid evolution of web pages' technology, which are far more dynamic and complex objects than they used to be in the past. This enables adversaries to embed advanced attacks in them, in a manner that's extremely hard to detect.

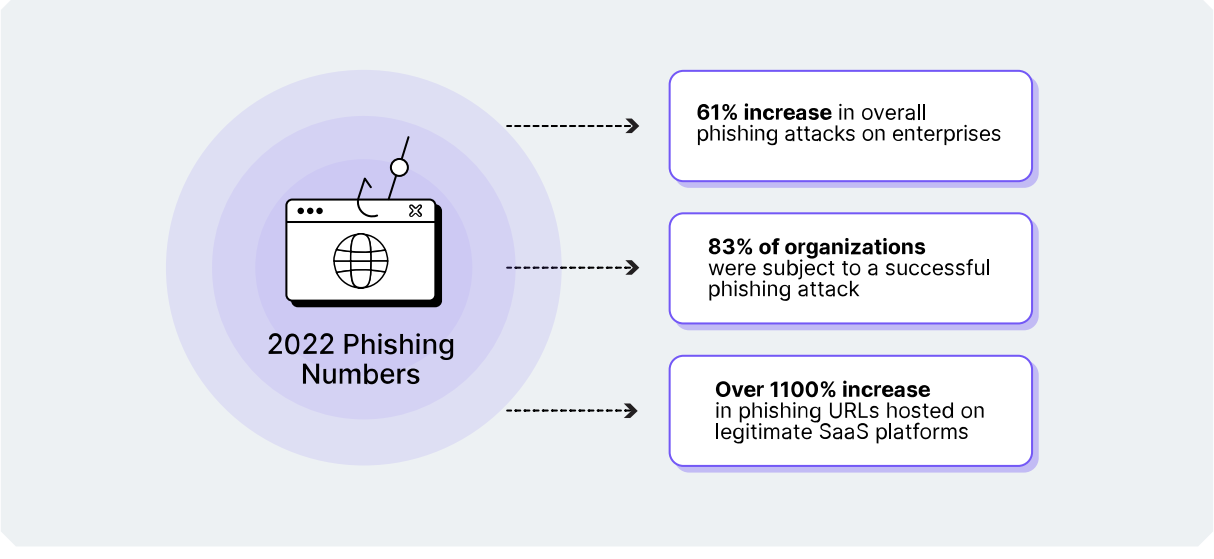
Organizations invest heavily in email protection, firewall rules, and employee education. But these measures aren't delivering the desired results. The number of successful attacks has risen to such a rate that numerous security stakeholders consider phishing one of the top challenges they face.

In this eBook we'll explore the state of phishing attacks today, come to understand the evolution of this attack vector, and review the protections organizations have in place today to prevent them.

The cyber security rule of thumb is that when a certain type of attack thrives, it's a clear indication that there is a blind spot threat actors are taking advantage of. We'll attempt to pinpoint said blind spot and conclude by showing how the new emerging solution category of browser security can address it and provide cloud-first organizations with the resilience they deserve.

PHISHING THREAT ACTORS ARE GAINING THE UPPER HAND

Numbers don't lie, and there is a consensus that both the volume and the success rate of phishing attacks are on the rise. This means that more and more enterprise users are lured into clicking a link, accessing a page, and inserting their credentials. We'll soon dive into why and how this happens. But first, let's contemplate the stats we've gathered from various sources and absorb the magnitude of the problem.



CLOUD-FIRST ENTERPRISES ARE THE TOP TARGETS OF PHISHING ATTACKS

The gradual transit to the cloud is one of the greatest productivity drivers in the modern enterprise. However, as in many other cases, this productivity comes with a security price tag. In the on-prem era, enterprise applications dwelled behind a firewall within the internal network. Today, their SaaS counterparts reside in the public cloud, and all it takes to access them – whether by a legitimate user or malicious threat actor – is a valid pair of credentials.

This introduces a grave challenge to enterprises that adopt a cloud-first mindset and strategy, as their most critical resources reside in the cloud, increasing the severity potential of a successful phishing attack.

A PHISHING ATTACK BREAKDOWN:

WHERE IS THE PROTECTION BLIND SPOT?

Phishing attacks comprise three key parts. Let's see what they are and the level of protection each of them has.

Email Delivery

What is it? Successfully sending maliciously crafted emails to the victim's inbox or through social media, SMS messages, and other productivity tools.

What's the protection? Use an email protection platform to scan email texts and search for any anomalies that can indicate it being a phishing message. In such a case, block it from ever reaching the user's inbox.

Social Engineering

What is it? Luring the user to click the malicious link.

What's the protection? Educate users to treat every incoming message, including email, social media, and the like, with caution. Never assume that being in the inbox implicitly means that the message is legitimate.

Web Access and Credential Theft

What is it? Having the user access the malicious web page and insert his\her credentials.

What's the protection? The blind spot we're looking for is here. Let's dive deeper into the available protections against this final and most critical stage in the phishing attack.

THE THREE ALTERNATIVES TO PROTECTING AGAINST PHISHING PAGE ACCESS

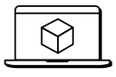
Page Reputation Analysis

Product: Firewall or proxy

How it works: Analyzing the target page's URL by utilizing threat intelligence feeds, as well as calculating its score with various metrics such as the age and the history of the URL, IP reputation, hosting location, website popularity, and others.

Protection gaps: Phishing pages are adding capabilities that intensively void the value of intelligence feeds. Moreover, a large number of phishing attacks utilized are embedded in pages of legitimate SaaS apps.

Result: Partial protection that misses up to 60% of phishing web pages.



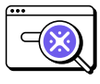
Browser Emulation

Product: Firewall or proxy

How it works: Any suspected web page is executed in a virtual environment that emulates the target browser, to unfold any phishing or other malicious features it embeds.

Protection gaps: Emulation cannot be applied at scale to all the target pages since it can't withstand the throughput. Additionally, executing in a virtual environment is time consuming and creates latency that harms the user experience.

Result: Partial protection that is randomly applied to a limited number of visited pages.



Browser Deep Session Inspection

Product: Browser Security Platform

How it works: Analyzing every live web session from within the browser and inspecting the gradual assembly of the web page to detect phishing behavior, which triggers either session termination or disablement of the phishing component.

Protection gaps: None

Result: Full mitigation of any scenario in which a user was lured to access a phishing page.

BROWSER SECURITY PLATFORM AND DEEP SESSION INSPECTION 101

What is a Browser Security Platform?

Browser Security Platform is an emerging category that was purpose-built to confront web-borne threats. Specifically, it detects phishing pages and either neutralizes their password theft capabilities (if they are hosted on legitimate websites and SaaS apps) or terminates the session altogether. **A browser security platform resides in the browser itself and has real-time visibility, monitoring and policy enforcement capabilities that can be applied to any browsing event using Deep Session Inspection.**

What is Deep Session Inspection?

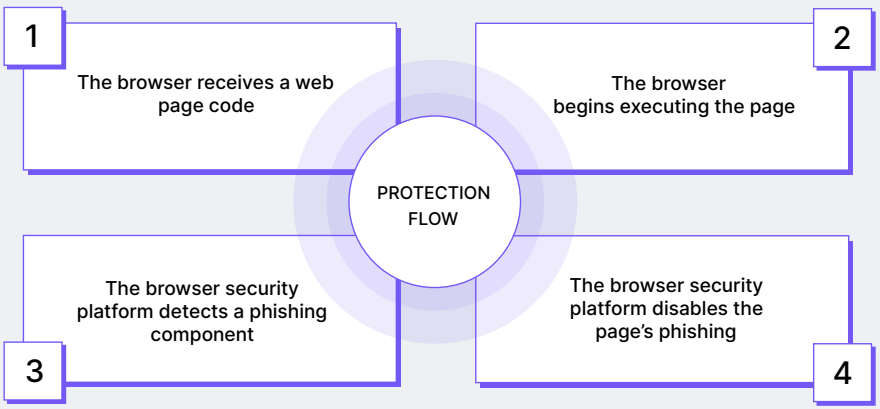
Unlike network traffic analysis that can see the encrypted network layer packets, Deep Session Inspection applies to the unencrypted session within the browser itself. Unlike emulation solutions which phishing pages can recognize and bypass by keeping their password theft behavior dormant, Deep Session Inspection applies to the live rendering of the web page code within the real browser.

ZOOM-IN:

PHISHING PROTECTION WITH BROWSER SECURITY PLATFORM

Let's take a closer look at how the browser security platform delivers its phishing protection.

Once the browser receives the web page's code from the web server or SaaS provider, execution begins. While the common user experience is that a web page is a monolithic object that is activated in a single click, it actually comprises many discrete components that the browser assembles consecutively. The browser security platform monitors each of these components as it loads and applies ML analysis to detect if it discloses indications of phishing behavior. If that's indeed the case, the platform will disable the page's ability to receive user input or even terminate the session altogether.



TURN BROWSER SECURITY PLATFORM INTO THE CORE OF YOUR PHISHING PROTECTION

In an ideal world, you'd have a multi-layered security architecture that places safeguards on every part of the attack kill chain. In real-life, however, you must make choices regarding where to invest your budget and resources.

The placement of the browser security platform at the critical point of where the attack's objective takes place, makes it the only choice that makes sense to start with. Placing additional layers of employee education and email protection is naturally recommended. But these protections should be considered only **after** a browser security platform is already deployed.

The reason is simple worst-case scenario planning. The first solution to choose should be the one that will deliver protection even if all others fail. If an email protection solution fails to flag a certain email as malicious and passes it to the employees' inbox and if the employee fails to avoid clicking the link in an email, social media, or any other delivery method, the browser security platform will still be there to block the attack step that really matters.

THE ESSENTIAL PHISHING PROTECTION SOLUTION CAPABILITIES CHECKLIST

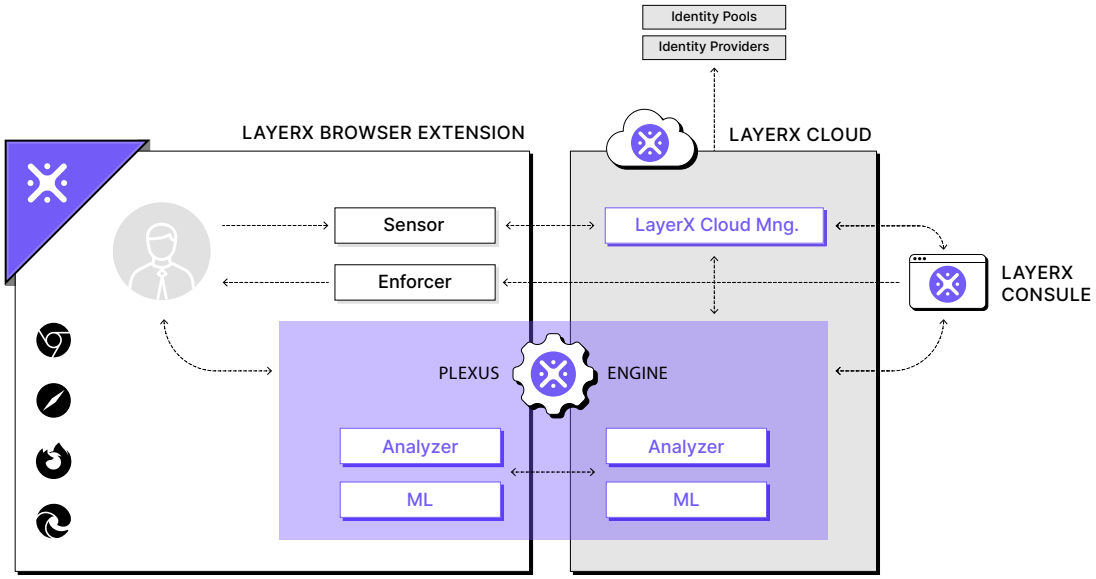
This table summarizes which capabilities the solution you are evaluating for phishing protection should have. While we can go into great detail specifying the granular browsing events that are associated with phishing attacks, we chose to stick to a general, yet inclusive, set of features that can vouch for sound protection.

Protection Capability	Evaluated Solution
Visibility into all browsing events at the application layer	
Monitoring of all browsing events and flagging malicious page behavior	
Detecting, alerting, and preventing password reuse	
Detecting phishing pages that are: • Hosted on high reputation sites • Hosted on compromised WordPress sites	
Triggering the following protective actions per detection of a phishing component in the web page: • Alerting with concrete forensic data to enable a rapid and efficient response from the security team • Disabling the page's password fill capabilities per detection of the phishing page • Preventing the submission of specific sensitive credentials the employee uses • Terminating the page session per detection of the phishing page	
Informing a user when a suspicious web page is detected, providing her/him with ad-hoc awareness enhancements	
Compatibility with any commercial browser	
Minimal interference with the user experience (browsing speed, chirurgic protection actions)	

THE LAYERX WAY:

PROTECT PHISHING FROM WITHIN THE BROWSER

LayerX browser security platform provides dedicated protection against phishing attacks. The LayerX solution is delivered as an extension that can be installed on any commercial browser, providing 360° granular visibility into all browsing events, preventing password reuse, and performing chirurgical removal or disablement of malicious web page components without impacting the overall user experience. To enhance the precision of its phishing detection capabilities, LayerX employs the Plexus engine that combines two parallel risk analysis mechanisms – one on the browser, for analysis of local events, and the other in the cloud, for additional group, company, and global context. These detection capabilities, coupled with the ability to transparently intervene in the web session to resolve risks, can turn any application to practically phishing-immune.

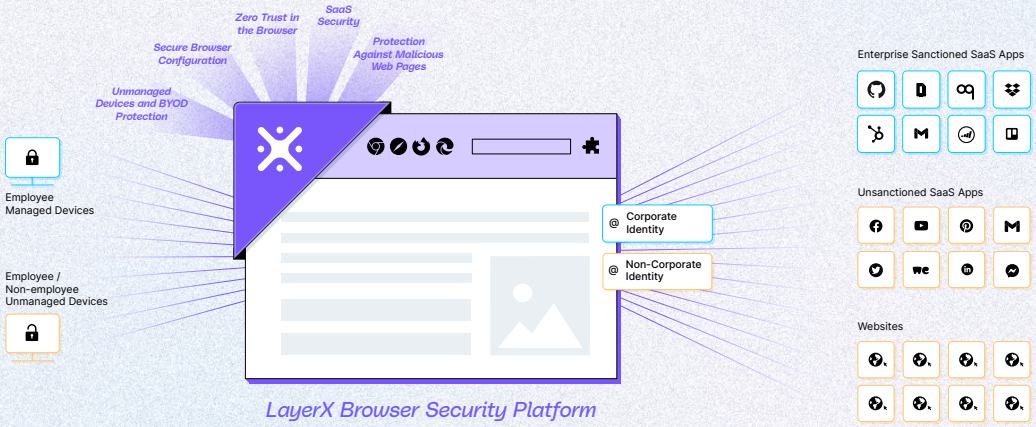


ABOUT LAYERX

LayerX provides a Browser Security Platform that's purpose-built to monitor, analyze, and protect against web-borne cyber threats and data risks. Delivered as a browser extension, LayerX natively integrates with any commercial browser, transforming it into the most secure and manageable workspace. Using LayerX, customers gain comprehensive protection against all threats that either target the browser directly or attempt to utilize it as a bridge to the organization's devices, apps, and data.

LayerX monitors every web-session at its most granular level to detect and disable risky activity at its utmost early stage with near-zero disruption to the user's browsing experience. With LayerX your workforce can securely browse anywhere.

Request Demo



KEY BENEFITS

Eliminate critical blind spots

Gain the most granular visibility into unsanctioned apps, shadow identities, DNS over HTTPS, SaaS apps, and dynamic websites.

Real-time protection

Enforce access & activity policies to restrict browsing activities that expose your apps, devices, and data to compromise.

High-precision risk detection

Multilayered AI analysis of every user activity and web session flags anomalies that can indicate risk in the browser session.

Unified browser management

Manage and configure your workforce's browsers from a single, centralized interface.

Bring your own browser

Enable your users to keep on using their browser of choice for both work and personal use.

Rapid deployment

Deploy across your entire environment and integrate with browser management tools and identity providers in a single click.