



**Zero Trust
Browsing:
Protect your
organization
from its own
users**



Contents

03 Scams come and go:
Human nature remains

05 Phishing sites out-nimble
browser safe modes

06 We have met the enemy,
and he is us

07 Zero Trust Browsing:
What you can't authenticate,
isolate

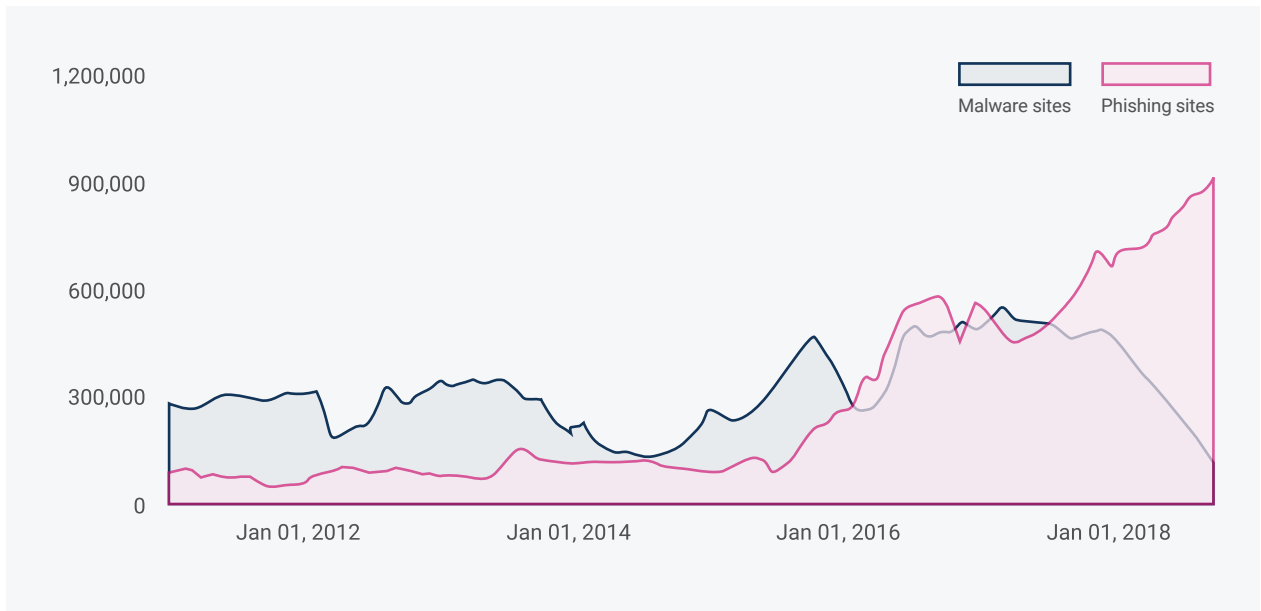
07 Protect users – and your
business -- from their
own errors

Scams come and go: Human nature remains

To the casual observer, the cyberattack landscape is constantly shifting. In recent years, the threats and scams have evolved from Nigerian princes to stranded travelers, pop-ups warning of outdated software to ransomware, cryptojacking, phishing and spear phishing.

Security blogs are full of dire warnings about the very-real explosion of phishing¹, backed by geometric increases in phishing sites as the number of malware sites drops. Just as previous predictions focused on cryptojacking and ransomware was the topic du jour (or de l'année) in earlier years, we're now well into the year of the phish.

Users get smart to individual scams (Nigerian prince emails, anyone?) But our susceptibility to manipulation remains.



Phishing is the top cybersecurity vector, and still growing²



While specific threats wax and wane, the common thread that underlies most is human susceptibility to the social engineering and manipulation at which hackers excel. As users get burned and get wise, and cybersecurity vendors develop relevant defenses, threat actors simply adapt and move on.

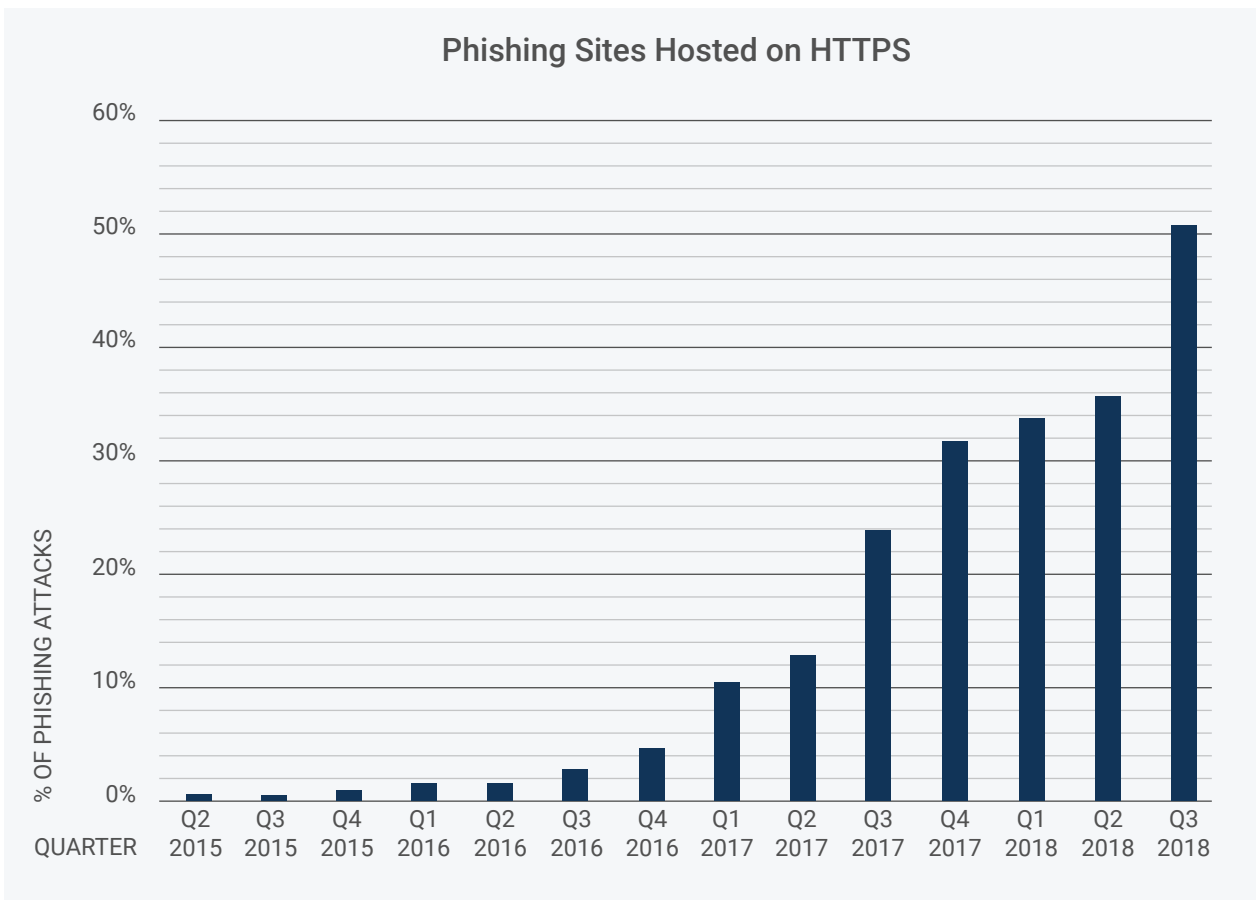
So, for instance, recent data indicates that by September 2018, almost 50% of phishing sites featured the green lock which Chrome uses (or used at the time) to indicate SSL certification, up from about one third at the end of 2017 and just 5% in 2016³.

1) <https://casecurity.org/2018/12/06/ca-security-council-casc-2019-predictions-the-good-the-bad-and-the-ugly/>
 2) Google Transparency report
 3) <https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https>

Phishing sites leverage SSL certification and domain names resembling legitimate URLs to assure susceptible users that entering credentials is just fine.

Hackers are most likely not committed to encrypting the data that unsuspecting visitors enter on phishing sites to protect it. Instead, they quickly realized that many users mistakenly interpret SSL certification as an indication that the site they are browsing is safe. Like domain names that incorporate the URLs of the legitimate sites they imitate, certification is one more way to falsely reassure users that it is safe to enter credentials on a phishing site.

For hackers using phishing techniques that involve enticing users to inadvertently download malware onto the endpoint, SSL/TLS encryption offers the added “benefit” of encrypting malicious payloads. Thus, in an ironic reversal, SSL certification falsely reassures users while shielding malware from the encrypted traffic management systems of many traditional proxy, firewall and IDS/IPS security solutions.






In a cynical twist, cybercriminals certify phishing sites to hide malware from traditional security solutions⁴

Phishing sites out-nimble browser safe modes

URL filtering provided by browsers is too little, too late, to save users from dangerous clicks.

The major browser providers make diligent efforts to save users from their own susceptibility to manipulation by hackers. In the best case, these efforts meet with only partial success. For instance, almost all browsers now offer safe modes that include filtering options, including Google Safe Browsing and Microsoft Smart Screen. In theory, when a user enters the URL of a phishing site, the browser warns him that the site is malicious.

In practice, however, filtering efforts are too little, too late. Edge, Chrome and Firefox take three days to identify, respectively, 98%, 96% and 96% of phishing sites⁵. Edge offered the best performance, identifying 89% of sites on the day they were created, with Chrome and Firefox lagging seriously behind with only 79% and 77% identified. However, given that most phishing sites are put up and taken down within mere hours, even Edge's performance is insufficient at best.

By end of...	% of phishing sites blocked by		
	Microsoft Edge	Google Chrome	Mozilla Firefox
			
1 day	89.0 %	79.0 %	77.0 %
2 day	97.0 %	95.0 %	95.0 %
3 day	98.0 %	96.0 %	96.0 %

Browser categorization is too little, too late: Most phishing sites are taken down within hours⁶

Moreover, URL filtering fails to identify phishing techniques such as keylogging, session hijacking, content injection and malvertising, which leverage legitimate URLs for nefarious purposes. As such, most browser safe modes hardly scratch the phishing attack surface.

Ultimately, browser providers and major cybersecurity vendors will develop technologies to stymie phishing attacks. But by then hackers will have moved on to new and better ways to entrap unsuspecting users.

5) <https://casecurity.org/2018/12/06/ca-security-council-casc-2019-predictions-the-good-the-bad-and-the-ugly/>

6) <https://research.nssllabs.com/reports?cat0=22>

We have met the enemy, and he is us

After years of effort and countless investment in protecting networks and data from outsider attacks, responsible organizations are finally defending from threats from within. While some insider attacks are indeed malicious, many more are the result of human error, “assisted” by sophisticated social engineering tactics.

How can a responsible organization protect its networks and data from falling prey to constantly evolving, highly-effective social engineering attacks?

The answer lies in the Zero Trust precept to “trust no one, verify everything.” The Zero Trust security model was initially proposed in response to a spate of insider data breaches that the widely accepted “castle and moat” approach to security was powerless to stop. Companies’ increasing tendency to spread their systems and data across cloud service providers and mobile devices also makes applying traditional security controls more difficult than ever before.

The Zero Trust approach to securing organizational assets and networks requires every person and/or device to be validated and authenticated to access each resource. Microsegmentation stops the spread of malicious agents, should they get in.

Social engineering attacks exploit their targets’ trust.



Internet use is the antithesis of Zero Trust. Each time a user browses a site, he is trusting that it will do him no harm.

While Zero Trust has proven effective for protecting organizational data, systems and assets, it is nearly impossible to apply to internet use. The internet is by definition, an amorphous and highly dynamic content sprawl, which businesses and the individuals who work for them use in myriad, not-always-predictable ways. Each time a user browses a site, he trusts that it will do him no harm.

Limiting user access to a strictly defined set of sites impairs productivity and is most likely ineffective at preventing attacks, since even legitimate sites can be infected with malware. Yet as we have seen, no enterprise should rely on users to reliably avoid questionable sites and clicks.

Zero Trust Browsing: When you can't authenticate, isolate

Websites cannot be verified safe in real time. Hence, they simply shouldn't be trusted.

To protect organizations – and users themselves – from the dangers of websites infected with malware or malicious payloads, the Zero Trust mantra must be taken still further, to “trust no one – full stop.” Since most websites cannot be verified as safe in real time, the sites, including attachments and payloads, simply shouldn't be trusted.

Unlike detection-based solutions, such as anti-virus, or URL categorization solutions, which attempt to verify websites and their content as safe, Zero Trust Browsing assumes no site can be trusted. Instead, it leverages remote browser isolation (RBI) to enable users to access the sites that they need, while keeping all content safely away from endpoints and networks. That's why industry leaders are now advocating for RBI functionality to be integrated in secure web gateways.

Using RBI, each website is opened in an isolated container located in the DMZ or the cloud. Within each container, a virtual browser renders the website as a safe media stream. Delivered to the user's browser on the endpoint, it provides a natural interactive user experience. No active code from the internet reaches the browser on the endpoint, so users can access any site – even the dodgiest – with no concern that malware will infect the device or corporate resources.

Protect users – and your business -- from their own errors

Many phishing schemes and other social engineering attacks recruit users as active and willing partners in their own downfall. A fine balance must be struck when generally benign online activity such as filling in forms or downloading files can also be toxic: Block such activity entirely, and your users – and productivity – will suffer. Depend on your users to identify as-yet-unlisted spoofed sites or wonky file extensions, and risks of credential theft and malware downloads skyrocket.

A Zero Trust browsing solution never trusts users to decide whether an activity is risky or safe. To prevent users from entering credentials on what might be a phishing site, as-yet uncategorized sites should be streamed from the isolated remote browser in “view only” mode. Similarly, content for download must be checked for malware and sanitized (maintaining full file functionality) before it's released from the remote container to the endpoint.

Because remote browser isolation does not depend on detecting known threats or recognizable patterns, it protects users and organizations from unknown threats, fresh-from-the-hacker malicious sites – and most of all, from their own errors.

Zero Trust Browsing protects users from unknown threats, fresh-from-the-hacker malicious sites and most of all, from their own errors.

Ericom Shield is an advanced remote browser isolation solution that adds a powerful layer to organizational defense-in-depth strategy by isolating malware, ransomware and other threats where they can't harm corporate network or user devices. It transparently secures Internet use, including file downloads and phishing sites, while reducing risk, costs and operational burden to IT staff responsible for browsing operations. Ericom Shield harnesses the power of isolation to deliver secure browsing and protect the corporate network and endpoints.

**For more information about how
Ericom Shield Remote Browser
Isolation can protect your organization
from browser-borne malware, human
error, and other threats**

Contact us

[www.ericom.com/solutions/
browser-isolation](http://www.ericom.com/solutions/browser-isolation)

shield@ericom.com

US: (201)767-2210

Europe: +44 (0)1905 777970

ROW: +972-2-591-1700

