SLASHNEXT

Phishing in the Dark

Organizations are drowning in a sea of increasingly sophisticated cyber threats and cyber anglers are using a greater variety of phishing tactics to lure and hook their prey.

The SlashNext 2018 Phishing Survey

Growing Gaps in Protections Against Short-Lived, Yet Dangerous Phishing Threats on the Web

The SlashNext 2018 Phishing Survey suggests a dangerous lack of understanding and gaps in protection against modern, fast-moving phishing attacks. The survey of cybersecurity decision-makers showed that most companies lack adequate safeguards against phishing threats on the web and many don't fully understand the prevalence and risks of this growing threat. As such, most organizations are left in the dark when it comes to understanding their exposure to modern phishing tactics and in evaluating what solutions are needed to keep employees protected and to reduce the risk of breaches.

The SlashNext 2018 Phishing Survey was conducted by Survata, an independent research firm based in San Francisco. The survey was taken by 300 IT security decision-makers in mid-sized firms in the U.S. between Sept. 21, 2018 and Sept. 26, 2018.

Survey Reveals 95% of IT Security Pros Underestimate Phishing Attack Risks

Ninety-Five percent of respondents underestimate how frequently phishing is used at the start of attacks to successfully breach enterprise networks. Only 5 percent of respondents realize that phishing is at the start of over 90 percent of successful breaches. (Figure: 1) In fact, phishing is one of the most used and most successful attack vectors, but despite multi-level security controls and phishing awareness training for employees, most organizations remain unaware of their increasing vulnerability to these threats.

When it comes to protecting employees from phishing threats, the top three concerns cited were: 1) Employee awareness / training; 2) Email phishing with links; 3) Email phishing with malware attachments (Figure 2). The focus on employee training to sense social engineering threats and email phishing speaks to the long-term focus on email phishing attacks. But when it comes to the nature of phishing attacks, phishing attack vectors outside of email becomes a top three concern (Figure 3, next page).

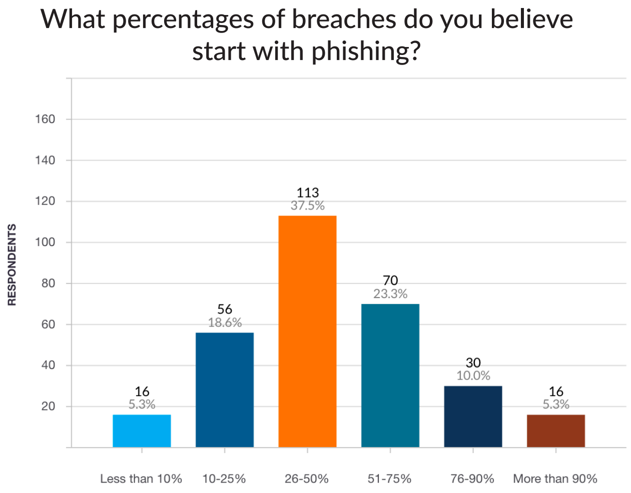

What percentages of breaches do you believe start with phishing?

Figure: 1

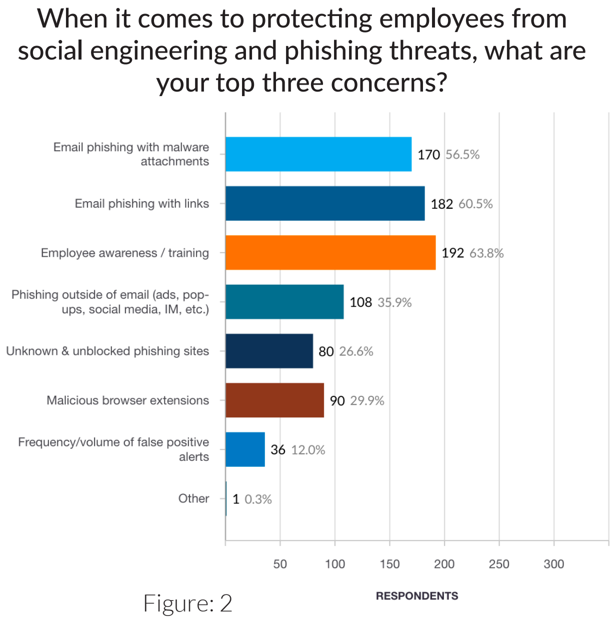

When it comes to protecting employees from social engineering and phishing threats, what are your top three concerns?

Figure: 2

IT Security Pros Cite Shortfalls for a Growing Number of Attacks

While phishing attacks are often equated with phishing emails, phishing attack vectors are expanding beyond email. Both employees and consumers are subject to targeted phishing attacks in ads, search results, pop-ups, social media, IM and chat applications, rogue browser extensions and apps. Users encounter these threats on the web or in free apps, where even a single mistaken click can open their companies up to costly data breaches or extortion attempts.

Over half of respondents to the survey named the growing number of phishing attack vectors beyond email as a "Top 3" concern in terms of potential phishing threats. The other top concerns involved the growing sophistication and realism of spoofed sites, and the difficulties in training employees to spot these new types of phishing threats, with two-thirds (64 percent) of IT security pros citing shortfalls in employee awareness and training as their top concern for protecting workers against social engineering and phishing threats (Figure: 3).

Threat actors' tactics have evolved to using very fast-moving phishing sites and attack vectors that evade existing security controls. Phishing awareness training offers little to protect employees when phishing sites appear more legitimate and often manipulating users.

The survey revealed that four out of ten (39 percent) cite the inability of their current defenses to reliably detect phishing attacks as a top concern (Figure 3). Nearly half of respondents (45 percent) believe they experience 50 or more phishing attacks per month and 14 percent believe they experience more than 500 phishing attacks per month (Figure: 4).

Of the following, what are your top three concerns regarding the nature of tactics of phishing attacks?

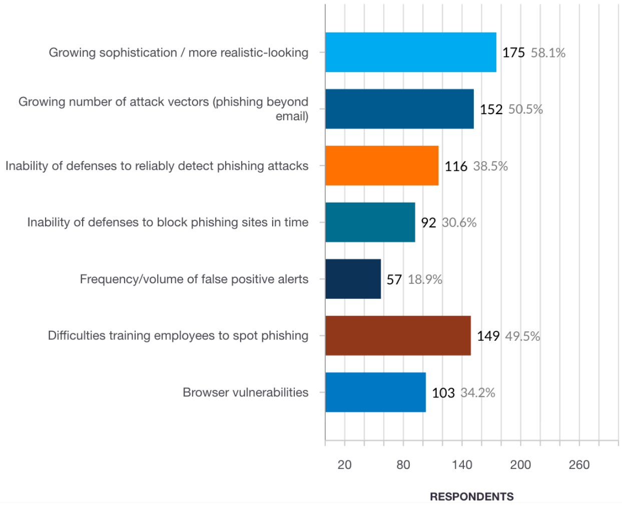


Figure: 3

How many phishing threats do you believe your organization experience each month?

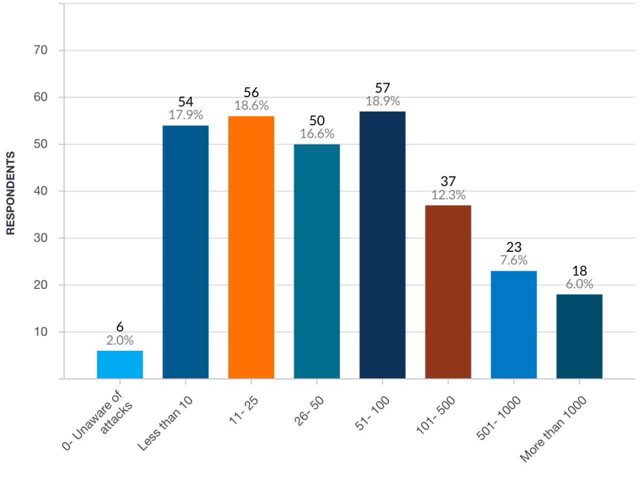
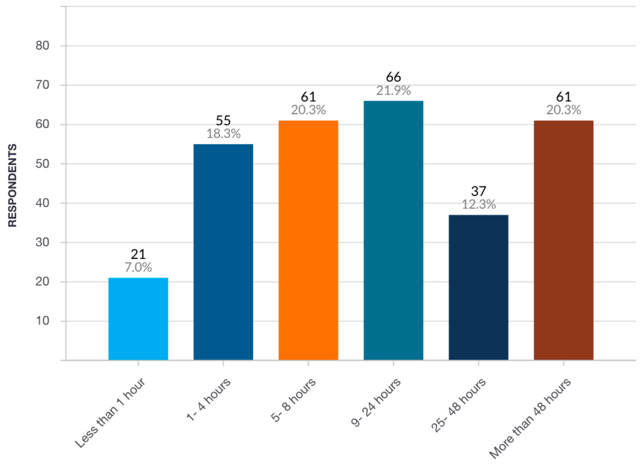


Figure: 4

Fast-Moving Phishing Sites are Evading Existing Eecurity Controls

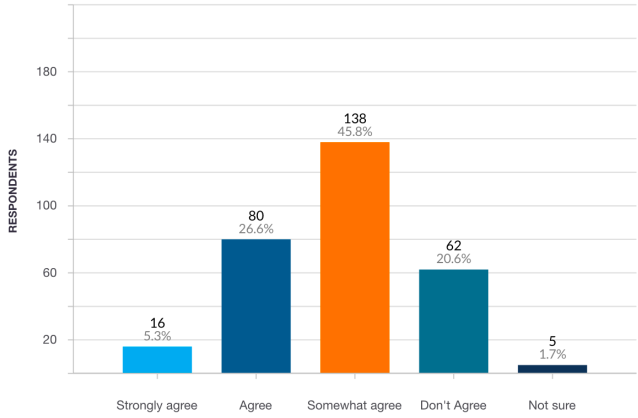
Most phishing sites stay online for just four to eight hours, with some up for only minutes, according to the 2018 Webroot Threat Report. Yet only 46% of respondents were aware most sites are online and active for 8 hours or less (Figure 5). More than half (56%) believed phishing sites were typically online for more than 8 hours, with 1 out of 5 respondents believing phishing sites are typically online for more than 24 hours. However, the respondents know they need improved protection, with only one-third of respondents (32 percent) agree or strongly agree that their current threat feeds and block lists are adequate to protect users from new phishing sites (Figure: 6).

Such brief durations demand that organizations use anti-phishing solutions that can detect a malicious phishing site in real-time, rather than putting faith in static threat feeds that cannot keep up with the volume and short lifecycles of today's fast-moving phishing threats. This is supported by the survey where less than a third (32%) of respondents agreeed or strongly agreed that the threat feeds / block lists they get from security vendors are adequate to protect them from new phishing sites (Figure 6).



How long do you believe malicious phishing sites are typically online?

Figure: 5



How much do you agree with the following statement: Threat feeds/block lists we current get from security vendors, or other sources, are adequate to protect us from new phishing sites.

Figure: 6

Phishing Defenses and Tools

When asked what are the top defenses for protecting against phishing, respondents cited: 1) Employee awareness / training; 2) Anti-virus/Malware protection; 3) URL filtration systems such as firewalls (Figure 7). The continued emphasis on employee training to spot phishing comes through, but it's less effective these days as phishing attacks get more realistic looking. Also surprising was that despite the large emphasis on email phishing, Secure Email Gateways (SEGs) came in as fourth highest rated rather than being in the top three.

When it comes to the effectiveness of their current security tools to protect against phishing, only 14% rated their tools as extremely effective (Figure 8). Most believed their tools were only somewhat effective or not very effective. This echoes what SlashNext hears from customers. As phishing attack vectors become more varied, do not include files for AVs or sandboxes to examine, and become more legitimate looking, it is harder for traditional security tools to spot malicious phishing sites and attacks.

Of the following, what are your top three defenses to protect your organization from phishing?

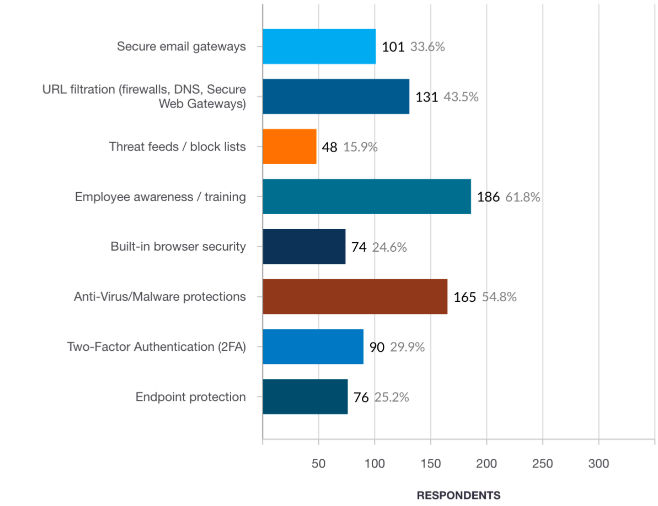


Figure: 7

How would you describe the effectiveness of current security tools in place to protect against phishing threats?

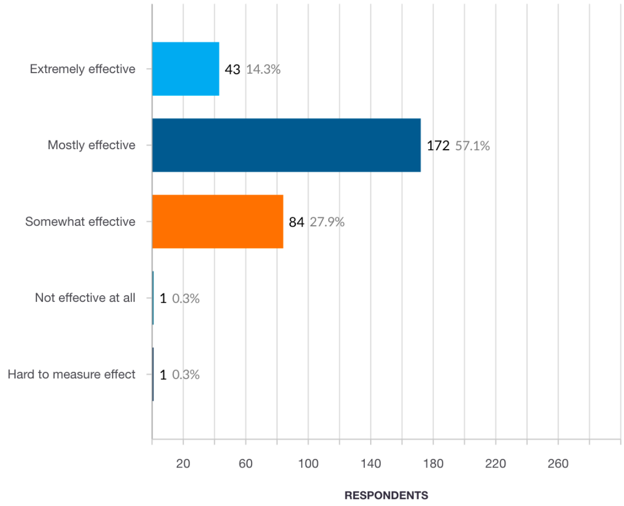


Figure: 8

Views on Real-Time Phishing Site Detection

When asked if their organization currently has real-time phishing site detection capabilities, 69% believed they did (Figure 9). This is a very surprising finding. While URL filtration systems maintain “block lists” to block known bad sites, there are very few technologies (other than SlashNext) that provide real-time phishing site detection. Thus, to see such a large percentage of respondents believe they have this capability demonstrates a misunderstanding of their current phishing protection capabilities and/or a misunderstanding of the question.

Fortunately, with targeted phishing attacks now employing very short-lived phishing sites, nearly half (49%) of respondents are currently evaluating real-time phishing site detection capabilities (Figure 10). And another 38% are planning to evaluate this kind of protection. That’s a good thing when real-time phishing site detection is key to better phishing protection.

Are you currently evaluating technologies that provide real-time phishing site detection capabilities?

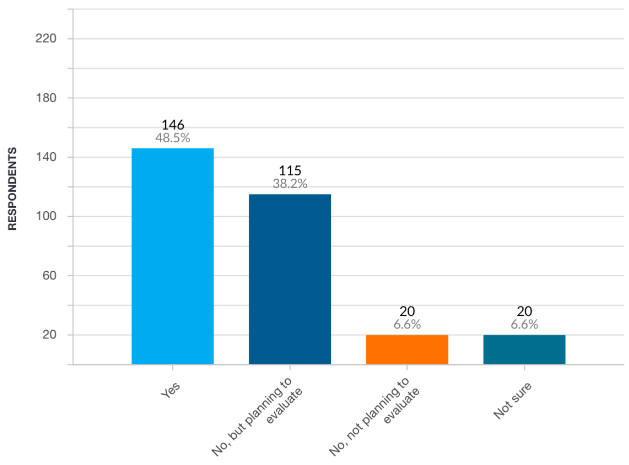


Figure: 9

Does your organization currently have technologies that provide real-time phishing site detection capabilities?

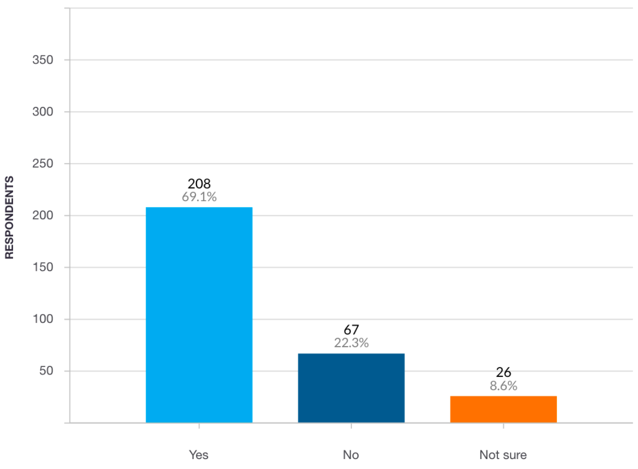


Figure: 10

About SlashNext

SlashNext pioneered an entirely new, cloud-powered, adaptive approach to real-time, zero-page Phishing site detection. Instead of relying on outdated methods like domain reputation and URL analysis–which hackers can easily evade—SlashNext uses live Session Emulation and patent-pending SEER™ detection technology to detect malicious sites in real-time. By dynamically inspecting suspicious browsing contents and server behavior, SlashNext can detect previously unknown phishing threats in seconds. Confirmed malicious URLs are immediately available as a dynamic block list for firewalls, DNS servers, or other blocking infrastructure. This approach enables SlashNext to stop complex zero-hour Phishing threats in real-time with the speed, power, and scale of the cloud.

Learn more:
Phone: (800) 930-8643
Email: info@slashnext.com
Website: www.slashnext.com

SLASHNEXT