

RR


# REDUCING THE RISK OF PHISHING ATTACKS: THE RACE IS ON

December 2018

Derek E. Brink, CISSP

Vice President and Research Fellow, Information Security and IT GRC

**ABERDEEN**



From mere minutes to the first user opens and clicks on malicious emails, attachments, and URLs, attackers hook virtually 100% of their phishing victims within the first 4 to 8 hours — by which time they have shut down 75% of their phishing URLs and moved on. With so much at stake based on this accelerating race against time, successful protection of your organization’s email and websites against phishing attacks requires a high-speed, highly automated approach.

---

### Why the Race Against Time Matters in the Defense Against Phishing Attacks: Users are Quick to Click

Empirical data continues to show that **nearly all successful data breaches begin with an attack on your users** — e.g., the Verizon 2018 *DBIR* found that **93%** of confirmed data breaches involved *phishing* (which tends to rely on getting users to click on malicious attachments or links) and the closely related *pretexting* (which relies more on convincing users to give up information or take action, such as responding to the urgent request of an impersonated executive or business partner). Virtually all (**96%**) of these attacks continue to use **email**, although there is an increasing use of **social media** and other methods (e.g., ads, browser extensions, freeware, instant messages, pop-ups) in the attacker’s campaign mix.

Unfortunately, enterprise users are absurdly quick to open, click, and act on these attacks. Aberdeen’s analysis of empirical data from *more than 1,400 simulated phishing attacks* helps to visualize and quantify why the race against time matters for defender protection from and response to malicious emails (see Figure 1):

- ▶ The likelihood of the first user click on malicious emails occurring **within 30 seconds** was **about 8%**.
- ▶ The likelihood of the first user click on malicious emails occurring **within 60 seconds** was **about 30%**.

---

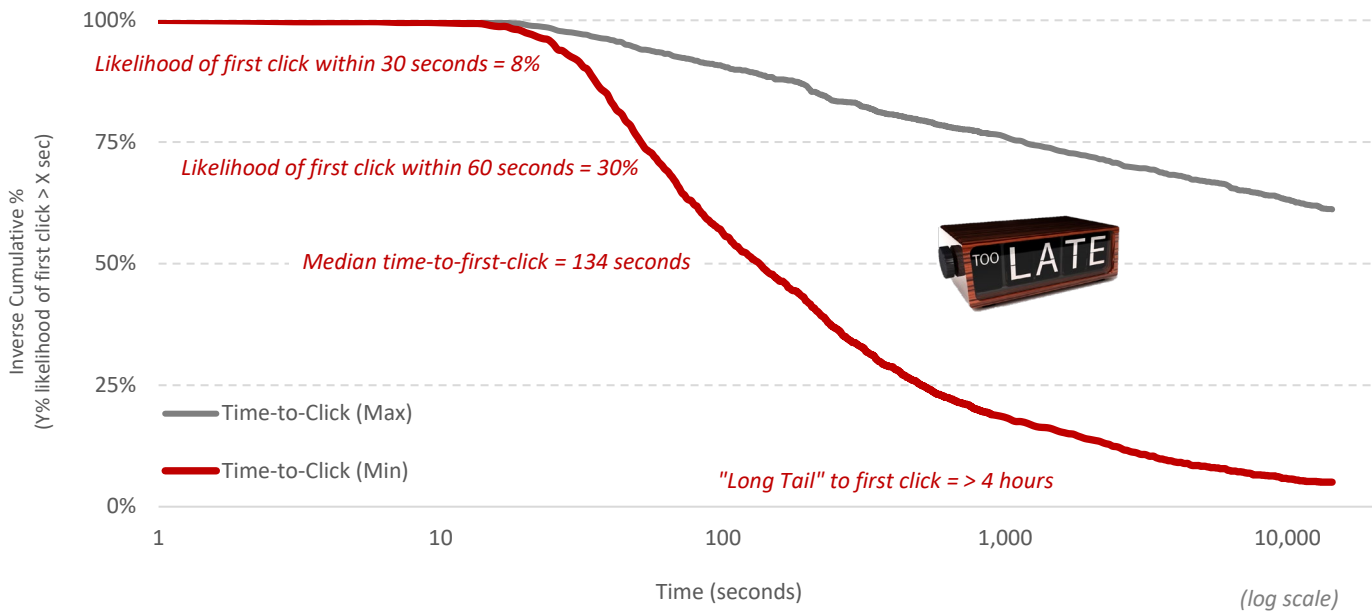
**Over more than 1,400 simulated phishing attacks, the median time-to-first-click on malicious emails was just 134 seconds.**

---

- ▶ The **median** time-to-first-click on malicious emails was **just 134 seconds**.
- ▶ The “long tail” for how long until the first user click on malicious emails was a still-modest **4 hours**.

The **red** line in Figure 1 sets the bar for how fast malicious email must be identified, verified, and remediated — before the organization’s users start falling victim to phishing or pretexting attacks. Performance which is to the right of the red line is simply too little, too late.

Figure 1: Phishing Risk — Users are Extremely Quick to Click



Source: Data adapted from IRONSCALES; Aberdeen, September 2018

### Browser Blocking is Still Too Slow to Be Effective

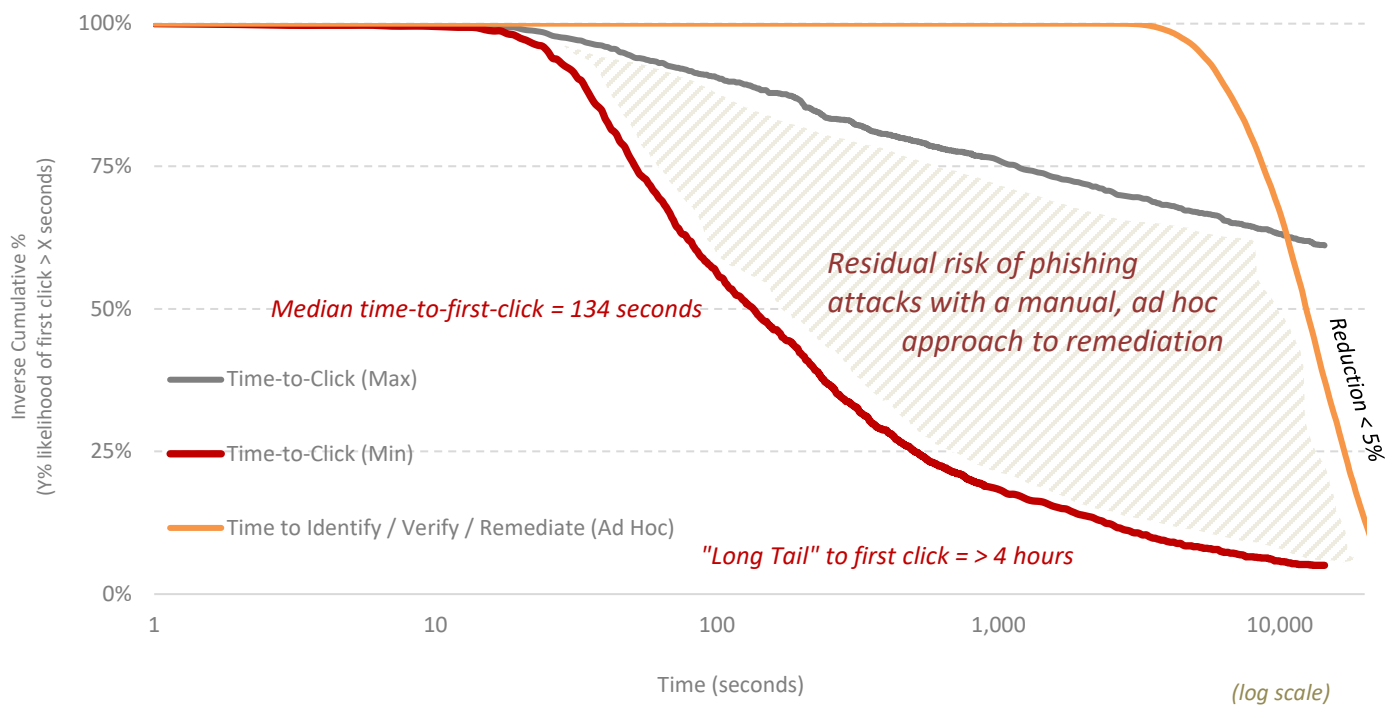
Popular web browsers (e.g., Mozilla Firefox, Google Chrome, Microsoft Edge and Internet Explorer, Apple Safari) are designed to provide protections against phishing attacks and socially engineered malware — but given the reality of user time-to-click behaviors described above, these protections are too slow to be effective. Empirical testing shows that by the end of the first 60 minutes, automated browser-based protections range from 77.3% to 89.5%, and increase over time to between 94.3% and 96.7% (Source: NSS Labs, December 2018). But again, the red line in Figure 1 shows that the empirical likelihood of first click within 60 minutes is more than 90% — so browser blocking is still too slow to be effective as a first line of defense.

**As a first line of defense, browser blocking is still too slow to be effective against phishing attacks and socially engineered malware.**

## Manual Remediation is Much Too Slow to Be Effective

Additional analysis makes it painfully clear that manual, ad hoc efforts to identify, verify, and remediate phishing attacks by generalized IT staff is much too slow to be effective (see the orange line in Figure 2). The **median** total time to identify / verify / remediate using this approach to post-delivery incident response is **more than 3 hours**, which reduces the organization's risk from phishing attacks by **less than 5%**.

Figure 2: Phishing Risk — Manual Remediation is Much Too Slow

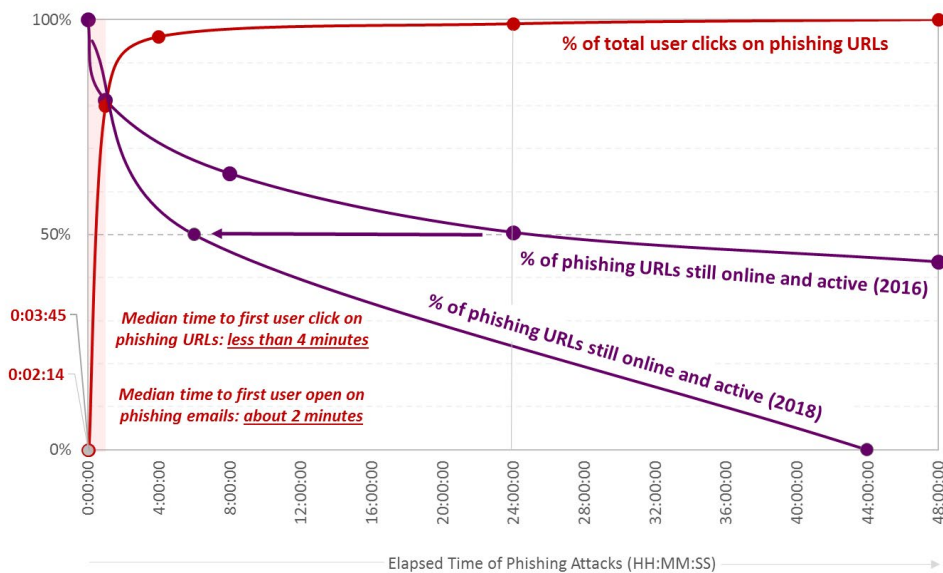


Source: Data adapted from IRONSCALES; Aberdeen, September 2018

## Meanwhile: Attackers are Fast, and Getting Faster

A continued focus on the timeline of phishing attacks (see Figure 3) sheds new light on how much is at stake based on just the first few minutes of phishing attacks, and makes it clear why successful front-end protection of your organization's email and websites against phishing attacks requires a **high-speed, highly automated approach** that is designed to operate faster than both users and attackers.

Figure 3: From Mere Minutes to the First User Opens and Clicks on Malicious Email, Attackers Hook Virtually 100% of Phishing Victims Within 4-8 Hours — And 50% of Phishing URLs are Already Gone



Source: Data adapted from Cyren 2016 *Phishing Threat Report*, Verizon 2016 *DBIR*, IRONSCALES 2018, Webroot 2018 *Threat Report*; Aberdeen, December 2018

Take a moment to study the timelines represented in Figure 3:

- ▶ **User behaviors (red line)** — It's not surprising that email continues to be the leading delivery mechanism for phishing attacks and pretexting attacks: empirical data shows that the median time to the *first user open of phishing emails* is **about two minutes (2:14)**; the median time to the *first user click on phishing URLs* is **less than four minutes (3:45)**; and within the first 4-8 hours attackers have already hooked virtually 100% of their phishing victims.
- ▶ **Attacker behaviors (purple line)** — Given the speedy success of their phishing campaigns, it's also not surprising that after just **4-8 hours**, attackers have already taken down about 50% of their malicious URLs and moved on — down from about 24 hours just two years ago (Source: Webroot 2018 *Threat Report*).

The sheer volume of domain names and URLs, and the speed at which they change, only exacerbates the problem. In a large-scale analysis of URLs in 2017, about 3 out of 4 sites were deemed to be trustworthy or low risk — leaving an astounding **25%** that organizations must deal with to successfully manage these highly dynamic threats (Source: Webroot).

## The Need for Speed: Leading Security Solution Providers are Enabling Faster Detection, to Improve Prevention

For some CISOs, the solution for protection is simply to block *all* URLs for a sufficiently long period of time (e.g., 24 - 48 hours) — but this practice also creates an artificial impediment to business users from doing their legitimate tasks, in pursuit of the organization’s strategic business objectives. Aberdeen considers this an old-school, obstructive, “*Department of No*” approach to security and risk that most security leaders have rightly been working hard to cast aside and overcome.

In Aberdeen’s view, **security awareness and training** for users also continues to play an important — and cost-effective — role in reducing the risk of phishing attacks, and with respect to protection, it continues to act as the organization’s vital last line of defense.

Fortunately, there are more automated and effective ways to detect and defend against phishing attacks at the *beginning* of their lifecycle. Innovative security solution providers are now combining the **visibility** and **scale** of a global, cloud-based security platform with continuous, automated **analysis** and **correlation** of data across billions of email and web transactions per day — at speeds which are fast enough to turn *detection* of phishing emails and malicious phishing sites into more effective *protection*. In addition, solutions that close the loop between detection and protection — for example, by integrating with network firewalls or DNS services to automate blocking of malicious sites — are designed to move defenders even closer towards the vision of a dynamic, real-time defense.

In Aberdeen’s view, the superiority of information that comes from this emerging blend of real-time analytics, automation, and integration — across a broad observation space — reflects the agile, technology-based approach to security that defenders need to have going forward to successfully manage the highly dynamic risk of phishing attacks. A combination of **pre-delivery detection and protection** and **post-delivery protection and response**, leveraging the expertise and focus of specialized solution providers, is by far the fastest and most effective approach in the accelerating race against time.

---

**It’s generally accepted that no defense can be 100% effective. In Aberdeen’s view, security awareness and training for enterprise users continues to play an important — and cost-effective — role in reducing the risk of phishing attacks, and with respect to prevention it continues to act as the organization’s vital last line of defense.**

---

## Related Research

---

*How to Conquer Phishing? Beat the Clock;*  
November 2017

*Reducing the Risk of Phishing Attacks: It's About Time;*  
November 2017

*Enterprise Email: Are You Adequately Addressing Your Risks?;*  
August 2017

*Security Awareness Training: Small Investment, Large Reduction in Risk;*  
July 2017

### **About Aberdeen Group**

Since 1988, Aberdeen Group has published research that helps businesses worldwide to improve their performance. Our analysts derive fact-based, vendor-neutral insights from a proprietary analytical framework, which identifies Best-in-Class organizations from primary research conducted with industry practitioners. The resulting research content is used by hundreds of thousands of business professionals to drive smarter decision-making and improve business strategies. Aberdeen Group is headquartered in Waltham, Massachusetts, USA.

This document is the result of primary research performed by Aberdeen Group and represents the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group.