KB

HOW TO CONQUER PHISHING? BEAT THE CLOCK

September 2018

Derek E. Brink, CISSP
Vice President and Research Fellow, Information Security and IT GRC

ABERDEEN

Aberdeen's analysis of empirical data shows that manual, ad hoc efforts to *identify*, *verify*, and *remediate* phishing attacks by generalized IT Staff is much too slow to be effective, reducing the organization's risk from phishing attacks by **less than 5%**. The combination of automated, technology-driven *pre-incident protection* and *post-incident protection and incident response* is by far the fastest and most effective approach — quantifiably reducing the organization's risk from phishing attacks by **more than 70%**, with ongoing upside.

Framing the Risk of Phishing Attacks for Senior Business Leaders: How Likely; How Much Impact?

As Aberdeen's previous research has shown, the annualized risk of phishing attacks can be *quantified* to help senior leaders make a better-informed business decision — and the business impact can be financially material, a risk which most organizations determine they cannot simply ignore.

Although the risk of a phishing attack varies significantly by *industry* (e.g., based on observable differences in empirical click rates, and the percentage of investigated security incidents resulting in successful data breaches), as well as by *organization* (e.g., based on the number of business users, and the type and volume of data), the following estimates from Aberdeen's analysis provide some useful perspective:

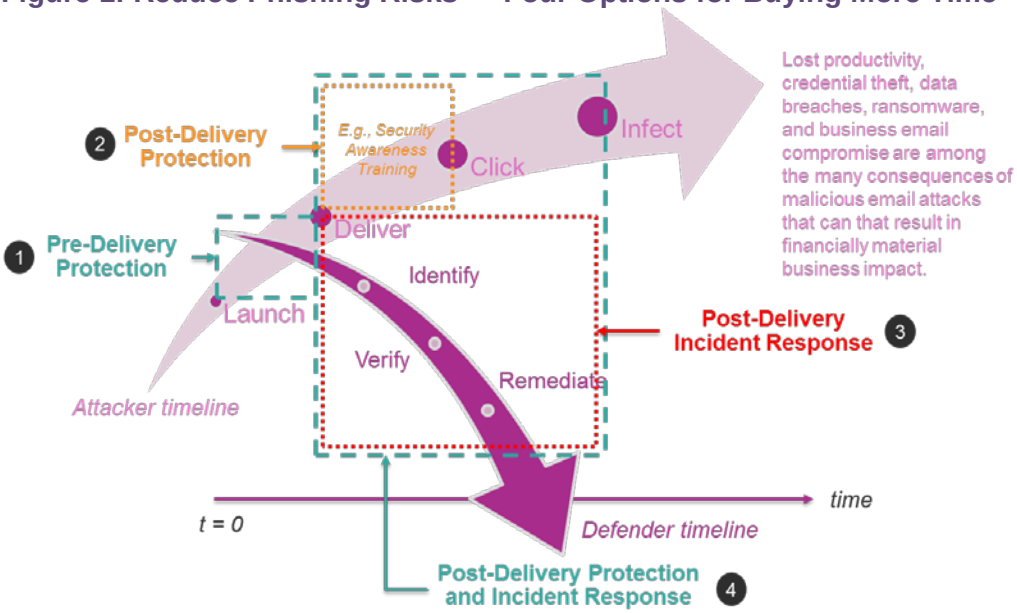
- **The annualized business impact is 90% likely to be more than $0** — i.e., organizations will almost certainly incur *some* negative business impact because of phishing attacks.
- **The median annualized business impact is between $100K and $500K** — for the private sector as a whole (across all industries), it's *about $260K*.
- **The annualized business impact is 10% likely to be more than $3M to $18M** — i.e., there's a material likelihood of a large, potentially catastrophic business impact; this is the *"long tail"* of phishing risk. For the private sector as a whole (across all industries), it's *about $10M*.

Lost productivity, credential theft, data breaches, ransomware, and business email compromise are among the many consequences of malicious email attacks that can result in financially material business impact.

Reducing the Risk of Phishing Attacks: It's About Time

In multiple dimensions, **reducing the risk of phishing attacks is a race against time** — i.e., the ability of *defenders* to protect and respond more quickly to malicious emails than the *attacker* timeline, as well as more quickly than *their own users* are to open phishing emails and click on malicious links.

Figure 1: Reduce Phishing Risks — Four Options for Buying More Time



Source: Aberdeen, September 2018

Reducing the risk of phishing attacks is a race against time — defenders must protect and respond more quickly to malicious emails than the attacker timeline, as well as more quickly than their own users are to open phishing emails and click on malicious links.

In a simplified model of the phishing attack lifecycle, defenders essentially have **four options** for buying more time (see Figure 1):

- **Pre-delivery protection** — from the attacker's initial launch of a malicious email campaign (*t = 0*), can defenders successfully apply **monitoring and filtering** technologies to prevent those emails from being delivered? Leading solution providers are applying advanced *automation*, *artificial intelligence (AI)*, and *machine learning (ML)* technologies to *identify*, *verify*, and *remediate* malicious email before it ever hits the organization's inboxes. Effectiveness at prevention will never reach 100%, but it can be expected to increase over time.

- **Post-delivery protection** — for malicious emails that are successfully delivered, can defenders successfully engage their Business Users to reduce the likelihood of those emails being opened and clicked? **Security awareness training** initiatives can effectively *increase user awareness* of malicious emails; *reduce user click rates* on malicious emails; *delay user time-to-click* on malicious emails; and *increase user reporting* of potentially malicious emails for review and

remediation by Technical Staff. On the other hand, security awareness training itself does *not* verify or remediate malicious emails, or generate intelligence about identified phishing attacks.

- **Post-delivery incident response** — for malicious emails that are successfully delivered, can defenders successfully leverage their in-house Technical Staff to *identify*, *verify*, and *remediate* those emails before they result in financially material business impact? Human review and verification by generalists (i.e., **IT Staff**) on an ad hoc, best-effort basis is slow and inconsistent in speed, and remediation (e.g., blocking specific senders, instructing users *"don't click"* and *"please delete"*) is limited and uncertain in effectiveness. Human review and verification by specialized, dedicated staff (i.e., in an in-house **Security Operations Center**) can be faster and more consistent, but requires an investment in 24 / 7 capabilities. Without automation, both generalists and specialists can quickly be overwhelmed by the sheer volume of malicious email.

- **Post-delivery protection and incident response** — in combination with **pre-delivery protection**, specialist solution providers are now integrating *automated real-time checks* for malicious email at the individual inbox level, based on the latest *threat intelligence*, *behavioral analytics*, *sender reputation*, and other *metadata*. Automated capabilities for identification and verification are complimented by the focused, dedicated technical staff of the solution provider to review and verify malicious emails when necessary. *Automated removal* of malicious email from all affected inboxes provides remediation which is much faster and more certain than primarily manual approaches.

Reducing the Risk of Phishing Attacks: Quantifying Why Beating the Clock Matters

Aberdeen's analysis of empirical data from *more than 1,400 simulated phishing attacks* helps to visualize and quantify the value of time for defender protection from and response to malicious emails (see Figure 2):

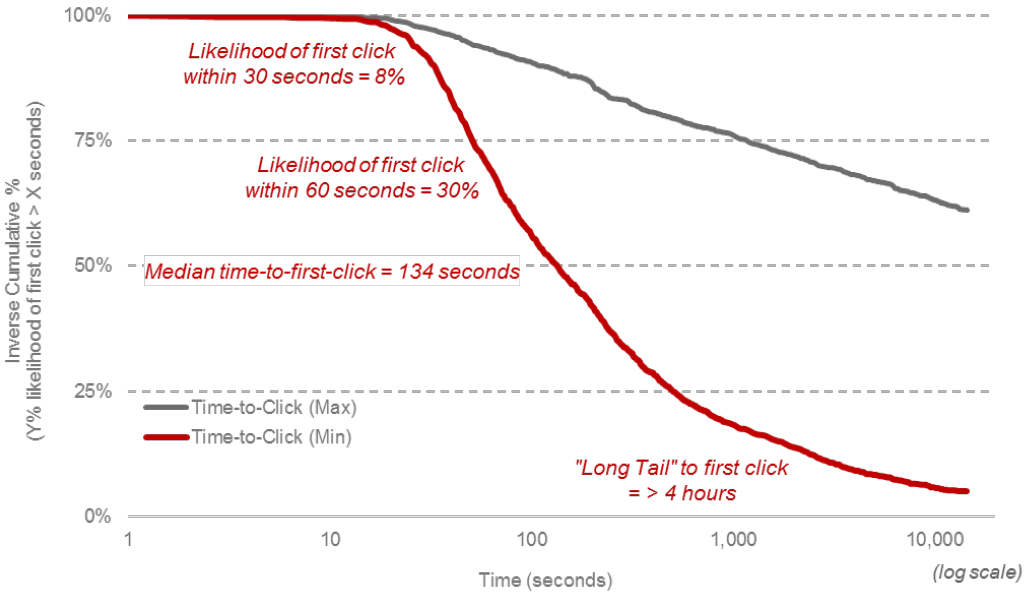
- The likelihood of the first user click on malicious emails occurring **within 30 seconds** was **about 8%**.
- The likelihood of the first user click on malicious emails occurring **within 60 seconds** was **about 30%**.
- The **median** time-to-first-click on malicious emails was **just 134 seconds**.

Over more than 1,400 simulated phishing attacks, 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 2 sets the bar for how fast malicious email must be identified, verified, and remediated — before the organization’s users start falling victim to phishing attacks. Performance which is to the right of the red line means that the risk of phishing attacks has not been addressed.

Figure 2: Reducing Phishing Risks — Why Beating the Clock Matters



Source: Empirical data adapted from IRONSCALES (N = 1,407 simulated phishing campaigns); Aberdeen, September 2018

Additional analysis shows 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 3). 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%**.

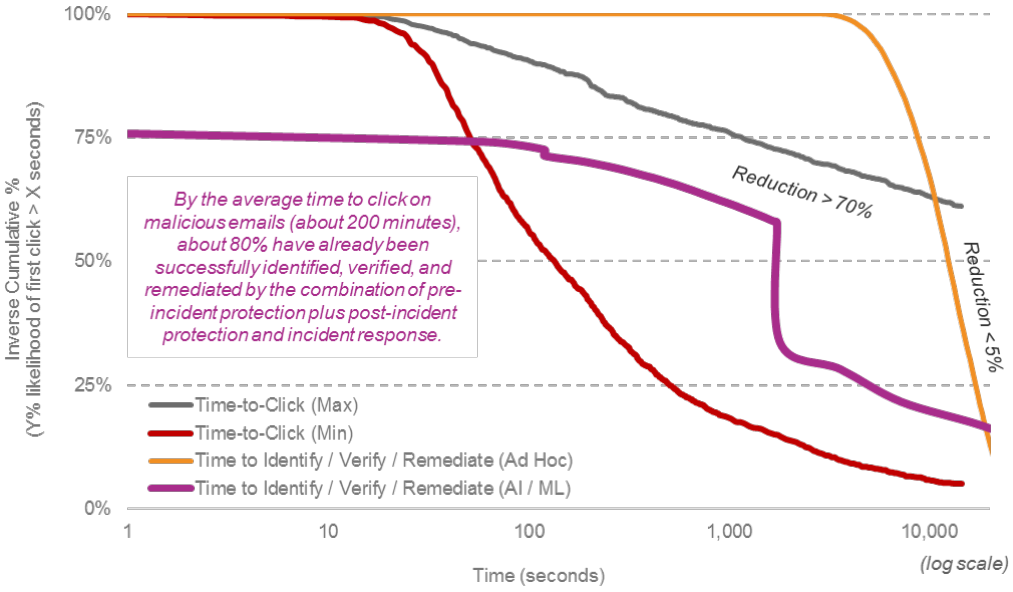
In contrast, the combination of automated, technology-driven **pre-incident protection** and **post-incident protection and incident response** is by far the fastest and most effective approach (see the **purple** line in Figure 3). Aberdeen’s analysis of more than 51,000 fully remediated email attacks by one specialist solution provider shows that:

- **25%** of malicious email was automatically identified, verified, and remediated before ever hitting the organization’s inboxes.

Manual, ad hoc efforts to identify, verify, and remediate phishing attacks by generalized IT Staff is much too slow to be effective, reducing the risk from phishing attacks by < *5%*.

- The median time to identify / verify / remediate malicious emails was **less than 30 minutes**.
- Automated, real-time checks at the individual inbox level — complemented by expert review and automated removal from all affected inboxes — provides remediation which is much faster and more certain than manual methods. In Aberdeen's analysis, this reduces the organization's risk from phishing attacks by **more than 70%**, with ongoing upside as technology-based automation, AI, and ML continue to improve.

Figure 3: Reducing Phishing Risks — Why Beating the Clock Matters



Source: Empirical data adapted from IRONSCALES (N = 1,407 simulated phishing campaigns; N = 51,558 fully remediated email attacks); Aberdeen, September 2018

The combination of automated, technology-driven pre-incident protection and post-incident protection and incident response is by far the fastest and most effective approach — quantifiably reducing the risk from phishing attacks by *more than 70%*, with ongoing upside as technology-based automation, AI, and ML continue to improve.

Summary and Key Takeaways

- The risk of phishing attacks can and should be *quantified*, to help senior leaders **make a better-informed business decision** regarding what to do about it.
    - The annualized business impact from phishing attacks can be financially material, a risk which most organizations determine they cannot simply ignore.
    - In multiple dimensions, reducing the risk of phishing attacks is **a race against time**.

- *Defenders* must protect and respond more quickly than the *attacker* timeline — as well as faster than *their own users* are to open phishing emails and click on malicious links.

- **Post-delivery incident response** by generalized IT Staff is the least effective approach, reducing the risk from phishing attacks by **less than 5%**.

- Automated, technology-based **pre-delivery protection** and **post-delivery protection and incident response** from specialist service providers is by far the fastest and most effective approach:

  - The risk from phishing attacks is reduced by **more than 70%**, with ongoing upside from continued improvements in technology-based automation, AI, and ML.

  - It makes the most effective use of internal technical staff, by leveraging the expertise of specialist service providers.

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.

17632