KB

# EMAIL SECURITY IS INEFFECTIVE, AND GETTING WORSE: WHAT YOU CAN DO ABOUT IT

June 2019

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

ABERDEEN

The prevalence and business impact of **phishing email attacks** continues to illustrate the ineffectiveness of current email security controls and countermeasures. To adapt and evolve with financially motivated and technically sophisticated attackers, effective email security requires a purpose-built blend of *advanced technologies*, *human intelligence*, and *user behaviors*.

## Email Security: A Simple Framework for Discussion

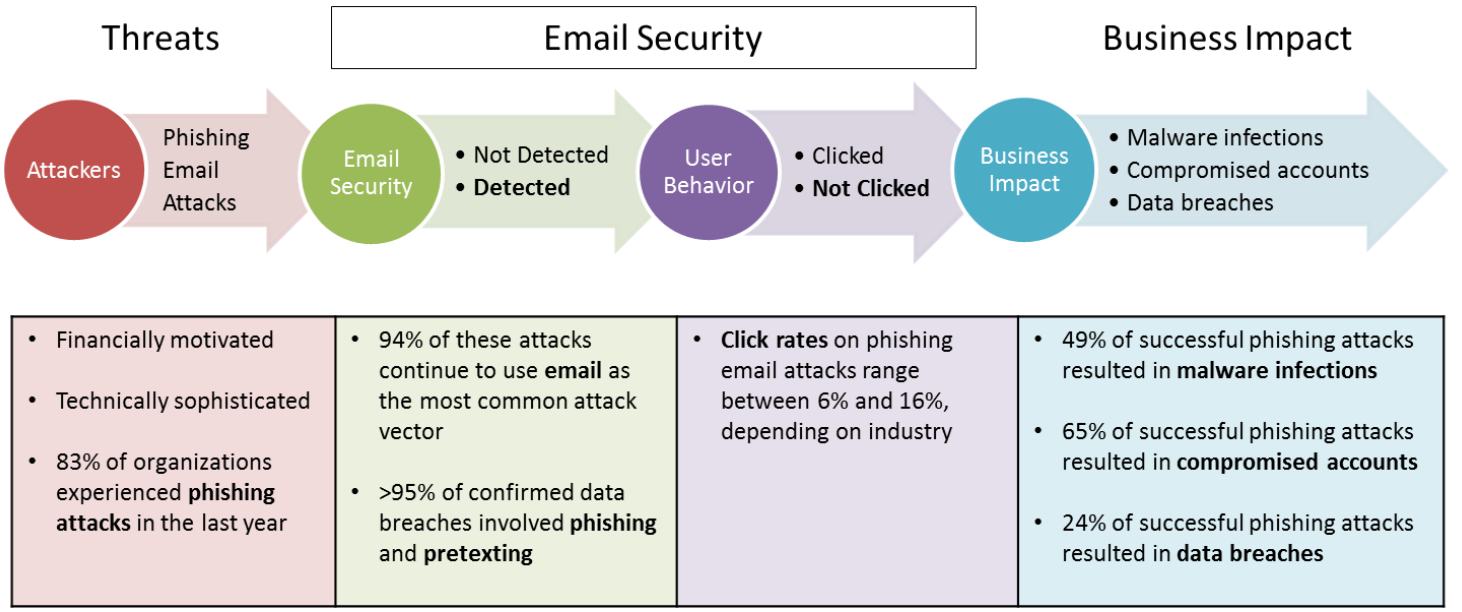
Effective email security involves a blend of advanced technologies, human intelligence, and user behaviors. Figure 1 provides a simple framework for a quick review of current trends in these areas:

- **Attackers** — who are financially motivated, and technically sophisticated — continue to leverage phishing attacks to achieve their criminal objectives. Most (83%) organizations report having experienced phishing attacks over the last year, nearly all (94%) of which continue to use **email** as the most common attack vector.
- **Email security**, in the form of technology used in combination with human intelligence, is designed to detect and protect against phishing email attacks — yet inevitably, some attacks go undetected. *Phishing* relies on getting users to click on malicious attachments or links; *pretexting* relies on convincing users to voluntarily give up information or take action, for example by responding to the urgent request of an impersonated executive or business partner. Almost all (>95%) confirmed data breaches involved phishing and pretexting.
- **User behaviors** are another critical component to effective email security, representing the last line of defense for phishing attacks that evade detection and show up in enterprise inboxes. Over the last year, user *click rates* on phishing email attacks ranged between 6% and 16%, depending on industry.
- **Business impact**, i.e., the directly observable consequences of successful phishing email attacks, is a big part of what makes any of the above discussion really matter. Over the last year, half (49%) of successful phishing attacks resulted in *malware infections*, and two thirds (65%) resulted in *compromised accounts* — both of which

**Nearly all (94%) of phishing attacks continue to use email as the most common attack vector — 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.**

negatively impact the productivity of users, as well as any technical staff required for remediation. One in four (24%) successful phishing attacks resulted in *data breaches*, i.e., the confirmed disclosure of an enterprise information asset to an unauthorized party.

**Figure 1: The Current Mix of Email Security is Ineffective**




Source: Data adapted from Proofpoint *State of the Phish Report 2019*, Verizon *Data Breach Investigations Report 2019*; Aberdeen, June 2019

## A Closer Look at Why Email Security Matters: Quantifying the Risk of Phishing Email Attacks

If we want to communicate effectively about the **risk** of phishing email attacks, we need to use the proper language. Too much of the time, IT and Security professionals tend to focus intensely on the technology-oriented details of "who, what, and how" regarding the latest threats, vulnerabilities, and exploits. The senior leadership team, however, is primarily interested in the business-oriented details of "how likely," and "why it matters."

If we're not talking about phishing email attacks in terms of both *how likely* and *how much business impact*, we're not really talking about *risk*!

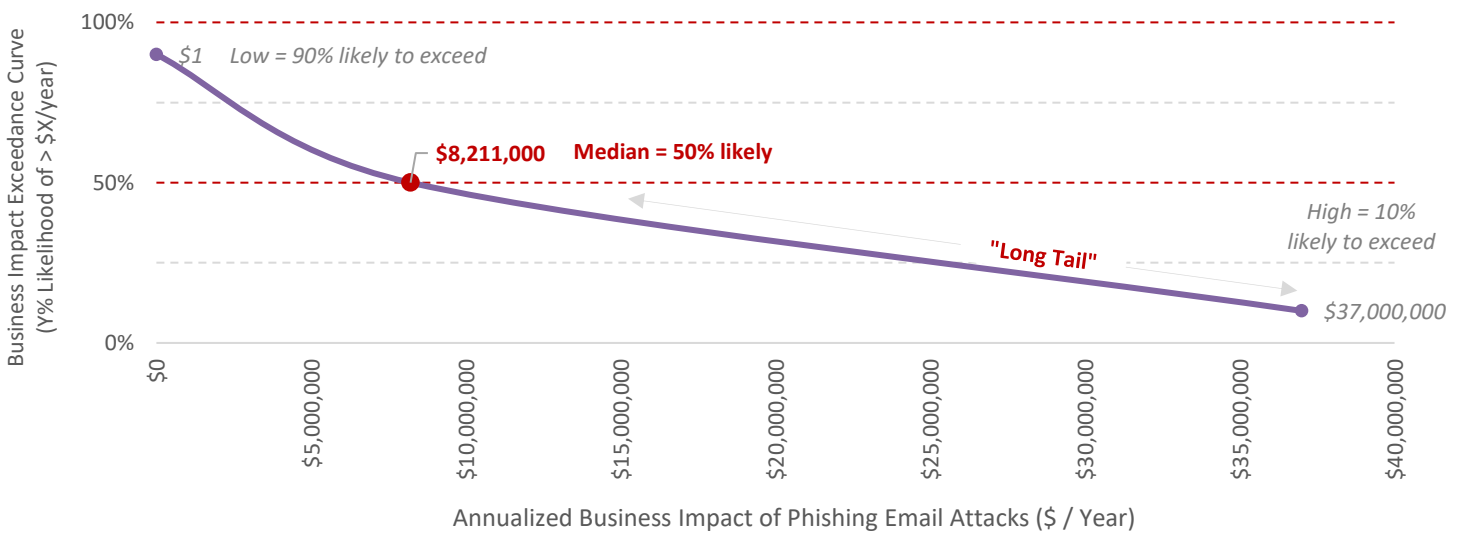
To help bridge this critical communications gap, Aberdeen continues to make use of the growing body of empirical data regarding the likelihood and business impact of phishing email attacks to *quantify* the risk, as risk is properly defined — i.e., not as a falsely precise, single-point estimate, but as *a range of possible outcomes* and their *associated likelihoods*.

For example, Figure 2 provides several valuable insights about the annualized risk of phishing email attacks for the **private sector** as a whole (all industries), for an organization with 1,000 users and an information asset of 10M records:

- The **median** total business impact of phishing email attacks is **about $8.2M per year**, under the current approach to email security.
- More importantly, there's a **10% likelihood** that the total business impact of phishing email attacks in this scenario will be **more than $37M per year**. This is the "long tail" aspect of the risk of phishing email attacks that is so important for IT and Security professionals to communicate effectively to the senior leadership team, to make a well-informed business decision regarding what to do about it.
- To the extent that the senior leadership team finds this level of risk to be unacceptably high, this analysis also explains — in straightforward business terms — **why more effective email security is needed**.

**For the private sector (all industries), for an organization with 1K users and 10M data records, the median total business impact of phishing email attacks is about $8.2M per year under the current approach to email security, with a 10% likelihood of exceeding $37M.**

**Figure 2: Quantifying the Risk of Phishing Email Attacks Supports Better-Informed Business Decisions About Email Security**




Source: Monte Carlo analysis, based on data adapted from Wombat Security *State of the Phish Report 2018*, Verizon *Data Breach Investigations Report 2018*, and Ponemon *Cost of a Data Breach 2018*; Aberdeen, June 2019

In a quantitative analysis of this nature, several factors (e.g., *click rates*, *likelihood of a data breach*, *total cost of a data breach*) vary based on industry. For example, for the same scenario of an organization with 1,000 users and an information asset of 10M records:

- In the **healthcare** sector, the median total business impact of phishing email attacks is about $26M per year, with a 10% likelihood of exceeding $112M.
- In the **financial** sector, the median total business impact of phishing email attacks is about $9M per year, with a 10% likelihood of exceeding $56M.
- For the **education** sector, the median total business impact of phishing email attacks is about $10M per year, with a 10% likelihood of exceeding $46M.

## How Threats to Email Security are Getting Even Worse

Aberdeen's analysis of empirical data from a leading email security solution provider (Source: IRONSCALES 2019) illustrates the incredible leverage currently enjoyed by attackers, which significantly amplifies the threats to email security. For every uniquely identified phishing email attack:

- The number of unique user mailboxes affected ranges from 2 to more than 40
- The total number of organizations affected ranges from 5 to more than 150

Said another way, even in an era of more specifically targeted attacks, every phishing email attack affects **multiple mailboxes at multiple organizations** — and requires **hundreds of successful detections** by the email security capabilities of enterprise defenders.

Going forward, it's getting even worse. Empirical data shows that more than 40% of phishing email attacks are **polymorphic** — i.e., they undergo at least one permutation designed to evade traditional email security controls — with the most sophisticated attackers already implementing polymorphic phishing email attacks that undergo *hundreds of permutations* to evade traditional defenses (Source: IRONSCALES 2019).

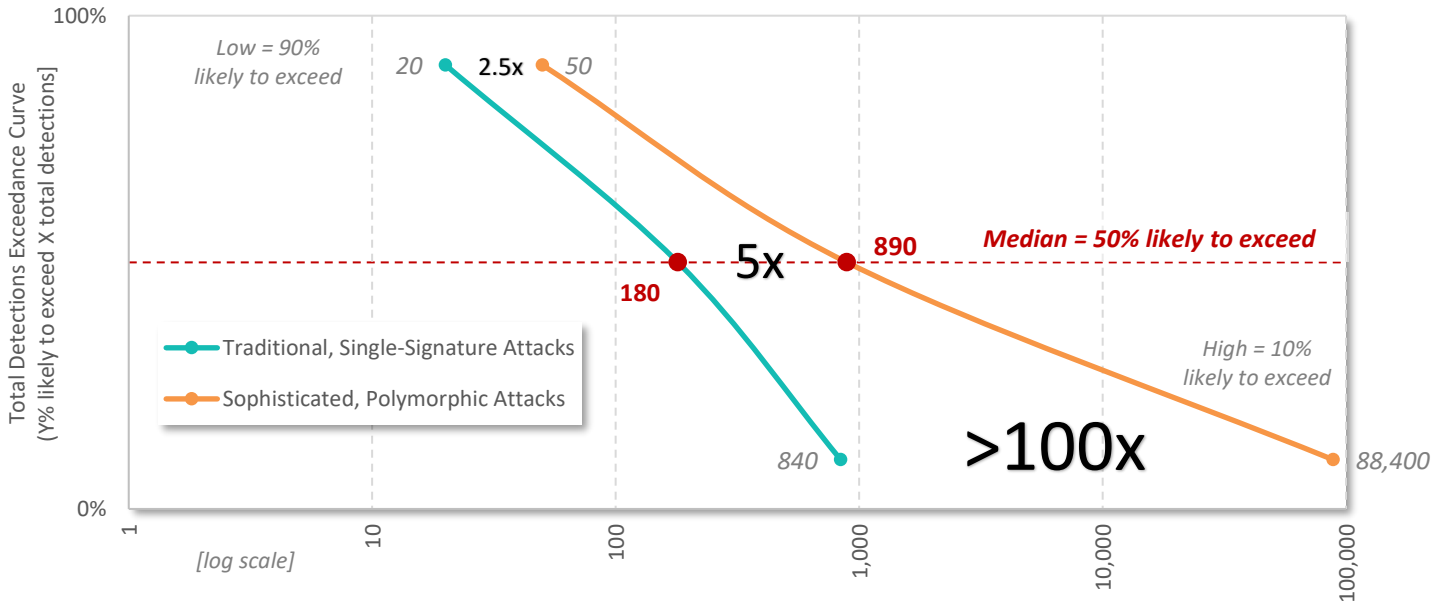
Aberdeen's analysis shows that these techniques can increase the total number of detections required by enterprise defenders — the "blast radius," if you will — by *more than 100 times* compared to traditional, single-signature attacks (see Figure 3).

The obvious insight is that to address these fundamental asymmetries between attackers and defenders, effective email security must also continue to adapt and evolve.

**Every phishing email attack affects multiple mailboxes at multiple organizations — and requires hundreds of successful detections by the email security capabilities of enterprise defenders.**

**It's getting worse. More than 40% of email phishing attacks are polymorphic, which can increase the total number of detections required by enterprise defenders — the "blast radius," if you will — by more than 100 times compared to traditional, single-signature attacks.**

**Figure 3: Polymorphic Phishing Email Attacks are Significantly Increasing the "Blast Radius," Raising the Bar for Email Security**




Source: Empirical data adapted from IRONSCALES 2018-2019; Aberdeen, June 2019

## What Does More Effective Email Security Look Like?

To adapt and evolve with financially motivated and technically sophisticated attackers, effective email security requires a purpose-built blend of *advanced technologies*, *human intelligence*, and *user behaviors* (see Figure 4).

In Aberdeen's view, the two biggest opportunities for more effective email security are found in the following high-level capabilities:

- **Increase the rate of detection / prevention**, based on a blend of
  - **Advanced technologies** (e.g., automation, artificial intelligence, machine learning), to counter polymorphism and other techniques used by ever-evolving attackers;
  - **More effective leverage of human intelligence** (e.g., solution provider services, user reporting, cross-enterprise information sharing), to complement advanced technologies with collaboration by the entire network of defenders; and

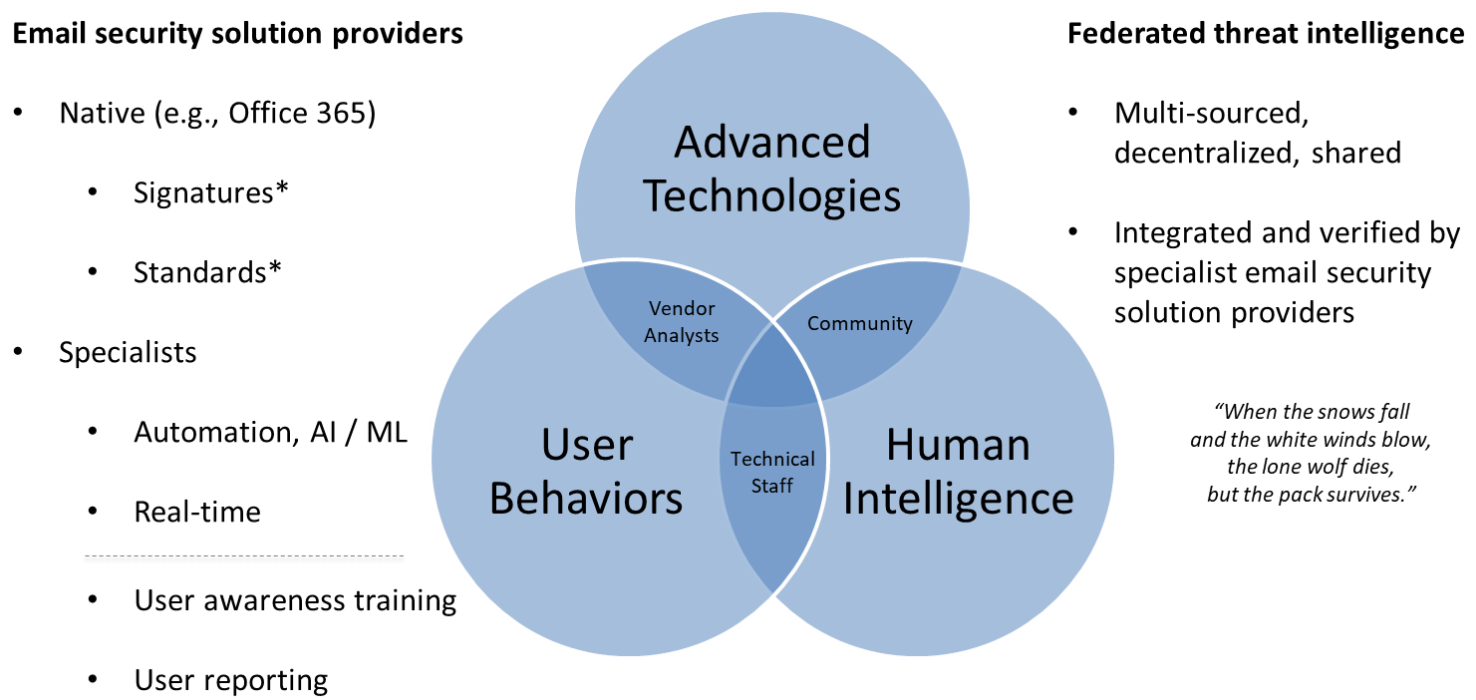
- **Better user behaviors** (e.g., security awareness training), to reduce click rates for the benefit of the enterprise, and to increase proactive reporting for the benefit of all defenders.

- **Accelerate the time to detection / prevention / remediation**, as detailed in the Knowledge Brief *How to Conquer Phishing? Beat the Clock* (September 2018), in which Aberdeen's analysis of empirical data showed 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%. In contrast, the combination of automated, technology-driven **pre-incident protection** and **post-incident protection and remediation** was by far the fastest and most effective approach — quantifiably reducing the organization's risk from phishing attacks by more than 70%, with ongoing upside as technology-based automation, AI, and ML continue to improve.

**Defenders must detect and respond to malicious emails more quickly than their own users are to open them and click on malicious links. Over more than 1,400 simulated phishing attacks, the median time-to-first-click was just 134 seconds.**

In Aberdeen's view, enterprises should establish their email security solution selection criteria — from specialist service providers — in line with the above.

**Figure 4: Effective Email Security Requires a Multi-Pronged Approach**




Source: Aberdeen, June 2019

**Vendor-provided signatures** of phishing email attacks are much too slow to provide an effective defense. For example, a representative sample of

signatures from Microsoft *Advanced Threat Protection* took between 6 days to more than 250 days from the time a phishing email attack was first reported, to the time a signature was made available to enterprise technical staff. In addition, the trend towards sophisticated, polymorphic phishing email attacks makes traditional signature-based approaches only marginally useful.

**Standards-based protocols** such as DMARC (Domain-based Message Authentication, Reporting, and Conformance) can be highly effective against phishing email attacks based on *domain name spoofing*, provided that both senders and receivers are DMARC compliant. For example, in an empirical analysis of more than 100,000 email phishing attacks that successfully evaded the native security of email gateways, less than 1% were based on exact domain name spoofing (Source: IRONSCALES, 2018-2019). Unfortunately, exact domain name spoofing represents only one of the many easily implemented weapons for email phishing attacks in the attacker's arsenal.

## Summary and Key Takeaways

- **Email security matters, as a business issue.** The risk of phishing email attacks can and should be *quantified*, to help senior leaders *make a better-informed business decision*. Aberdeen's analysis explains — in straightforward business terms — why IT and Security teams should be motivated to *re-think their current, ineffective approach to email security*. In addition, it helps to *justify an incremental investment in a more effective email security solution*.

- **Attackers continuously adapt and evolve; defenders must too.** Financially motivated and technically sophisticated attackers continue to adapt and evolve. For example, the most sophisticated attackers are already implementing *polymorphic* phishing email attacks that undergo hundreds of permutations to evade traditional defenses. Aberdeen's analysis shows that these techniques can increase the total number of detections required by enterprise defenders by more than 100 times compared to traditional, single-signature attacks.

- **Effective email security requires a multi-pronged approach.** Going forward, effective email security requires a purpose-built blend of *advanced technologies*, *human intelligence*, and *user behaviors*. Aberdeen's analysis shows that automated, technology-based pre-delivery protection and post-delivery protection and remediation from specialist service providers is by far the fastest and most effective approach. Defenders must also share and leverage multi-sourced, decentralized human intelligence about phishing email threats.

## About Aberdeen

Since 1988, Aberdeen 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. Aberdeen provides intent-based marketing and sales solutions that deliver performance improvements in advertising click-through rates and sales pipelines, resulting in a measurable ROI. Aberdeen is headquartered in Waltham, Massachusetts, USA.



XXXXX