ValiMail

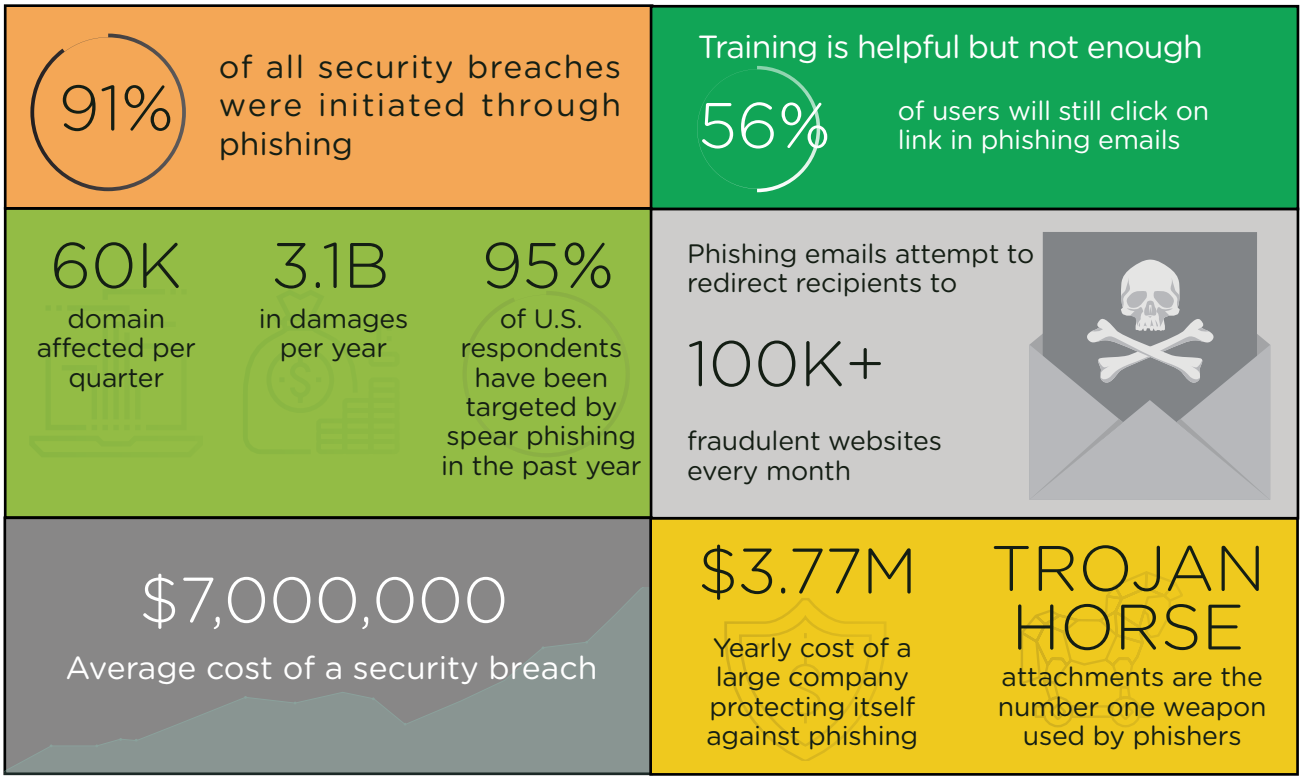
Phishing:
A Clear and Present Danger

For hackers, phishing is the most effective and economical vector for hackers that want to launch a cyberattack on any organization, bar none.

Its utility to hackers is so great that phishing has been implicated in 91% of all breaches. Phishing was the initial vector in the recent WannaCry and NotPetya attacks, as well as serious breaches at the Democratic National Committee, Seagate, Leoni AG, and one sad case of an unnamed U.S. company that lost $98 million in a single email impersonation attack in 2016.

Yet too many IT managers tend to regard phishing as an unavoidable problem and fact of life, like pollution or bad weather. By lumping it in the category of "social engineering," they recognize phishing as a security threat. But instead of stamping it out, they believe that the only effective remedy is user training.

The High Costs of Phishing



180 Montgomery St., Suite 1800
San Francisco, CA 94104

info@valimail.com
www.valimail.com

Unfortunately for them, research shows that training is only slightly effective at reducing risk. In fact, it can even give users a false sense of security and make them more susceptible to a sophisticated phishing attack that's disguised to seem genuine. According to a recent Carnegie Mellon study, training "reduced users' tendency to enter information into phishing webpages by 40%." Since it takes just one successful phish to wreak havoc on a company, a 40% reduction falls far short of being a solution.

There Is a Way to Stop Phishing

There is a technical solution that eliminates an enormous amount of phishing attacks. That is email authentication, which guarantees that any sender using an authenticated domain in the From field of an email message has the explicit permission of the domain owner.

Email authentication actually stops impersonation attacks at the domain level and can literally choke off phishing emails, solving the problem 100% of the time.

For domains that have configured email authentication through DMARC and set it to enforcement, bogus emails that attempt to spoof their domains don't ever reach recipients' inboxes. Messages failing authentication get discarded by mail servers (or quarantined in spam folders) before they even arrive.

With email authentication enabled, hackers can no longer use an organization's own domain (or domains) in phishing attacks.

Hackers can still use similar-looking domains (like yourc0mpany.com instead of yourcompany.com) or completely unrelated domains (like a throwaway Gmail address) but those are far easier for recipients to identify as fraudulent. In fact, many email systems already flag messages that contain lookalike domains that could easily be confused with more prevalent, legitimate domains.

Why ValiMail?

While it is a widely accepted standard, email authentication can be difficult to configure. ValiMail examined over 1 million domains and found that about 70% of all organizations that attempt email authentication don't succeed in getting it to enforcement mode.

ValiMail:
• Automates email authentication as a cloud service
• No drain on your IT team; set it and forget it
• Easy dashboard allows you to manage email sending services • One-click ability to authorize/de-authorize sending services
• Avoids blocking good senders
• Guarantees email authentication

180 Montgomery St., Suite 1800
San Francisco, CA 94104

info@valimail.com
www.valimail.com