TAG CYBER

UNDERSTANDING INKY: USING TRUSTED BANNERS FOR EMAIL SECURITY AWARENESS

EDWARD AMOROSO

Trusted email banners are subtle to implement in a trustworthy manner, but if properly created can significantly improve the likelihood that inbound email messages, including phishes, will be handled appropriately by recipients. The INKY platform exemplifies high-quality delivery and support of trusted email banners

INTRODUCTION

The threat posed to enterprise organizations by phishing is now well-established as a prime vector across which advanced persistent threats (APTs), ransomware attacks, and other serious offensive cyber campaigns are initiated. The good news is that many excellent commercial solutions are available to filter malware, improve authentication, train users, and block suspicious inbound messages. This has helped to reduce the risk – albeit not nearly enough.

The cyber security challenge that remains is that phishing successfully targets one of the most important aspects of email processing. That is, phishing attacks exploit the decision-making process that humans follow regarding how to respond to an inbound message. In particular, when humans receive an inbound email, they must make a thoughtful decision whether to delete, save, postpone, respond, forward, or take some other action.

Automation helps, but ultimately the purpose of most emails is to connect humans together. For this reason, the email process will always be vulnerable to social engineering threats which prey on the trust that humans tend to place in one another. As a result, the most successful anti-phishing methods help email recipients make better personal decisions regarding the inbound messages that actually reach their inbox.

In this report, we introduce a technique that seems obvious – but is more subtle to

implement in a trustworthy manner. The technique involves placing trusted banners on inbound emails to help recipients determine the proper level of integrity. As we will illustrate using a case study analysis of how cyber security vendor INKY[1] implements typical banners, the process will help users make better decisions.

TRUSTED BANNER INSERTION

The use of banners in email is intended to let recipients know that something might be amiss for a given inbound message. An advantage of this approach is that synergy emerges between the security system and users. That is, banners help to educate the user about dangerous aspects of an email, and the user's behavior and guidance can be used to optimize and tune the banner generation.

Today, most enterprise teams put layers of defense in place to prevent bad emails from reaching users. They install secure email gateways (SEGs) and other filters to reduce the risk of malicious message delivery. The target banner use case, however, is that if a suspicious email happens to make it through the security gauntlet, as many do, the banner will help the recipient to understand that the message should not be immediately trusted.

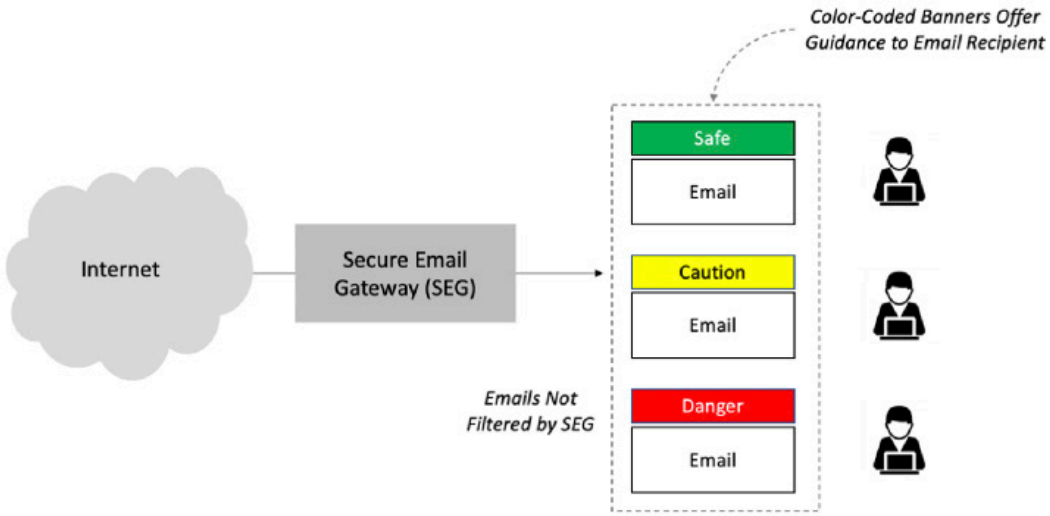

FIGURE 1. Role of Banners in Email Security

It is worth emphasizing that emails that do make it through SEGs and other security protections will generally look realistic. That is, the obvious spam that has clogged inboxes for years are usually filtered out by simple algorithms. It's the more subtle malicious emails - that mimic normal messages from colleagues or customers - that benefit most by the use of banners to alert the user to a detected risk.

INKY IMPLEMENTATION

The commercial email security solution from cyber security vendor INKY includes the use of color-coded banners to reduce the risk of phishing attacks. The platform can perform such insertion because of unique design decision. That is, unlike most commercial security enhancements to Office 365, which use Microsoft's API for access to end-user email traffic, INKY supports banner deployment in-line between the end-user and the SEG.

In addition, because the SEG has become a de facto component of most enterprise security architectures, INKY's deployment has been developed to complement SEG usage and to provide useful security assistance to existing infrastructure. Specifically, the platform generates security scores from a variety of different security modules operating in parallel to the email and then combines the results into an aggregate score.

It is these aspects of the INKY approach – namely, deployment in-line between users and SEGs, and scoring of security risk based on aggregated analysis – that make the insertion of banners possible. That is, by processing the email directly, INKY can insert warning banners and select color codes that are based on the aggregated score. As one might expect, red (dangerous), yellow (caution), and gray (safe)[2] are used to help users understand the risk. Alternative banner technology is binary - either email is "good" and is delivered or "bad" and is blocked. The caution option reduces click through rates and provides an opportunity to train users.

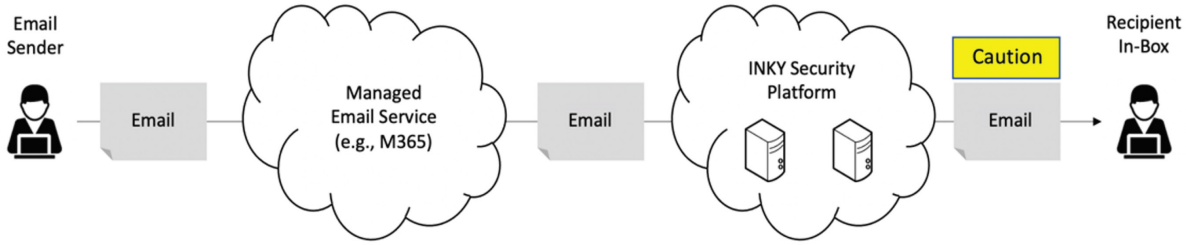

FIGURE 2. Insertion of Color-Coded Email Warning Banners

The INKY platform includes additional advanced security functionality that go beyond insertion of banners (readers are urged to review their website at https://www.inky.com/ for more information). The use of banner insertion, however, does represent an important additional tool for phishing avoidance and general improvement of email security posture, especially for enterprise teams with high consequence of cyber threats.

According to INKY, one of their customers in the oil and gas sector said that clicks on malicious links by end users was reduced by 15-20% a few months after INKY was installed. While INKY does many things automatically, human interactions are valuable. The two-way nature of the communication is important. A recipient using INKY's 'Report This Email' link in the banner helps train the system so that future results are more accurate.

An example extension to the banner capability supported on the INKY platform is that emails can be quarantined rather than delivered if the scoring suggests high risk. This allows the aggregate analysis to reduce the number of emails delivered with yellow or red banners, depending on local preference. In addition, the INKY platform encourages users to report emails if suspicion exists – which can help tune the learning algorithms.

ACTION PLAN FOR ENTERPRISE

It is recommended that enterprise teams engage an action plan immediately to determine if banners might be a useful extension of their existing phish avoidance architecture. The TAG Cyber analyst team recommends the following three steps in such a plan:

Step 1: Review Existing Email Security Program

Enterprise security teams are advised to review their existing email protection program to identify strengths and weaknesses. Like most companies, weaknesses will exist in user awareness of subtle indicators, but many more local issues might be present. Regardless of the specifics, a complete record

of the program should be documented and weaknesses should be prioritized for mitigation.

Step 2: Initiate Planning Discussions with Email Security Vendors

Existing and new commercial security vendors should be included in the planning process for local email security weakness mitigation. As suggested above, user awareness weaknesses are likely to be found, so vendors such as INKY with special notification capabilities, such as banners, should certainly be included in the analysis. The planning roadmap should be heavily influenced by the prioritization developed in the first step.

Step 3: Create Measurable Proof of Concept (POC) Trial Using Banners

The TAG Cyber analyst team strongly advises enterprise security teams to consider running a proof of concept (POC) trial using email warning banners to help notify and inform end users about subtle risks. The POC should include measurable success factors, and as suggested above, INKY provides an excellent experience in this area. Enterprise teams should always take the time to do their research and select vendors with suitable capability.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

[1] *Founded in 2012 by industry expert, Dave Baggett, Rockville-based INKY provides advanced email and anti-phishing security solutions based on artificial intelligence that supports email services such as Microsoft Office 365, Google G-Suite, and Microsoft Exchange.*

[2] *It is worth mentioning that the text used in the banner is sufficient to provide scored information to users. Many people (including the author of this report) are color blind, so this added text is important.*