M3AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP

APWG

Anti-Phishing Best Practices for ISPs and Mailbox Providers

Version 2.01, June 2015

A document jointly produced by the Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG) and the Anti-Phishing Working Group (APWG)

1. Introduction

Phishing is a type of online identity theft that uses email and fraudulent websites that are designed to steal personal data or information such as credit card numbers, passwords, account data or other information. It is a major concern for ISPs and mailbox providers with pressure coming from users who demand that service providers do more to protect them from attacks imitating financial institutions, online games, email providers and many others.

ISPs and mailbox providers now actively participate in globally reducing phishing attempts in order to mitigate customer churn and the potential for litigation. This document describes the best practices used by Messaging, Malware and Mobile Anti-Abuse Working Group members (www.m3aawg.org) to combat phishing attacks.

2. Inbound Protection Schemes

1. Inbound Filtering of Phishing Messages

The most common front-line defense against phishing emails is the use of anti-phishing/anti-spam filtering technology at the first receiving Mail Transport Agent (MTA) or email server. This is usually done using the same anti-spam software that the ISP or mailbox provider already has in place to detect and filter spam.

Several techniques have been developed that are currently used to filter spam. However, they are often designed to catch high volume, low profit, or low customization spam. They frequently do not perform well against lower volume, more highly customized, phishing messages.

In many messaging security systems, spam is tagged and then delivered to either a user's inbox or to a special "spam" folder, which allows users to review a message and personally determine whether it is spam or legitimate email. Unfortunately, it is common for users to see a bank phishing message in their spam folder, assume that the filtering engine made a mistake and click the link to the phisher's site. Therefore, rather than delivering a detected phishing message to users, ISPs and mailbox providers should prevent the user from accessing the message, or at least, from being harmed by it. This action can be accomplished by rejecting the message in the SMTP transaction with a 550 level response; by disabling links, attachments and reply or reply all functionality; or even deleting the message.

Accepting the message and subsequently deleting it successfully prevents the user from accessing it and incorrectly reversing a phishing verdict. However this is a risky approach because if the email filter incorrectly makes a phishing determination, neither the sender nor the receiver knows the message was deleted. The sender assumes the message was delivered while the receiver never realizes that they received a legitimate, and possibly important, message.

Visual cues indicating that a message is authenticated must be used with care. Evidence is inconclusive that they have any effect on user behavior and a poor implementation may reduce user security. Providing cues for all authenticated mail regardless of sender reputation will reduce user security because users confuse authentication with trust. Only a carefully managed system where trusted senders can get visual cues may encourage senders to authenticate mail.

Recommendations:

a. A multi-layered approach to filtering phishing with a combination of some, or all, techniques is recommended. Ideally, ISPs and mailbox providers should compare multiple solutions to determine their efficacy at stopping phishing attacks.

b. Deny or reject phishing messages where possible before accepting the email message.

c. When – due to user request, ISP or mailbox provider policy or legislative requirements – it is not possible to drop messages, ISPs and mailbox providers should indicate to the user those messages identified as phishing messages and, although they might look legitimate, that they are dangerous and should be ignored. ISPs and mailbox providers should further disable links and attachments in the phishing message.

d. ISPS and mailbox providers should rescan messages after they have been delivered to the user's mailbox to allow possible reversal of a previous filtering decision, if later information indicates that the message is phishing.

2. End-Point or Client-Side Filtering

There are several free and commercial end-point security solutions on the market that plug into users' email software and identify phishing messages. In instances where an ISP or mailbox provider is unable to provide server-level phishing filtering, these solutions can be effective. End-point solutions are also recommended so that users can be protected when they are accessing email from multiple accounts, some of which may not reside on the ISP's or mailbox provider's infrastructure.

Also, end-point security solutions are invoked when a user reads their email, as opposed to server-side solutions that are invoked when the mail is delivered. Often, the latency between delivery and processing of mail is long enough for end-point filters to be updated, and hence, provide better security.

Recommendation:

a. ISPs and mailbox providers should encourage their users to employ end-point security solutions such as local email scanning software to combat phishing and anti-malware software to combat malicious attachments.

3. Forgery Detection with Sender Authentication

Email authentication, including Sender Policy Framework[1] (SPF), Domain Keys Identified Mail[2] (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC)[3], is becoming widely adopted. Email authentication can be used to determine if the sender has forged the sender identity. Phishers often try to forge the information in the headers to make it appear as if the message originated from a legitimate institution. Sender authentication, where available, can often be used to detect this.

Recommendations:

a. ISPs and mailbox providers should filter or reject email if they can unequivocally determine that the sender's identity is forged.

b. ISPs should send organizational notification messages and user email from different domains; that is, from notifications@notifications.isp.example and user1@isp.example instead of notifications@isp.example and user1@isp.example. These system notifications should be authenticated using SPF, DKIM and DMARC.

4. Hide Images from Untrusted Sources

To differentiate between trusted senders who transmit legitimate email and phishers who do not, images should be disabled by default and be displayed only when embedded in trusted messages.

Another method of alleviating the threat of phishing is to disable hyperlinks in untrusted email. This makes it more difficult for phishers to trick users into clicking through to a fraudulent site.

Recommendations:

a. ISPs and mailbox providers should turn off images for all messages for which the identity and reputation of the sender cannot be established and provide the user the ability to enable those images.

b. ISPs and mailbox providers should disable remotely-loading HTML content from untrusted sources; e.g., new windows or iFrames.

c. ISPs and mailbox providers should disable all hyperlinks in email from untrusted sources.

[1] http://tools.ietf.org/html/rfc7208
[2] http://tools.ietf.org/html/rfc6376
[3] https://datatracker.ietf.org/doc/draft-kucherawy-dmarc-base/?include_text=1

5. **Block Attachment Types Commonly Used by Malware**

   Malware authors commonly send malware using certain types of attachments in email instead of trying to convince users to click on a link. These attachment types open and execute automatically. By blocking these attachments either at the mail server level or email client, it makes it more difficult for users to accidentally open them and become infected.

   Recommendation:

   a. ISPs and mailbox providers should disable attachment types that are commonly used to send malware. For example, Microsoft Outlook blocks many attachment types by default; see http://office.microsoft.com/en-us/outlook-help/blocked-attachments-in-outlook-HA001229952.aspx.

   b. End users who need to send these types of attachments can send them by providing locations for recipients to download them remotely or by transmitting the file compressed (zipped) and password-protected. Some ISPs and mailbox providers will still block even this attachment.

3. Web Traffic Filtering

Phishing messages often contain one or more links to a phishing website that will collect user credentials. One way to render phishing attacks useless is to block access to these sites. There are several free and commercial efforts underway that provide lists of known phishing URLs to organizations that wish to limit access to these URLs.

Modern Web browsers educate users about the authenticity or fraudulence of websites they visit, which can curb phishing victimization even if users click on links within phishing emails. These browsers examine the links, as well as the content of the Web pages, to make a decision regarding the safety of visited Web pages. All modern browsers also authenticate legitimate websites and instill confidence in users about the safety of their Web experience.

Recommendations:

1. Where possible, ISPs and mailbox providers should enable short-lived blocks on confirmed phishing sites using firewalls and/or Web-filtering products.

2. ISPs and mailbox providers should encourage their users to download the most recent version of Web browsers.

4. Outbound Protection

Phishers often launch their attacks from compromised servers without the knowledge of the owner of the server or the surrounding network. Phishers will either generate phishing emails directly from their own server, through compromised accounts, mail servers, or machines that are not mail servers. In any case, an unsuspecting carrier transports the malicious traffic. Often, these unsuspecting carriers are end-user machines connected to an ISP. As a result, phishers often use the ISP infrastructure to send out phishing emails.

In some circumstances it is within the capabilities of an ISP to filter outbound phishing attempts using anti-phishing filters. Several M^{3}AAWG members have reported great success in using their filtering solutions in "outbound mode" to stop phishing messages from leaving the ISP network. Another advantage of an outbound filter is that it might provide the ISP with a report of the location of phishing Web pages. If these Web pages are installed inside the ISP's infrastructure, the ISP can decide to remove or restrict access to them.

Recommendation:

1. ISPs should consider outbound content filters that prevent phishing messages from leaving their network. When considering an inbound filter, ISPs should also evaluate the outbound capabilities of the solution.

5. Phishing-related Customer Support Calls

Phishing problems inevitably generate support calls. Effective customer support processes and tools can save valuable time.

Recommendations:

1. Remember that phishing and spam are not synonymous. Train your support representatives to recognize the difference. This includes multiple types of scams including 419s (advance-fee fraud) and "my friend is stuck in a foreign country" scams.

2. If a user reports suspicious email asking for personal information, the ISP or mailbox provider should inform the user of the dangers of phishing attacks and warn him or her against giving out personal information online. The user should be further advised to send a copy of the email to the ISP or mailbox provider so it can be used to update filters.

3. If the user believes that he or she has been scammed, the user should be urged to file a complaint with the appropriate anti-fraud organization such as the U.S. Federal Trade Commission (FTC). The APWG maintains a list of anti-fraud organizations at http://docs.apwg.org/resources.html#antifraud.

4. Customer support processes should be in place for quick remediation in cases where a suspected phishing email or site is sent from, or hosted by, the ISP itself.

5. Customer support should also direct users to consumer education resources that enable them to understand the nature and scope of these threats and which describe measures the ISP or mailbox provider is taking to protect users.

6. Customer support should instruct users to change any passwords they may have given away, including other accounts that re-use the same passwords. Users should also be instructed to check their financial accounts for any fraudulent charges.

6. ISP-to-Phishing-Target Communications

Where possible, ISPs and mailbox providers who receive phishing messages impersonating an institution should communicate early knowledge of phishing attacks to the targeted institution.

Recommendations:

1. ISPs and mailbox providers should communicate knowledge of phishing attacks to the targeted institution via the APWG at www.antiphishing.org or via another similar, regional organization.

2. ISPs and mailbox providers should send DMARC aggregate and individual forensic reports to the reported mechanisms specified in the DMARC DNS records, if the message fails DMARC.

3. ISPs and mailbox providers should provide feedback loops that receive submissions when users at other ISPs report a message as spam or phishing and use these feedback loops to disable malicious users.

7. User Education

Phishing messages are difficult for the average user to detect. Mailbox providers, particularly those with valuable information to protect such as large organizations, should invest in anti-phishing training. Your users should know what your policies are, they should be clear, and they should be easy to find.

Recommendations:

1. ISPs should publish Web pages that display anti-phishing education for users or link to another organization's anti-phishing page[4]. Ideally, when a user clicks on a known phishing site, they should be redirected to the anti-phishing page.

2. Large organizations should provide regular anti-phishing training to end users. These can be either internally-developed training or services provided by an anti-phishing educational company.

8. Conclusions

Phishing is a difficult problem to combat. However, by implementing the M^{3}AAWG recommendations contained within this document, ISPs and other mailbox providers can greatly reduce the chances that their users will fall victim to it.

[4] See http://apwg.org/resources/Educate-Your-Customers/ for a list of possible education pages.