Messaging, Malware and Mobile Anti-Abuse Working Group
M^{3}AAWG Best Current Practices for Reporting Phishing URLs

December 2018

Reference URL for this document: www.m3aawg.org/ReportingPhishing

Introduction

"Phishing"—luring internet users to fraudulent websites in order to collect private identity information—continues to be a significant problem for hosting companies, mailbox providers, brand owners and, of course, for every internet user.

This M^{3}AAWG Best Current Practices for Reporting Phishing URLs document is intended to inform all of these groups. It sets out one simple recommendation that everyone should follow if they choose to report a phishing URL. It then, in a question-and-answer format, explains the current ecosystem for tackling phishing and explains why this recommendation has been made.

M^{3}AAWG has one simple recommendation: Phishing URLs should be reported to the APWG (Anti-Phishing Working Group).

The APWG is an international coalition which unifies the global response to cybercrime in general and to phishing in particular. For many years they have operated a "feed" of known phishing URLs. Reports made to the APWG rapidly disseminate, making every relevant party aware of fraudulent URLs.

1. What do you mean by "phishing"?

Phishing was originally a jargon term from the mid-1990s used to refer to emails that impersonated AOL sysops (system operations administrators) to try and obtain users' passwords and, hence, free access. The "ph" seems to have been used in a nod to the even older activity of "phone phreaking."

Here we consider phishing as the enticement of users to visit websites that impersonate well-known brands with a view to persuading them to disclose their access credentials. The enticement usually comes in the form of an email, but there is also phishing on other messaging platforms. It would be much better not to use a jargon term for this type of fraud, but it is too widely used to change now.

2. What is the APWG (Anti-Phishing Working Group)?

The APWG is an international coalition unifying the global response to cybercrime across industry, government, law-enforcement sectors and NGO communities. APWG's membership of more than 1,800 institutions worldwide is as global as its outlook. It was founded in 2003 and has been collating and distributing phishing URLs ever since.

3. How do I make reports to the APWG?

The APWG requests that phishing emails be forwarded as attachments directly to them at reportphishing@apwg.org. Forwarding the phishing email as an attachment allows them to inspect the header details and other information. Alternatively, you can use the Web form on the APWG's reporting page or make arrangements with APWG to submit URLs in bulk. Consult the APWG's instruction page at https://apwg.org/report-phishing/.

4. What if my email report gets blocked?

If email is blocked because it contains a phishing URL, use the APWG Web form. However, if an email system already knows that the URL is associated with phishing, it is very likely that someone has already reported it.

5. What will the APWG do with the reports?

The APWG collates all of the phishing URLs it receives and makes a feed of this data available to its members. Those members include brand owners (who will pick out the phishing URLs that impersonate their brand); brand protection companies that offer specialist services in getting websites removed (who will look for phishing URLs that affect their customers); and blacklist collators (who will put the URLs into their blacklists so that email services and browsers that use these blacklists will be able to block related phishing email, visits to phishing websites, etc.). Other members of APWG include hosting companies (who will remove phishing websites they are unintentionally hosting), URL-shortening services (who will prevent shortened versions of phishing URLs being created) and domain registrars (who will deal with maliciously registered phishing domains).

6. Besides the APWG, should I also make a report …

… to the brand owner?

You can if you wish. The brand owner will start the process of getting the phishing website taken down. However, only reporting it to the brand owner will make it less likely that all the other parts of the anti-phishing ecosystem (blacklist creators, email providers, browser makers, etc.) will learn of the URL. That will reduce overall protection. Reporting to the APWG will reach the brand owner very promptly and also all the other parts of the anti-phishing ecosystem.

… to a brand protection company?

It may be hard for you to determine whether any particular brand protection company has the relevant brand as their customer. Reporting to the APWG will reach all of the brand protection companies in parallel very promptly as well as the rest of the anti-phishing ecosystem.

… using the phishing reporting features of my browser?

You can if you wish. Most browsers have a mechanism for reporting bad websites. However, the browser companies do not generally share the lists of bad sites they learn about, so you will ensure protection for other users of that browser but for no one else. As above, reporting to the APWG will reach all other relevant parties.

… to the website owner?

When websites are insecure they may be compromised and phishing sites added. Reporting to the website owner may be effective, but the owner may be hard to locate. Reporting via the APWG will generally cause a brand protection company to ask for the website to be cleaned up—and their efforts at drawing the attention of the website owner to the problem are likely to be faster and more effective than yours.

… to a "free" webhosting service?

When a phishing website is hosted on a "free" webhosting service, there is usually a form to fill in meant to draw the attention of the service's abuse team to the problem. Reporting to the APWG will generally cause a brand protection company to leap into action and they will make contact with the Web hosting service and ensure that the website is promptly removed.

… to the registrar of a maliciously registered domain name?

Sometimes phishing URLs attempt to look legitimate by using a maliciously registered domain name. In such a case it will be necessary to have the domain name suspended, not just to have phishing website pages removed. Identifying the relevant domain name registrar is straightforward and they should act on abuse reports. However, reporting to the APWG will ensure that a report reaches the registrar in short order.

… to a URL shortening service?

Phishing URLs are sometimes obscured by using a URL-shortening service. This makes it impossible to tell the genuine URL from the destination URL the user lands on if they click through. The major services will prevent the creation of shorteners pointing to malicious websites, so once again the best approach is to make a report to the APWG. This way, all of the shortening services will learn about the phishing website, either directly or because the URL appears on a blacklist.

… to the PhishTank website?

PhishTank is a collaborative clearing house for data and information about phishing on the internet. People can submit suspicious URLs and vote on whether or not they are phishes. PhishTank takes data from the APWG feed, so submissions to the APWG are already effectively submitted to PhishTank.

7. Which URL should be reported?

A phishing email (or some other kind of phishing message) will be crafted to look like a genuine message from a particular brand. It usually asks message recipients to click on a link that leads to a website which will also look genuine—but credentials entered into this website will be delivered to the attacker.

A link is usually embedded in an email as `<a href ="http://BADURL">some text</a>` but in order to mislead, sometimes it will take the form `<a href ="http://BADURL"> http://GOODURL</a>`. It is the `BADURL` (where clicking the link would take you) that should be reported.

8. That was a bit complicated. Can I just report the whole email?

Yes. APWG can accept the entire email, and in fact it can be quite useful to brand owners and anti-spam teams, who can look at the APWG data and see what the original email looked like, not just the URL. However, privacy and data protection issues may mean that sending the whole email is in many cases impossible.

9. Should I report the phishing website URL?

It is often the case that you are redirected from the original URL in the email to another website, and often to a randomly-generated URL on that website. It is important to report the original URL from the email because that will allow the whole chain (be it HTTP forwarding, JavaScript redirecting or other technique) to be mitigated. It might well not be possible to reverse the chain, which means that if you report the final (random) website URL, then it will not be possible to deal with earlier parts of the chain.

10. What if the browser bar shows data: but there is no obvious URL to report?

RFC 2397 standardizes a way of recording data within a URL. It is a technique often used by phishing websites to obscure your location. The location bar of the browser will just display `data:` followed by some apparently random text, rather than the website actually being visited. This makes it hard to check whether it is the intended bank's website or a fake—and makes it difficult to find a URL for the fake website so that it can be reported. But since you will be reporting the URL from the email, this will not matter!

11. What about phishing emails that do not use websites?

Sometimes phishing emails are constructed so that they do not need a phishing website. This is achieved by including all the relevant HTML within the email. When the email is viewed in a webmail system, the phishing page will appear as a form that can be filled in. There will still be a relevant URL within the URL where the HTML `POST` command will send the results of filling in the form (with username, password, etc.) and reporting this will start the process of taking it down. However, there is a difficulty in this case, over and above the technical expertise needed to identify the URL, because, on its own, the URL is not obviously malicious. This may make it harder to persuade relevant abuse teams to take it down. In this case, it is much more effective, whenever possible, to report the whole email because the URL can then be viewed and reported further with the context that shows it is malicious.

12. Is marking a phishing email as spam useful?

Many modern anti-spam systems use machine learning to identify spam. Marking phishing emails as spam provides valuable feedback to the machine learning system that has misclassified an email. This makes it more likely to be correct in the future. However, this is only useful to this particular mail system. Making a report to the APWG, by contrast, ensures that the phishing URL ends up on a relevant blacklist so that the email system will not accept the phishing email at all.

13. I know this URL is a phish. Should I check to see if the website is still up?

When users know they are looking at a phishing email (sometimes it is hard to tell, but often it is pretty obvious) it is very tempting to visit the website just to see what it looks like (and perhaps only make a report if it has not yet been taken down). However, reporting the URL can still be of value whether the site has been removed or not—and a visit to the website is not without risk. From time to time phishing websites will also host malware, and it may be that users' machines will be compromised. Professionals use "throwaway" virtual machine systems to visit phishing websites so as to mitigate the risk.

14. I process lots of email and want to report URLs in bulk.

The APWG is able to accept bulk submissions of phishing URLs and will even allow bulk reporters to label the URLs with a likelihood value that their system has correctly identified a phish.

15. I provide website hosting and want to be proactive about phishing.

Besides monitoring the APWG feed or a relevant blacklist, hosting companies can consider not just removing phishing webpages, but taking advantage of what the APWG refers to as a "teachable moment" to replace them with a special webpage that will tell visitors that they were fortunate not to be misled into revealing their credentials to criminals. The cartoon page supplied by the APWG, in 21 different languages, is the result of rigorous academic research to ensure that it is clear and effective.
More details at: http://education.apwg.org/education-redirect-program/

16. What about more general impersonation of brands?

Impersonation of brands involves persuading users to open documents or visit sites so that malware can be placed onto their machines. This document does not attempt to cover in any detail what is best to do about brand impersonation. The best approach is to make a report to the brand owner, though there may be little they can do in practice. Also excluded from consideration in this document is "spear phishing" (more unhelpful jargon!) where individuals are targeted by individually crafted lures.

Conclusion

Phishing attacks can lead to serious financial and data integrity issues for businesses and internet users. This document has explained how and why to report phishing incidents in the most effective manner in order to have the best chance of reducing the impact of these attacks.

As with all documents that we publish, please check the M^{3}AAWG website (www.m3aawg.org) for updates.

M3AAWG123