International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

Email Tracking Beacon: Concerns and Solutions

[1]Hossin. M., [2]Yew L.K.
Faculty of Computer Science & Information Technology
Universiti Malaysia Sarawak (UNIMAS)
94300 Kota Samarahan, Sarawak, Malaysia

***Abstract*—Email tracking is an essential way to manage the recipients' responses especially in marketing and customer relationship management (CRM). However, the usage of email tracking beacons for monitoring purposes has brought the negative impacts to the security and privacy issues. This paper reveals the working flow of email tracking beacons and discuss the issues regarding to the usage of email beacons. Besides, some of the existing solutions have been reviewed to prevent the email user from being tracked by the email sender. This paper also proposed an alternative solution for tracking email responses without using the email tracking beacon.**

Keywords: Information security; email tracking beacon; email tracking; email monitoring

I. INTRODUCTION

Before the email was born, people were using the paper letters as the main communication tool. The message in the envelope did not have a guarantee in reaching the recipients as the letter may damage in the transportation. The sender had to wait for the reply letter from the recipient to confirm that the message has been successfully delivered.

In 1971, the electronic mail (E-Mail) has been introduced by Ray Tomlinson through his innovative email software named the SNDMSG [1]. The symbol "@" has been used in email address to separate the recipient's name and the location. The "user@host" standard has been used as the format of email address until now.

Email has provided the convenience of sending and receiving messages for replacing traditional letters method. The message deliverability has a better guarantee in ensuring the message delivery. In 2015, there are more than 2 million of users with 16 billion of emails in transaction [2]. In April 2018, this statistic has been increased with 4.1 billion email accounts and 2.5 billion of email users worldwide [3].

Although we have an email, the email sender still has to wait for the reply email from the recipient to confirm the message has been delivered. There are some situations where the recipient has read the email but did not give any response to the sender. Therefore, the email tracking method is used to know when the user has opened the email.

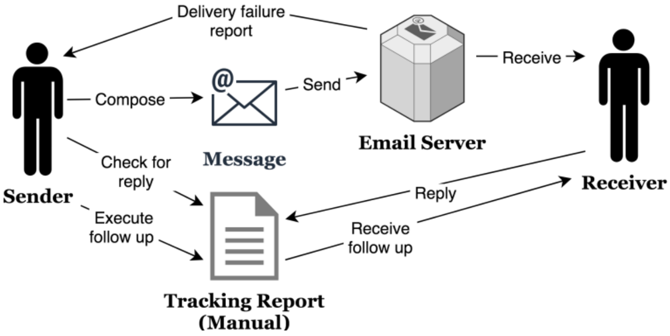


Fig. 1. General email tracking procedure

Figure 1 shows the general email tracking procedure using the manual method. Some company has started the business from the smaller platform, such as Facebook Marketplace. The instant messaging services like WhatsApp and Facebook Messenger came in handy when dealing with the customers. However, when the business scale has increased to a larger platform, the email is still a better conversation tool when dealing with large number of customers and suppliers.

On the other hand, the instant messaging services has provided the tracking function like the "double-blue-ticks" which indicates the recipient has read the message. Nonetheless, most email services did not provide the indicator for the updates of email status. Therefore, some third parties' application or plug-ins have provided the convenience for tracking recipient's responses. The most common method used by the email tracking tool is using the email tracking beacon [4]. Email tracking has never been easier today thanks to the existence of tracking beacon, and there were 40.6% out of 1.5 billion of emails have been tracked. According to the email tracking report which was released in June 2017 [4], the percentage of conversational email tracking was up to 35%, while the subscription type emails was 85%.

The usage of email beacon has become the essential item in email tracking where the sender will be notified when the recipient has opened the email. However, the email beacon has raised some issues regarding to the privacy and security. Besides, the uses of email beacon may reduce the message deliverability rate.

Next section will explain the working logics of the email beacons and some issues regarding its usage. Then, this paper reviews the existing solutions technically. This paper also proposes an alternative solution without using email tracking beacon to trace user email.

II. EMAIL TRACKING BEACON

The email tracking beacon is a very tiny pixel image, also known as the invisible image or tracking pixel. The email beacon will not be visible by the user or recipients in most cases. The email beacon can be viewed when translating the email into its original HTML text file format. The main usage is to allow the sender to know when the recipient has opened the email.

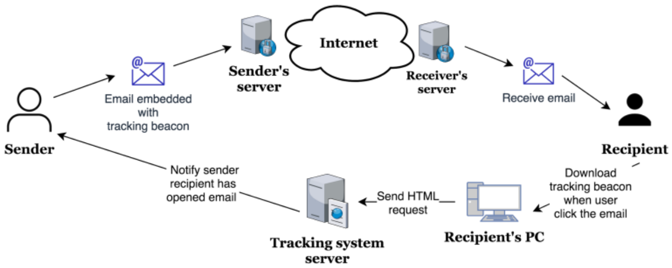

Internet
Sender's server
Receiver's server
Email embedded with tracking beacon
Receive email
Sender
Recipient
Notify sender recipient has opened email
Download tracking beacon when user click the email
Send HTML request
Tracking system server
Recipient's PC

Fig. 2. Email tracking beacon working concept.

The general email tracking working flow is shown in the Figure 2. There are total of three main components which are the sender's email server, recipient's email server and tracking system server [3]. The sender's and recipient's email servers are depending to the email services which they have subscribed to, such as Google Gmail and Microsoft Outlook. Despite the fact that there are some companies are using their own email servers.

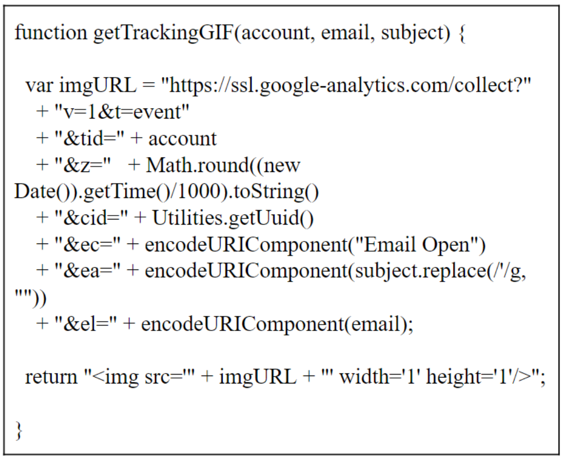
The tracking system server can be provided by the third party services or the sender's own server. When the sender sends an email, an embedded email tracking beacon is included into the email content and sent to the recipient's email server through the internet.

When the recipient clicked to open the email, the email beacon is downloaded into the user's computer. The user information such as opening time and location are logged, then sent to the tracking system server for analysis. The email sender will receive the notification from the tracking system.

The tracking system server will analyze the logged recipient's data and submit a report to the original email sender. The sender can use a dashboard provided by the email tracking services to view and monitor the recipients' responses.

There are three common types of email beacon which are used frequently, small pixel GIF file (1x1 pixels); invisible image embedded with recipient's metadata; URL links embedded with recipient's metadata.

The founder of Digital Inspiration has shown one of the example of email tracking beacon which used the Google Analytics as the tracking system service [5]. This technique uses the combination of Google Apps Script and Google Analytics.



```
function getTrackingGIF(account, email, subject) {

  var imgURL = "https://ssl.google-analytics.com/collect?"
    + "v=1&t=event"
    + "&tid=" + account
    + "&z="   + Math.round((new
Date()).getTime()/1000).toString()
    + "&cid=" + Utilities.getUuid()
    + "&ec=" + encodeURIComponent("Email Open")
    + "&ea=" + encodeURIComponent(subject.replace(/'/g,
""))
    + "&el=" + encodeURIComponent(email);

  return "<img src='" + imgURL + "' width='1' height='1'/>";

}
```

Fig. 3. Google Apps Scripts source code

The scripts as shown in Figure 3 is used to create an email tracking beacon for tracking in Google Analytics. The user has to provide the Google Analytics account identification number, recipient's email address and original email subject into this function. The function will return an email tracking beacon in the form of 1x1 pixel GIF file.

The user will use the Google Analytics as the dashboard for viewing the status. The recipient's location and the time which email is opened are logged into the dashboard.

Next section will discuss the privacy concern issues which has been raised by the usage of email beacons and its disadvantages.

III. PRIVACY CONCERN ISSUES AND DISADVANTAGES

The uses of email tracking beacon have raised the privacy concern as it collects the recipient's metadata through association with email activity, without awareness or approval from the user. In other words, the tracking beacon can be known as a surveillance [3]. The email tracking has becoming an invasion of the user's privacy when the email recipients has been tracked through devices, applications and locations instead of web tracking in traditional marketing strategies [10].

The tracking details can be as detailed as when and where the recipient opened the email. For example, the tracking report can show that the recipient has opened the email on Wednesday, 29th September 2019 in Canada using a MacBook [8].

According to [6], there are about 30% from the emails which used the email tracking beacon services showed the recipient's email address when third parties reviewed it. The further leak may happen when the recipient's click on the email links in the email body.

The information leakage can indirectly lead to phishing email attack. The attackers are able to impersonate the original email sender to deceive the email recipients in providing personal information and credentials for accessing private accounts or bank accounts [13]. The usage of email beacons can lead to serious financial loss indirectly.

For example, in [7] one of the respondent has encountered that his email is being tracked when he receives a call from the email sender a few minutes he after clicked on the email. The results in [7] shows that most email recipients did not know that their activities are being monitored, unless they knew the existence of email beacon in the email content. Cooper Quintin, a privacy advocate in the Electronic Frontier Foundation has defined that the email tracking is definitely a privacy concern.

Another example, the Bananatag, is working as an email tracking service which embedded a 1x1 pixel invisible image in the email and hosted in their server [9]. The cost of using the email tracking service can cost up to $35 per month according to the number of tracked emails.

Some email tracking services like Mailtrack.io and Yet Another Mail Merge has provided the free versions of their services. However, in most cases "If you are not paying for the product, then you are the product" concept has been applied [12]. There is no guaranteed that the data of sender or recipients are well protected in the third party servers, as they need funds from advertisements to maintain the free services.

More importantly, the email tracking beacon may collect users' information which more than just email addresses. The email tracking beacon method provided by [5] also collects the user's location when he or she opens the email.

The Acxiom, Conversant Media, LiveIntent, Neustar, and Litmus Software have been classified as the top five organizations which receives the leaked email addresses [16]. There is one technique named the canvas fingerprinting, which uses the tracking beacon to track user's web history through subscription emails [19]. The marketers also use the cookie syncing which shares the discovered information.

The usage of email tracking beacon can cause the email being rejected by the email recipients. As the privacy issue about email tracking beacon has been raised, hence some company email servers has embedded the algorithm into the server to filter out the email with suspicious embedded image or URL links. The firewalls of the company email server will block all suspicious contents, even the contents might be valuable to the recipients [11]. In short, the message deliverability will be reduced as most tracked emails are being blocked was 85% [4].

In some cases, the email tracking beacons did not guarantee that the email has reached the right person for intended purpose. For example, some company has installed the automation in redirecting emails to the correct department based on the email subject. The email tracking beacon did not guarantee the correct tracking status as most email tracking services did not consider forwarded emails into account [11]. The tracking report might not be accurate if the company has used a different email address for replying the sender's message.

Moreover, when sending a group email which has multiple recipients in a single email, the tracking report normally will only show the number of emails which has been opened. However, the tracking system might not show which recipients has opened the email.

Besides, not all the tracking reports are reliable. For example, the report showed that a recipient has opened the email somewhere in United States. However, the recipient is currently in Singapore. This shows that the email may opened by the recipient's email service provider or company server, which is located in the United States for virus checking purposes. In result, the sender might think that the recipient has away for a trip to United States, which the fact is not.

The small pixel GIF type of email tracking beacons requires the image loading features to be turned on in the recipient's email settings in order to execute its functions in tracking. Some users have disabled the image auto loading function due to limited internet bandwidth (slow connection) and privacy concerns. Hence the sender will not receive any reports if the image does not load automatically and the HTML request is not generated to the email tracking system server.

Next section will discuss about the existing solutions to prevent from being tracked by the email beacons.

IV. EXISTING SOLUTION FROM BEING TRACKED

Before mentioning the methods of preventing from being tracked, users should know how to check manually whether the incoming email is tracked by third party applications. Google Gmail has provided the "show original" option which shows the HTML view of the email. If there are other ".com" domains except the sender's domain, the email has a high possibility being tracked by email tracking services [20].

There are some solutions which have been applied to reduce the possibility of email from being tracked. A research has been done by Steven Englehardt in surveying 16 email clients to identify the behavior of the email providers and the clients [6]. The research has found five possible email beacon tracking technique which are, content proxy; HTML filtering; blocking cookies; blocking referrer; blocking request. These techniques can be applied by three parties which are the email server, the user agent of email and web.

Besides, there is a simpler way which is suggested in the New York Times article, which is adjusting the email settings [9]. One of the type of email beacon is by using the small pixel GIF file, or known as the invisible image. The email users can disable the image rendering in the email settings [9]. When the image is blocked from loading, the embedded link in the GIF file will not work automatically.

The email users who does not use much images in the email conversation can consider to use the plain text email services. The plain text emails will not load any hidden URLs like the HTML emails which may embedded with hidden functions [17]. Some people tends to believe that nothing will happen if he or she did not click anything in the email, but the tracking beacon activity is loaded without awareness of users. Plain text emails are safe from embedded links or images and provide an exact plain words as it arrives [18].

The email tracking beacon can be detected through the phishing email detection applications as the embedded image is considered as an attachment in HTML format. A research paper has proposed a technique which uses the hybrid features to detect the phishing emails [13]. The effectiveness of the technique has proved the accuracy up to 97.25% within the 1000 email, which contains equal numbers of phishing and legitimate emails.

The email users are encouraged not to click on any links in the email content before they have confirmed that the link is safe from tracking. Google Gmail will request for user's permission before loading images in the email. The users can decline the permission to prevent the tracking beacon from being loaded while reading the email [19].

There are some Google Extensions which are able to identify and block incoming emails with tracking beacon for the Google Chrome users such as Block Email Trackers and Ugly Email.

Besides, the iOS device users can disable the "load remote images" option in the default Mail application settings menu [19].

The PixelBlock is a Google Extension which currently has 88,395 of Gmail users in the Google Chrome Web Store. Other extensions such as the Ugly Email will indicate that the email is being tracked, but the service did not stop the tracking process. The PixelBlock will identify and block the tracking pixel, which allows users to view email safely [21].

V. ALTERNATIVE SOLUTION

In this section, we will discuss another possible solution to track and monitor recipient emails without using email tracking beacon. The proposed solution is to use the assumptions for defining the script logics where the email status is identified from the sender's inbox. The defined script logics can be applied through Google Apps Script or JavaScript applications without connecting to third party services or servers for identification. This method is designed to identify the four types of email status which are sent, bounced, replied and out of office.

Sent: When the email is successfully sent from the sender's inbox, the email status is considered as "Sent" as long as the email is not found as "Bounced" status.

Bounced: When the email could not reach the recipient, either the email address is invalid or the email has been rejected by the recipient's email server, the email status is considered as "Bounced".

Mail Server	Email Address (before @)
Microsoft Outlook	postmaster
Google Gmail	mailer-daemon

Fig. 4. Bounced mailer

Figure 4 shows the bounced notification email sender from both Microsoft Outlook and Google Gmail. The bounced notification email is located in the same email thread with the original email. When the recipient's email address is found in the body content of the email sent by the bounced mailer, the email status is considered as "Bounced".

Replied: The email status is considered as "Replied" when a new incoming email is found in the same email thread, with the same email subject as the original email from the recipient.

Out of Office: Out of office notification email is received when the recipient is not actively reading the inbox. The out of office email is not located in the same email thread as the original email. The characteristics of the out of office email are, the email is located in the inbox, but in a different thread as the original email; the email subject contains one of the possible out of office subjects as shown in Figure 5; the email subject contains the original email subject; the sender is the email recipient.

auto	automatic reply	autosvar	automatisk svar
frånvaro	abwesenheitsnotiz	automatisch antwoord	risposta non al computer
away	auto aesponse	respuesta automática	fuori sede
not available	out of office	réponse automatique	out of the office

Fig. 5. Possible out of office subjects

Through this designated track email responses, the email tracking beacon is no longer needed. It means, the email tracking process becomes more secure and maintain the recipient privacy. As we can see in Figure 1, all the tracking and monitoring processes were done manually where it takes more man working hours to handle this. Via this new designated track email responses, all processes in Figure 1 will be fully automated. We believe, with full automation, the man working hours to monitor and track the emails will reduce significantly. All these processes can be depicted as in Figure 6.

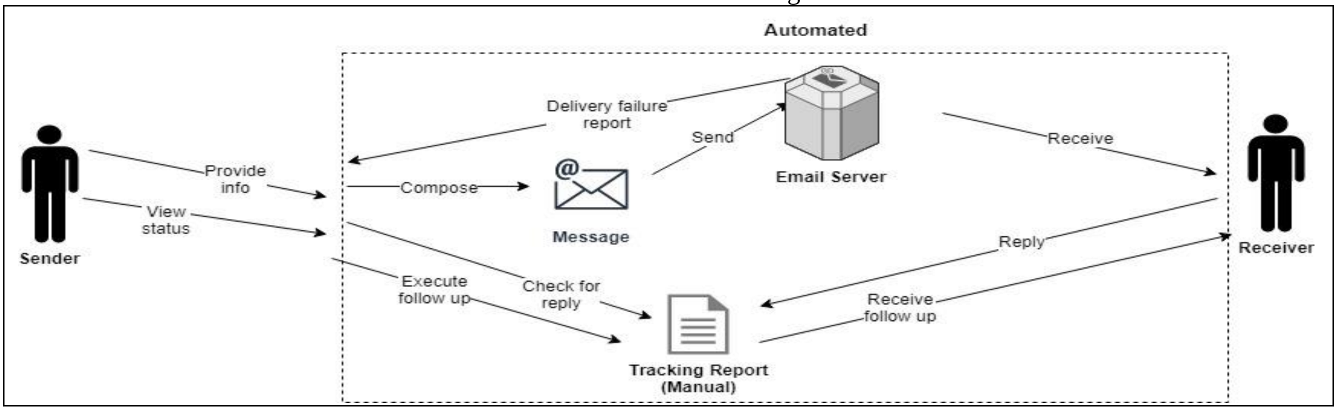


Fig. 6. The Proposed Email Tracking and Monitoring Framework

VI. CONCLUSION

Tracking beacons collects recipient's email metadata without the awareness of user, which can be considered as a surveillance. The privacy and security issue has been raised as email tracking beacons are commonly used in most email tracking services. There are three commonly used tracking beacons which are the small pixel GIF file, invisible image and URL links embedded with recipient's email metadata. The possible ways from being tracked by the email beacons also discussed in this paper. Then, this paper proposes a new framework to track and monitor email without embedding any email tracking beacons. This proposed framework is believed has minimum security and privacy issues. Importantly, we also assume that this framework can reduce the man working hours to track and monitor email manually by making this process fully automated.

ACKNOWLEDGEMENT

This project was fully supported by Universiti of Malaysia Sarawak (UNIMAS). We thank our colleagues from FCSIT, UNIMAS who provided insight and expertise that greatly assisted and improved this project.

REFERENCES

[1] Swatman, R. (2015, August 19). 1971: First Ever Email. Retrieved from http://www.guinnessworldrecords.com/news/60at60/2015/8/1971-first-ever-email-392973

[2] Kooti, F., Aiello, L. M., Grbovic, M., Lerman, K., & Mantrach, A. (2015). Evolution of Conversations in the Age of Email Overload. Proceedings of the 24th International Conference on World Wide Web - WWW '15. doi:10.1145/2736277.2741130

[3] Xu, H., Hao, S., Sari, A., & Wang, H. (2018, 04). Privacy Risk Assessment on Email Tracking. *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. doi:10.1109/infocom.2018.8486432

[4] OMC releases state of email tracking report. (n.d.). Retrieved from https://evercontact.com/special/email-tracking.html

[5] Gmail Tracking with Google Analytics and Apps Script. (2016, March 09). Retrieved from https://ctrlq.org/code/19543-analytics-with-google-script

[6] Englehardt, S., Han, J., & Narayanan, A. (2018, 01). I never signed up for this! Privacy implications of email tracking. Proceedings on Privacy Enhancing Technologies, 2018(1), 109-126. doi:10.1515/popets-2018-0006

[7] Chen, B. X. (2018, January 19). Foiling Electronic Snoops in Email. Retrieved from https://www.nytimes.com/2015/11/19/technology/personaltech/foiling-electronic-snoops-in-email.html

[8] Merchant, B. (2017, December 13). How Email Open Tracking Quietly Took Over the Web. Retrieved from https://www.wired.com/story/how-email-open-tracking-quietly-took-over-the-web

[9] Murphy, K. (2018, January 10). Ways to Avoid Email Tracking. Retrieved from https://www.nytimes.com/2014/12/25/technology/personaltech/ways-to-avoid-email-tracking.html

[10] Haupt, J., Bender, B., Fabian, B., & Lessmann, S. (2018, 11). Robust identification of email tracking: A machine learning approach. European Journal of Operational Research, 271(1), 341-356. doi: 10.1016/j.ejor.2018.05.018

[11] The Truth About Email Attachment Tracking (And How to Do It Better). (2019, March 05). Retrieved from https://www.cirrusinsight.com/blog/email-attachment-tracking

[12] Fitzpatrick, J., & Fitzpatrick, J. (2013, June 24). If You're Not Paying for It; You're the Product. Retrieved from https://lifehacker.com/if-youre-not-paying-for-it-youre-the-product-5697167

[13] Form, L. M., Chiew, K. L., Sze, S. N., & Tiong, W. K. (2015, 08). Phishing email detection technique by using hybrid features. 2015 9th International Conference on IT in Asia (CITA). doi:10.1109/cita.2015.7349818

[14] Five Reasons Why Email Tracking Doesn't Work. (2016, April 12). Retrieved from https://www.docsend.com/blog/email-tracking-doesnt-work/

[15] Is Email Tracking the Next Big Privacy Concern? (n.d.). Retrieved from https://www.mediapost.com/publications/article/311651/is-email-tracking-the-next-big-privacy-concern.html

[16] Smith, & Smith. (2017, October 01). New research details the privacy implications of email tracking. Retrieved from https://www.csoonline.com/article/3229931/new-research-details-the-privacy-implications-of-email-tracking.html

[17] The Difference Between Plain Text and HTML Emails. (n.d.). Retrieved from https://sendcheckit.com/blog/plain-text-emails-vs-html

[18] Bratus, S., & Shubina, A. (2018, September 19). The only safe email is text-only email. Retrieved from http://theconversation.com/the-only-safe-email-is-text-only-email-81434

[19] Do Not Click: Emails Are Tracking You More Than Ever. (2017, June 16). Retrieved from https://www.digitaltrends.com/mobile/email-tracking-online/

[20] How to Detect and Stop Email Tracking. (2019, January 16). Retrieved from https://www.hongkiat.com/blog/detect-disable-email-tracking/

[21] How to Block Email Tracking? (2016, July 16). Retrieved from https://7labs.io/tips-tricks/block-email-tracking.html