Canary Tracker

# BACKGROUND

In the realm of information security, a canary token or honeypot is like a tripwire alarm; you can deploy them where you think bad actors will look for them. If the bad actors then trip the alarm, you will be notified.

A canary token is a customizable link that can be used to alert you when they are clicked on. One of the oldest versions of this technology was baked into some email services - a 1x1 transparent pixel was embedded in the email. When the recipient opened the email, they could not notice the image, but because it was hosted on a server, all sorts of information was logged (date it was accessed, the geographical location of the user, browser information, etc.)[[1]](#footnote-0).

The web has advanced quite a bit, and trackers have taken over our daily browsing ([Ghostery](https://www.ghostery.com/) is a cool web browser extension that really highlights how invasive trackers have become).

This lab will explore just how easy it can be to track people on the internet.

# REQUIREMENTS

A web browser and an internet connection.

# PART I: Understand how the tokens work

1. Once a token is configured, anytime it is “tripped”, the owner will be notified. A lot of information about the visitor will be sent to the owner - anything that can be gleaned from the visitors browser.  
     
   Tokens can be in many different forms (websites, redirects, emails, images, etc.). I have configured a token to be a redirect. You are not required to, but you can click on this link - [daveghidiu.com/security](http://canarytokens.com/tags/feedback/kfecqz91v8lrzdq7fz0j8p5l4/submit.aspx%20%20%E2%86%BB). You will take a quick pit stop at a bespoke canarytokens.org page (which will grab your browser information) and then you’ll almost instantly be shuttled over to daveghidiu.com/security. In the meantime, I’ll get an alert that someone visited the canarytokens.org page and I’ll get a ton of information from the visitor’s computer. The best part is that there is *another* website that tracks all those visits! You can see it [here](https://canarytokens.org/history?token=kfecqz91v8lrzdq7fz0j8p5l4&auth=2a4e2733c1a92e734ac62b9b75c7a5f7); you’ll see when a user clicked on the token, from where, and all sorts of other information.

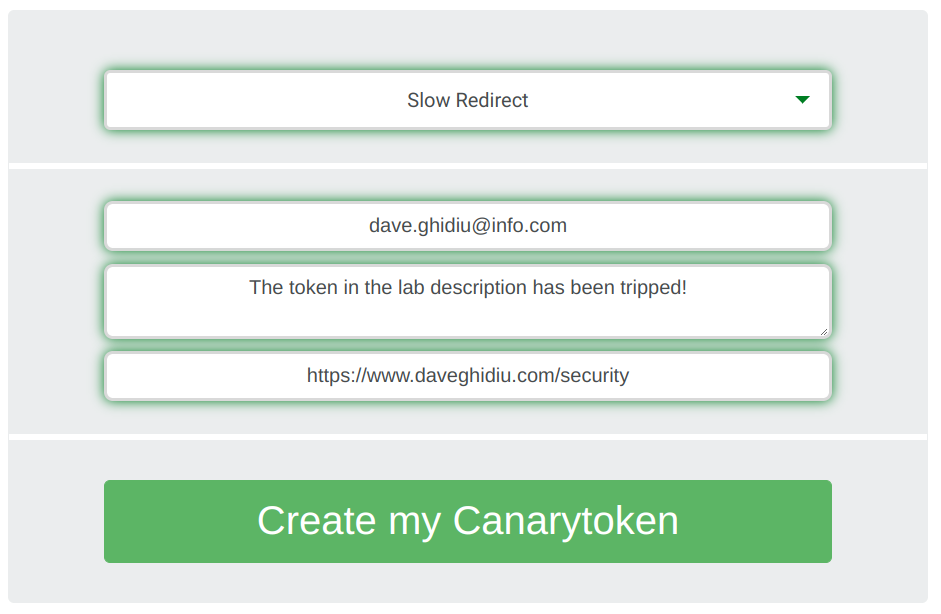
Go ahead and try it! [Trigger the token](http://canarytokens.com/tags/feedback/kfecqz91v8lrzdq7fz0j8p5l4/submit.aspx%20%20%E2%86%BB) and then [view the results](https://canarytokens.org/history?token=kfecqz91v8lrzdq7fz0j8p5l4&auth=2a4e2733c1a92e734ac62b9b75c7a5f7) (again, this is optional). It is worth mentioning that the free canarytokens are public; once you create them, they theoretically could be viewed by anyone.

# PART II: Generate a token

1. Go to [canarytokens.org](https://canarytokens.org/generate) and generate a token. You have a few different menu options, but for this exercise, let’s generate a “Slow Redirect”. Don’t worry - it’s still really fast. Most people won’t even realize what happened.

You’ll need to enter some information, too:

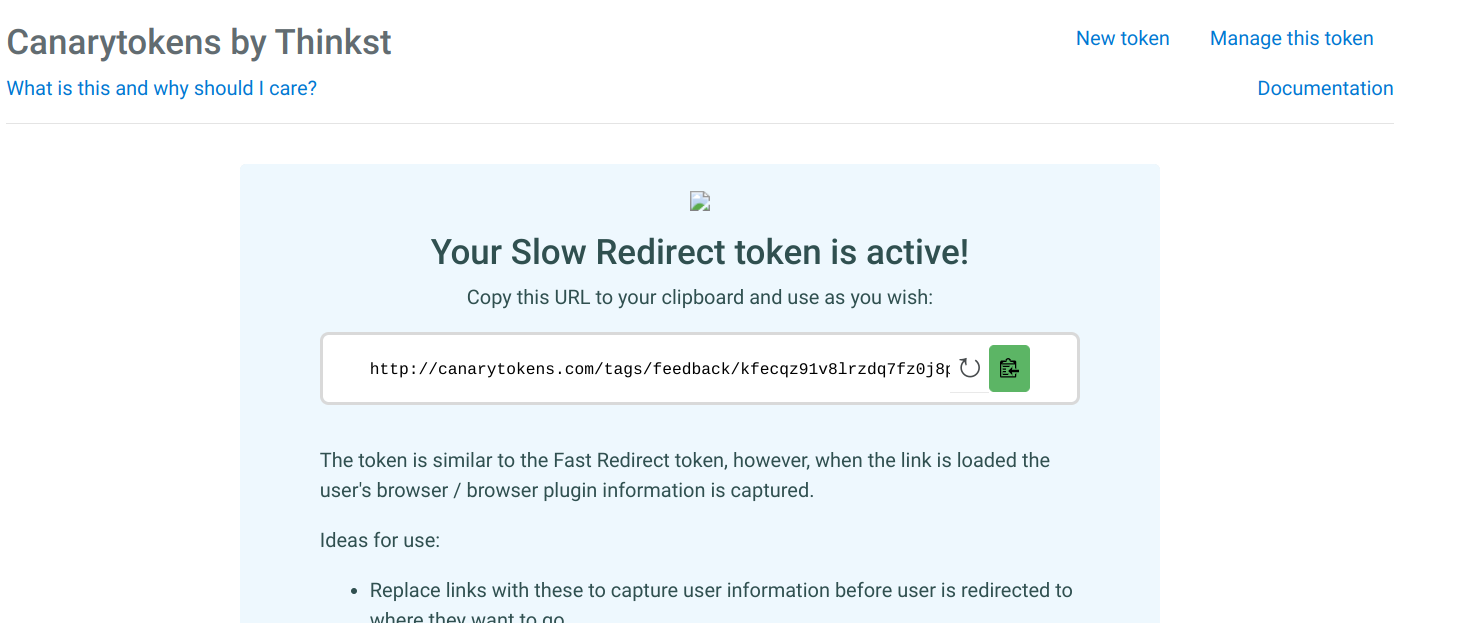
* The email address that will be notified when the token is tripped
* A message to include in the email to help you identify which token was tripped
* The website to redirect to



1. Once you “Create my Canarytoken”, you will be given the actual link for your token. You can make that a hyperlink and embed it on a website, in an email, or anywhere else you would want people to encounter it.

Note also that there is a “Manage this token” link in the upper right; that is the link to your dashboard; don’t lose it!

You should test your token and make sure it is logging properly.



# PART III: Send me the token in an email

1. Send me an email with your token in it. Once I receive it (there may be up to a 48 hour delay), I’ll click on the link and email you back to let you know I clicked on the link. At that point, you will have to go to your dashboard and take a screenshot of my interaction with your token.

| EVIDENCE #1 |
| --- |
| **INSERT A SCREENSHOT OF THE EMAIL WHERE I REPLIED TO YOUR REQUEST** |

1. Once I’ve tripped the alarm, you’ll be notified. Take a screenshot of the notification.

| EVIDENCE #2 |
| --- |
| **INSERT A SCREENSHOT OF THE ALERT** |

1. You’ll have to expand the incident to reveal all the information. Your screenshot should show the location that I clicked from. It’s quite likely you’ll have several hits. In that case, you should cross-reference the timestamp from my email with the timestamp from the events to see where I tripped it from.

| EVIDENCE #3 |
| --- |
| **INSERT A SCREENSHOT OF MY INCIDENT MAKE SURE IT INCLUDES MY LOCATION** |

# FURTHER EXPLORATION

Check out null-byte’s piece on canary tokens for a cool history and some interesting artifacting from the way services like Slack and Twitter process links.

* [Track a Target Using Canary Token Tracking Links](https://null-byte.wonderhowto.com/how-to/track-target-using-canary-token-tracking-links-0192830/)
* [Tracking Pixel](https://en.ryte.com/wiki/Tracking_Pixel) at RyteWiki offers tips on avoiding tracking pixels
* Thinkst (the company that provides CanaryTokens also offers Canary, a solution for monitoring network intrusions) wrote a piece about [why you should care about trackers](https://blog.thinkst.com/p/canarytokensorg-quick-free-detection.html)
* [Null Byte has a sweet YouTube tutorial, too](https://www.youtube.com/watch?v=FNiBNdM7srE)

1. [How Email Open Tracking Quietly Took Over the Web](https://www.wired.com/story/how-email-open-tracking-quietly-took-over-the-web/) [↑](#footnote-ref-0)