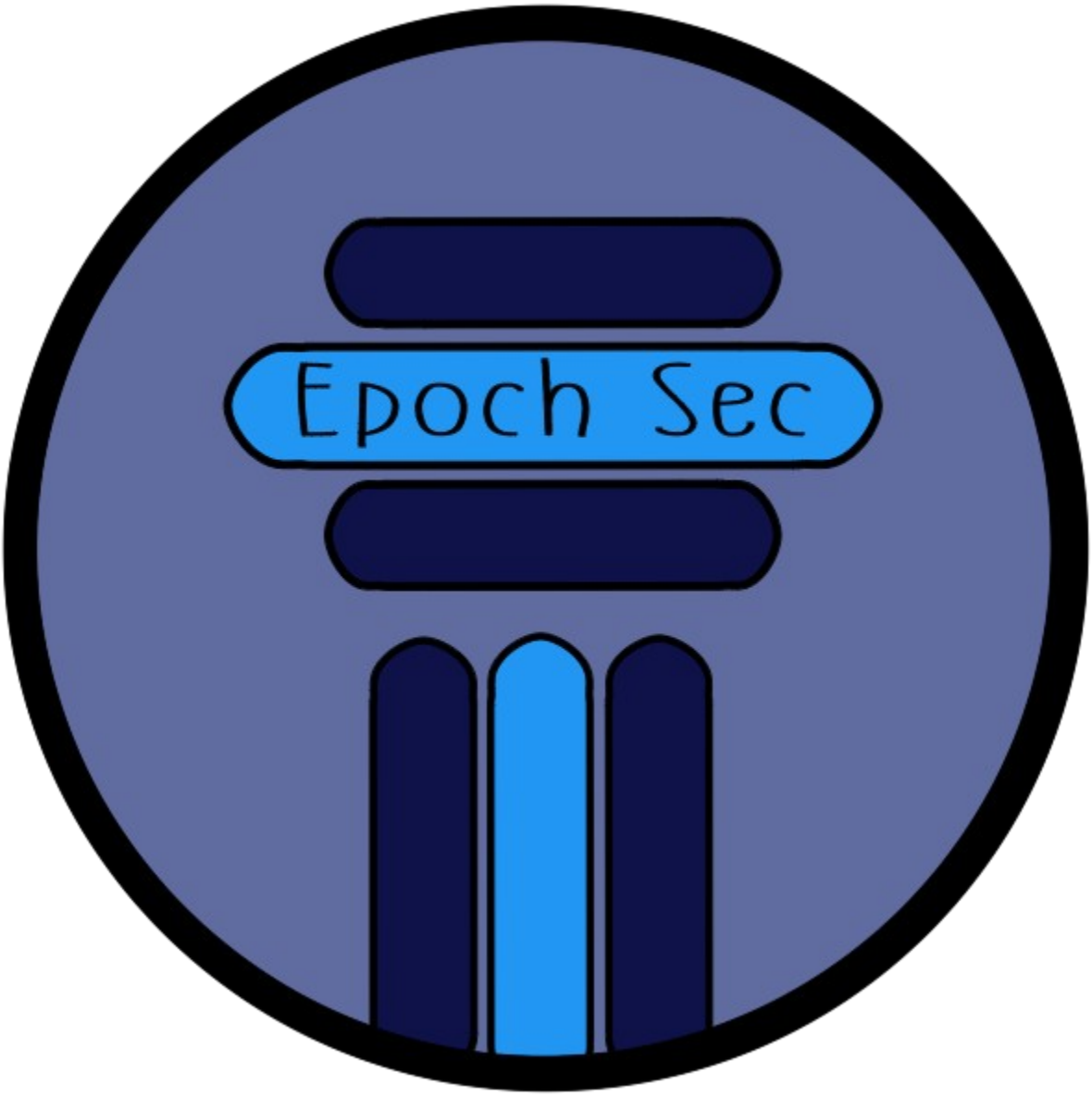

SPOTTING UNSAFE WEBSITES

TABLE OF CONTENTS

OVERVIEW

In this article, I wanted to provide a list of tools/site to use to help identify if something is potentially malicious or safe to use.

These will help aid you in checking websites for safety, learn helpful information about websites, how to report them, and a couple of other tools that I like to use.

Do not ever use just one tool to determine if you believe some thing is safe or not to use. Use multiple methods.

If you do not prefer to read the document, you can watch my video where I walk through each item: https://youtu.be/9wTcWnZDwnw

MALICIOUS OR SAFE WEBSITE?

The first two websites/tools I would suggest using are:

- https://www.virustotal.com/
  - This is a very common tool that is used throughout the Security space. Virus Total allows you to check URLs and domains, upload and check files, and much more. It uses available information from a large database of Security Vendors.
- https://transparencyreport.google.com/safe-browsing/search
  - This is Google's website checker. It is a very easy tool to use to check if a website is safe or not.
- There are many websites out there that have similar functionality, e.g. urlvoid.com. Be careful with using random websites, as you need to verify they are safe to use, before you use them to check other sites.

SECURITY VENDORS

There are many Security Vendors who provide solutions and services for businesses to improve their security posture.
Most of them typically have free, public facing sites or tools that anyone can use to check their databases for malicious or safe websites.

Two examples:

- Sucuri - https://sitecheck.sucuri.net/
- https://sitelookup.mcafee.com/

WEBSITE DETAILS AND INFO

Another key tip is to look up registration information of websites. The majority of the time, personal information is redacted. But you can find useful information.

Such as date of creation or purchase, where the site is hosted, and where it was registered (the registrar).

- The two most commonly used tools:
    - https://who.is/
    - https://lookup.icann.org/en/lookup

REPORTING WEBSITES & MALICIOUS ACTIVITY

With the information learned in the previous section, if something malicious is identified, you can easily file reports.

- Google Reporting Site Tool
    - https://safebrowsing.google.com/safebrowsing/report_phish/?hl=en
- Registrar Reporting
    - You can also go directly to the registrar (found in the previous section with who.is or icann.org)
    - Examples of registrar websites
        - https://www.godaddy.com/help/reporting-abuse-27154
            - godaddy is a commonly known platform for registering websites/domains
        - https://1api.support/en/index.php
            - 1API is a lesser known registrar (at least it was to me). But I wanted to give this alternative example. I actually ran across this one when I was reporting a malicious website that I had been made aware of.

REPORTING AGENCIES

There are also ways to report to law and enforcement agencies. Two example that I am aware of, that I'd like to share are:

- https://www.ic3.gov/Home/ComplaintChoice
- https://www.cisa.gov/report

ADDITIONAL REPORTING AND LOOKUP

This is another popular site that allows you to look up websites, as well as report them

- https://www.abuseipdb.com/

MX TOOLBOX

MX Toolbox is a website full of a suite of tools that can do everything. There is a lot that one can do on this site. Just start playing around with it, and the more you do, the more

comfortable you will become with using MX Toolbox. It is kind of like a one stop shop for many different tasks. Just take a look!

- https://mxtoolbox.com/NetworkTools.aspx

EMAIL HEADER ANALYZERS

Have you ever wanted to better understand an email you received? Where it came from, the path it took, who, etc? Start looking at email headers. Two common analyzers to start with:

- Google - https://toolbox.googleapps.com/apps/messageheader/
- Microsoft - https://appsource.microsoft.com/en-us/product/office/wa104005406?tab=overview&exp=ubp8