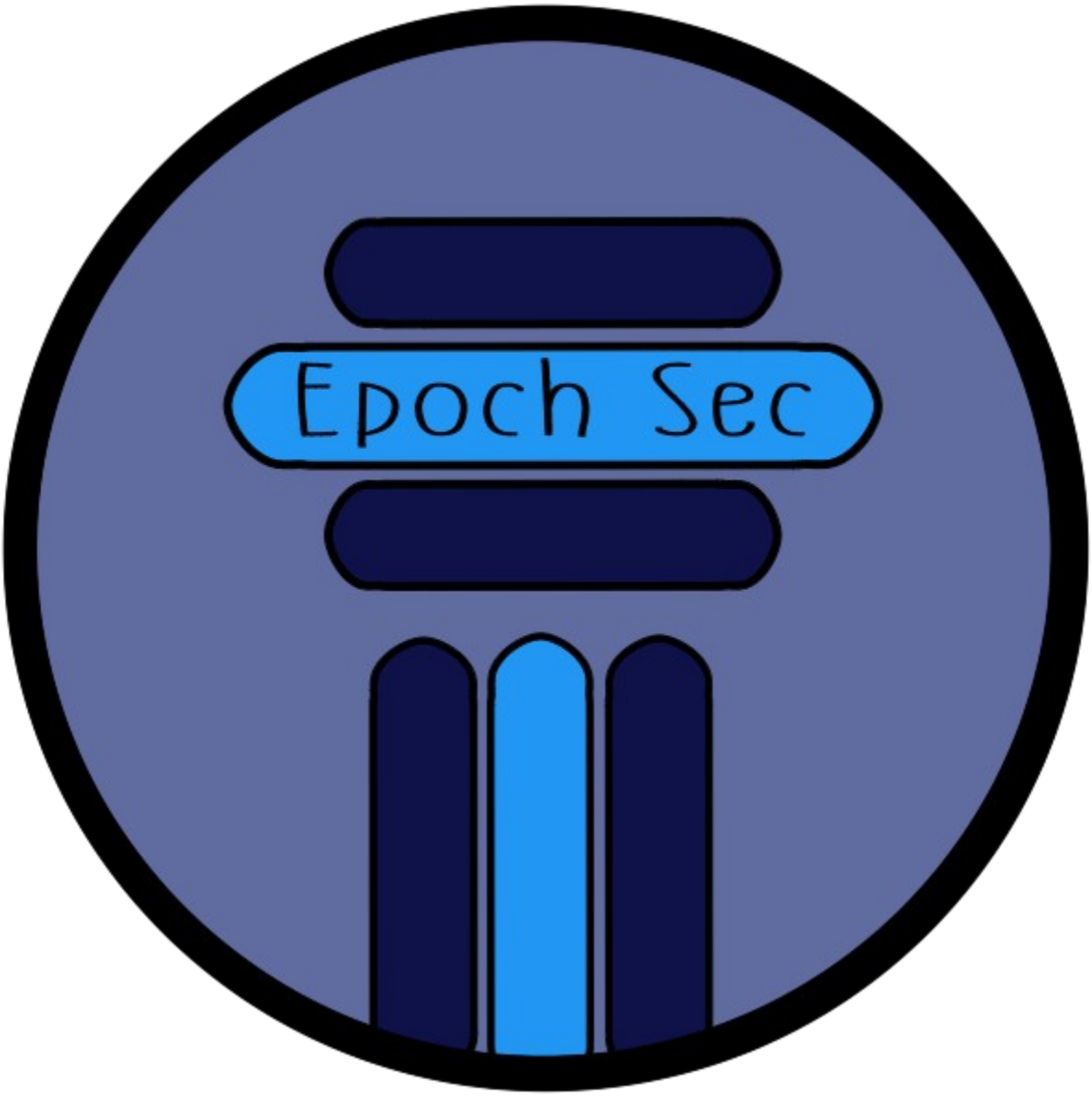

DAILY ACTIVITY – BEST PRACTICES

TABLE OF CONTENTS

OVERVIEW

The overall premise of this document is to give the average user some guidance and direction on better protecting themselves on a routine basis. While we are active in Cardano and Blockchain technology, most of what we do is still interacting with traditional “Web2”, or general internet, activity. Therefore, all of the common attack methods and vectors for bad actors are still present. This document, and most documents will either be an organized bulleted list, or a PowerPoint. I am also discussing with other teams about incorporating my content into their process/application.

STOP CLICKING!

The best and most simple advice I can give is to stop clicking links. This doesn’t mean to never click a link again. However, be very cautious and skeptical of links you find or receive.

- Avoid reacting to messages in social media (i.e. Twitter, Discord, telegram)
- Even if your best friend sends you a link about some project they are looking into, do not click that link. You do not know if your friend could have been socially engineered, unknowingly.
- Go to the source.
    - If you do receive links and you are interested, instead of accepting and using that link, go to the source. Find their official website, or social media, or link tree for example.
    - If you are making a purchase such as a Ledger or Trezor, go the source as well. Do not buy from a third party or anywhere other than their official site/location.
- Hover over hyperlinks. whatever.io
    - If you notice in the hyperlink above, it says whatever.io. But if you hover over it, you will see my website epochsec.io. Be careful and do this for any links messaged to you, links on sites, or even links on the official page for the project
- Example: I left a discord server because I did not trust their administrators to protect their users.
    - Story: I received a message from someone I was not familiar with, and that person sent a rather normal looking message. Instead of engaging, I decided to look into them. I first looked if we shared any other discord servers. I am in a lot of them, and we only shared one. So next I went to that discord server to search that user. I identified them as a “new user”. Discord will tell you that if you click on their profile/name. I also then noticed this person had never said anything in that discord server. The administrators did not feel this was suspicious

CORRELATING INFORMATION

Correlating information means to find multiple pieces of information or evidence from multiple sources to identify a person, project, or of that nature.

- Take multiple areas data gathered and combine it with other information gathered. This is an attempt to build trust or skepticism. Which is correlation.
    - User social media accounts such as Twitter, Discord, or Telegram.
        - Review their activity. Are they very active? How long have they been active? How involved are they? What type of communication do they have? Are they just sharing “buy this ‘crypto’ now, it’s going to pump” messages. Are they involved in the community?
    - What is their general community sentiment? What are others saying?
        - This can be misleading. So as said above, never use this (or any one thing) as enough information. Combine it with other methods of gathered details to make your own determination.
    - Find any interviews. Have they had a YouTube interview? Have they participated in any Twitter Spaces?
    - Do a reverse image search. If you have images of the project, or team members, you can use google images page, click the camera icon, and load an image to search.

USE PUBLIC TOOLS

There are many public tools and sites available to help you validate information that you find. Verify URLs, files, websites, and etc.

Below, I will list some of them. I will also give a visual presentation with these tools, separate from this document. I posted links down below, but verify if they are currently valid at the time of trying to use them. Remember – Go to the source!

- VirusTotal.com
    - This is a free service that analyzes files and URLs for malicious content. The tool also leverages many Security Vendor reports as well. For example, if you were to search a URL on VirusTotal, it will let you know if it aware if the URL is safe, potentially malicious, or malicious, along with green/red marks from each Security Vendor.
    - It is very easy to use this site for URLs or files.
- Sites to looks up Sites. You can look up domain information (or URL information) to see if they are trustworthy, or potentially ownership details, as well as technical details (i.e. various record information like DNS|MX Records|A records, and much more). Some of the more popular options below:
    - lookup.icann.org – lookup domain information
    - who.is
    - godaddy’s who.is database
    - transparencyreport.google.com/safebrowsing

    - sitelookup.mcafee.com (there are many Security Vendors who have these options. Find one you prefer

BROWSERS AND WALLETS

- Do not keep your wallet connected to sites when you are not using those sites.
    - For example, go review your “Dapp Allow List” in Eternl and ensure you are keeping that cleaned up. Any wallet who supported Dapps, should have this option.
        - Also use hardware wallets. Ledger and Trezor as mentioned earlier.
    - Use browser security. As an example, if you are using Brave, go to Settings -> Privacy and Security. Those settings are general easy to understand. If there is something you do not understand, look it up or ask myself.
        - Those settings even have a button to check for breeches, bad extensions, and more.
    - Do not log in with your Google account on your browser. Also, if you do that, do not sync across devices. This can be a potentially dangerous habit.

PASSWORD MANAGER

This is an easy topic to explain, but it did not seem to fit into another section.

- It is common for individuals and teams to use the same account and password for many accounts they have. Another habit to use the same username, but slightly change the password each time a new account is made on a new application, or website, etc. The problem is if a bad actors gains your password, they can then log into any other accounts you may have. Or they can easily brute force additional passwords.
- Use a password manager. Create different, complicated password for every account. We all have many accounts for multiple email accounts, websites, cryto sites, retails site, and so on. But you can use a password manager to maintain your encrypted passwords. Then create another unique password for the password manager. That is then what you routinely use.
    - Examples: Lastpass, Keypass, bitwarden, 1password, and Dashlane.
- Be careful with using password managers, as you would with any other application. For example, Lastpass released that they had user data compromised. I believe that Bitwarden (and possibly 1password) has self hosting.

ADDITIONAL TOPICS

- Be careful opening unknown documents.
    - Go back to the tools section to help with this.

    - Files, upon being accessed, can execute activity. An example here is that Microsoft Office products can run Macros. Macros are used by bad actors to their advantage for their malicious activity.
- Use your Security Software!
    - Linux: UFW and fail2ban are two common options and are great. Security AV products are also widely supported.
    - Windows: Use your AV and your firewall. Nothing is guaranteed to 100% protect you, but everything helps.
    - Apple: The same context above, applies to Apple.
    - It is a misconception that one OS is more safe or more Secure than another. It is all about opportunity and return of investment for bad actors.
- Use YouTube
    - If you don't know something, go search YouTube. I am constantly watching and learning something new.

CONCLUSION

DO NOT BE AFRAID TO MISS AN OPPORTUNITY!

If you are not confident in a project or tool, do not engage and participate until you are confident. I would rather miss 9 out of 10 opportunities, instead of getting compromised 1 out of 100 times. It only takes once.

Keep in mind an easy tactic used by bad actors. That is obfuscation and is used along with Social Engineering and Phishing, which are the two most common attack methods (using vehicles such email, websites, and social media). Obfuscating is taking a domain URL, discord user or server, Twitter Account, or Telegram Account and make a very slight change in hopes that the user/target does not notice. So pay attention!