Anti-Scam Bounty

Task 1: Detection and takedown of scam/phishing sites

This task is an expansion of the previous community initiative. Its goal is for the community to find and take down scam sites that pose a threat to users' DOT or KSM.

Eligible members

- Current members of the initiative (individuals)
- Legal entities (companies) that specialize in this field
- New *individuals* who wish to join the recurring tasks must attain Tier 1 (see below) for two consecutive months, before being admitted as full members.

- If a member doesn't attain Tier 1 for 3 consecutive months or 5 months overall in a one-year period, they'll be removed from the program.

- An *individual* can abstain from the initiative for any period of time without this counting against them, provided they declare it to the curator beforehand. During this time they won't receive the rewards of Tier 0.

- Under special circumstances, to be approved by the curator, an *individual* can declare *reduced* participation for a period of time. In that case failure to attain Tier 1 won't be counted against them, and they'll receive the rewards of Tier 0, as long as they submit at least 1 site per month.

- Individuals can work as teams for this bounty. In that case they need to declare it to the curator and specify a new account to receive the bounty. The account needs to have an on-chain identity as per above. The distribution of the bounty among the members of the team is up to them.

- Legal entities can acquire a "power of attorney" from Web3 Foundation and/or Parity to file DMCAs for trademarks held by W3F and/or Parity. In the future, if other projects/foundations join the initiative they can provide similar "power of attorney" statements for their respective trademarks.

Current implementers

Currently four members of the community, all moderators on Discord, that are already part of the current community initiative have expressed interest in participating as implementers:

[Update May 30, 2022] Removed dubstard (15iZD84rHAjuvaiKXBj2YAEPRJ8Tt4VS1M79HsYhieTvtJR4) who's been removed from the program and added a new implementer, Tim Janssen (1pHpxvp2CYscDreozYQdBkJkUkLFQftxQTAwMs5M1a6GRBf)

[Update July 2022] ccris02 (14fhQS5myHCh3AQZZoELKpQuy2AfNe5am3PzTDvKi7i172n5) has left the bounty

[Update October 2022] Abdulaziz added as implementer (12bprALAt9PYJ5gqcLpLfevnGH1Lfwnkk5CyZYaWqatGJ37i)

- frankywild (13YWynHAu8F8uKZFbQwvPgJ67xizvo21HCEQU3Ke8z1XHoyT)
- pastaMan (14tcZ9ibPGdMwb7XXE4QChgVuJU1xXTvDFpV3E1HpMajbBsH)
- Tim Janssen (1pHpxvp2CYscDreozYQdBkJkUkLFQftxQTAwMs5M1a6GRBf)

(Update January 2024) Tim changed his onchain identity to (1249Qsh72ZcXFjLEDKAp879SfmFpzQMqb1qQKcfkdZgqbt3a)

- Abdulaziz (12bprALAt9PYJ5gqcLpLfevnGH1Lfwnkk5CyZYaWqatGJ37i)

None of the implementers have expressed the intention to work as a team at this point.

The invitation to participate has not been extended to companies at this point, although four of them have been notified about the bounty (PhishFort, Allure Security, Appdetex, Red Point).

Curator

The member of the community that will assume the duties of curator is Chris Malize, Head Ambassador (cmalize#8352 on Discord).

Chris Malize | Head Ambassador Africa
I started to contribute to the Polkadot and Kusama ecosystem in 2019 when I joined the Ambassador program as an apprentice. In 2020, I was promoted to the rank of Head Ambassador Africa. I built a local community in Nigeria, and still manage the community in collaboration with other Ambassadors in my region. I also contribute as Ambassador to other Polkadot ecosystem projects like Astar Network, Bit Country & Subquery. I have always fought scam in the ecosystem.

Account: 1BqHUUwZ6kuRhFZTdbhPwSmwxVnGdCVJTsUf1FU2DXWtEwc
Verified on-chain identity: CMALIZE

Rewards

[Update May 2022]: After evaluating the tasks performed by the implementers and the curator and their respective workloads and responsibilities, it was agreed to adjust the rewards in favour of the implementers, keeping the total reward per site the same. The implementer's reward was adjusted from 1 DOT per site to 1.13 DOT and the curator's reward from 0.33 DOT per site to 0.2 DOT. This change is effective from May 1st, 2022.

[Update: June 11, 2022] The rewards for all tasks have been renominated to USD with the price per DOT set at $20. The rewards below have been updated to reflect that.

Also, a reward ratio per site for the implementers and the curator has been set to 85:15, that will apply to any changes to rewards per site, and there was added a fixed reward per month for the curator, for the general management of the task.

- **Tier 0:** 0-10 sites taken down per month
  Reward: $200
- **Tier 1:** 11+ sites taken down per month
  Reward: $22.6 per site taken down

Curator reward: $500 per month for the management of the bounty + $4 per site submitted

Max Reward per implementer per month: $8000

(update: September 2023) curator reward changed to $3000 max monthly. $500 per month for the management of the bounty + $2 per eligible site submitted.

Max Reward per implementer per month: $6000

- **Tier 0 (old)- Reward:** $22.6 per site
- **Tier 1 - Reward:** $22 per site
- **Tier 2 - Reward:** $15 per site
- **Tier 3 - Reward:** $8 per site

- The implementers' rewards are calculated based on the sites taken down during the month. The curator's reward is calculated based on the sites submitted during the month.

- Any sites reported during the current initiative that haven't been taken down will be added to the child bounties of following months, when they're actually taken down.
- If an implementer gets the maximum reward in a month, any submitted sites that have not been taken down by the end of the month **will not** roll over in subsequent months. To incentivize the takedown of these sites, any other implementer can claim their rewards if they are the first to submit proof of reporting the site to the DNS registrar. **(Update March 15, 2022)**
- **False positives:** Any site that cannot be confirmed as valid (per the rules below) or as active at the time of submission is considered a false positive and is not eligible for reward. Each implementer is allowed a max of 15 sites per month to be false positives. For every false positive beyond that, the implementer will lose $10 from their total rewards which will go to the curator. **(Update March 15, 2022)**

- Curator rewards have been set quite high for this task as it requires quite the effort on their part

Payout

This is a recurring task. On the 1st of each month the curator of the bounty will report the aggregated numbers of sites submitted and taken down by each implementer, along with the rewards they should receive and their own fee.

After reviewing the submission, the General Curator will open one child bounty for each implementer on the 1st (or as close to it as possible). As soon as it's accepted by the Child Curator, the bounty can be paid out.

Details on the submissions of each implementer can be found in this spreadsheet.

Process

1. Any found sites should be reported with a PR to the GitHub phishing repo.

The PR should include in the description the domains added and links to urlscan.io, where the screenshot and the existence of reference in the DOM tab prove they're a scam and their relation to Polkadot/Kusama (example of urlscan proof).

They should also include a screenshot of the site with the date and time of the system clock visible, as proof of the liveness of the site at the time of submission.
[Update: June 11, 2022]

The timestamp of the PR will be proof of the discovery, in case more than one implementer finds the same site(s).

Important: Implementers that also submit sites irrelevant to the bounty should take care to separate those from the ones valid for the bounty and submit them in separate PRs.

2. Then the implementer fills out this form, that automatically fills out the above spreadsheet. As mentioned above, the PR should contain only sites relevant to the bounty.

3. Right after the submission, the implementer starts taking all the necessary actions to take down the offending site, including submitting it to Google Safebrowsing for blocklisting.

4. The curator expands the submission to create one row per site in the PR.

5. Then checks each site for liveness and, if it's live, compares its content to the proof provided. Any sites that are not live are marked as such by the curator in Column H of the **"Form responses"** sheet. **[Update: June 11, 2022]**

6. The curator checks again for liveness at mid-month and at the end of the month any site that hasn't been verified as taken down, from the current or previous months. **[Update: June 11, 2022]**

7. The **"Aggregates"** sheet is populated automatically based on the values of the columns in "Form responses" to calculate the rewards.

8. On the first of each month, the curator must fill out the **"Monthly rewards"** sheet, based on the values produced in "Aggregates", and then update the "Current month" cell in "Aggregates" (cell I2). Then they report these numbers by adding a comment to the bounty page on Polkassembly.

- Implementers can submit valid sites reported to urlscan by other users, provided the sites are live at the time of submission and they provide the relevant proof of liveness **[Update June 11, 2022]**

Valid sites

Any site that poses a threat to users' DOT or KSM is considered valid for submission. More specifically these include:

1. Sites promoting giveaways of DOT or KSM (“send us X and we’ll send you 3X back”).

Important: In this case the implementer also needs to add the site’s advertised address to *address.json* either in the same PR or a different one, for the submission to be valid. If it’s a different PR, the PR for *address.json* should be included in the description of the PR for the submitted site.

2. Generic seed stealers that include one of the following as advertised to “connect/sync”:

- Polkadot
- Kusama
- Parity Signer
- Polkadot JS (extension or UI)
- Other popular third-party wallets specific to the Polkadot ecosystem where users are likely to hold their DOT or KSM (like Polkawallet, Fearless, Talisman etc)

3. Any copycat of the official Polkadot, Kusama, Web3 Foundation or Parity sites not deployed by Web3 Foundation or Parity, even if they have no clear scam intention (beware of staging sites deployed from time to time by Web3 or Parity).

4. Any other site deemed a threat to users’ DOT or KSM (but see the note at the end!)

Invalid sites

At this point, the bounty only covers sites targeting Polkadot and Kusama, so sites like the following are not considered valid:

1. Sites impersonating parachains or posing a threat to holders of their tokens (native or not)
2. Sites impersonating other projects in the ecosystem (unless by doing so they pose a threat to users’ DOT or KSM)
3. Sites posing a threat to DOT or KSM *pegged* tokens on other chains
4. Generic seed stealers that don’t include one of the above tokens/wallets, even if they have “Other wallets” as an option.
5. Sites impersonating multi-asset wallets not specific to the ecosystem, like Imtoken, Exodus, Trustwallet, Enjin, Math Wallet etc., even if these wallets support DOT and/or KSM.
6. Generic seed-stealers that include the aforementioned multi-asset wallets.
7. Investment scam sites that just list assets such as DOT & KSM without asking for users’ mnemonic phrases or otherwise attempting to compromise the users’ accounts.

Clarifications on site validity
1. A site that impersonates a third-party multiasset wallet is **not** eligible, even if that wallet supports Polkadot and/or Kusama
2. A site that impersonates/offers a service to sync/restore/create etc but does not mention Polkadot or Polkadot-specific wallets is **not** eligible, even if it includes multiasset wallets that offer Polkadot, "other wallets", or allows the user to type in their asset/wallet.
3. A site like that that includes Polkadot or Polkadot-specific wallets **is eligible**, regardless of the name it uses in the URL, as long as it doesn't fall in category 1.

Important: The implementers should check with the curator first before submitting a site that's not specifically mentioned as valid or invalid, but they deem a threat to stakeholders. They should make their argument and submit it only if it's deemed valid. **[Update: June 11, 2022]** In any case, the responsibility of proving the threat lies with the implementer and the final judgement whether a submission is valid or not is at the discretion of the curator.

Sites submitted to the repo by others [Update: July 18, 2022]

The implementers will be able to submit for the Task any sites submitted to the phishing repo by people outside the bounty and take upon themselves the responsibility of taking down these sites. To maintain a fair and random distribution of these submissions, the implementers can "claim" any PRs on a daily rotation.

An implementer that submits such a PR to the Task needs to:

1. Check all submitted sites for eligibility and liveness
2. Separate the submissions into eligible, non-eligible and "dead"
3. For the eligible ones, add a urlscan link and a screenshot per the normal submission process/format
4. The curator then adds to the spreadsheet only the "Eligible" sites
5. He marks them as "Yes" under the new "From others" column

The process from then on is the same as all other submissions, but these sites give to the implementers smaller rewards because they didn't find them themselves, which is a big part of the job. The curator gets the same reward, since the process doesn't change for them.

These sites count normally with regard to attaining Tier 1 or against the limit of ineligible submissions.

Implementers' reward per site: $10