



Безопасность в Drophunt

Блок "Drophunt". Урок 10



Что вы узнаете из этого урока:

- Почему нужно соблюдать правила безопасности;
 - Важные правила безопасности, которые помогут уберечь ваши средства и ферму аккаунтов от скама.
-

Почему нужно соблюдать правила безопасности?

Мы с вами все понимаем, что каждый участник крипторынка хочет заработать. Но ввиду отсутствия компетенций или просто по наивности есть риск стать добычей опытных скамеров, которые только и ждут чужих ошибок.

Если в начале пути скам может обойти стороной, то в дальнейшем появляется преувеличенная уверенность в своей безопасности. При этом депозит будет расти, и следующая ошибка будет стоить дороже.

Примеры скама

- // Рассылки в личные сообщения в Telegram или Discord в виде ссылок на скам-сайты, при переходе на которые вас могут попросить подписать сообщение с доступом на вывод всех ваших средств с кошелька.
- // Ссылки на сайты с якобы получением какого-то аирдропа.
- // Предложение помощи и последующая отправка ссылки на фейковый обменник 1inch или PancakeSwap.



Скам-NFT и просьбы зайти на вредоносные сайты, чтобы продать эту NFT.



Сомнительные токены, отражаемые на кошельке.

Ключевые правила безопасности

1. В Telegram - полностью отключить возможность приглашать в группы, а также отключить автоскачивание файлов. Среди них могут быть и вредоносные файлы: даже открытие простого PDF-документа может поставить систему под угрозу.
2. В Discord - отключить личные сообщения в настройках и никогда не читать их: там будет только скам и спам. Исключением может быть общение с администрацией проекта при участии в амбассадорских программах (но обязательно нужно сверять никнеймы).
3. Discord часто взламывают и размещают в официальных каналах фишинговые ссылки. Не спешите переходить по тем ссылкам, которые вы только что увидели.
4. Если на каком-то Discord-сервере просят подключить свой кошелек, то лучше убедиться в том, что это правильный Discord.
5. Twitter - в настройках уведомлений отключить уведомления от тех людей, на которых не подписаны.
6. Использовать длинные и надежные пароли от 12 и выше символов, включая буквы верхнего и нижнего регистров, цифры и символы.
7. Использовать биометрию и двухфакторную аутентификацию.

8. Не заниматься пиратством на рабочих машинах, где хранятся данные от кошельков, бирж.
9. Использовать надежный платный антивирус (например, Kasperskiy или Malwarebytes).
10. При работе с финансами по возможности перейти на продукцию Apple. MacOS и iOS менее уязвимы и больше защищены от различных угроз.

Основные выводы



Никто не заинтересован в том, чтобы бескорыстно предлагать возможность заработать. Чтобы уменьшить поток скам-предложений, можно отключить личные сообщения в Discord, возможность упомянуть вас тем аккаунтам, на которых вы не подписаны в Twitter, и возможность приглашать в группы в Telegram.



Вся информация, все токены для покупки, все аирдропы и остальные настоящие выгодные предложения никогда не обойдут стороной, если находиться в правильном инфополе.



Необходимо взять ответственность за свой успех на себя.



Нужно соблюдать все правила цифровой гигиены: использовать длинные и надежные пароли, использовать биометрию и двухфакторную аутентификацию, не скачивать пиратские файлы, использовать платный антивирус.