Мошенники регистрируют новые аккаунты и с них пишут оскорбительные комментарии под публикациями и всячески провоцируют жертв на ответные грубости. Только ссылки, которые злоумышленники оставляют на виду якобы для перехода для ответов им в другие соцсети, на самом деле являются вредоносными.

По словам замдиректора центра мониторинга внешних цифровых угроз Solar Aura ГК «Солар» Александра Вураско, потенциально эта схема может работать и вдругих соцсетях и мессенджерах. Эксперт посоветовал стараться не реагировать на хейт, а если всё же пользователь хочет ответить, необходимо проверять домены на соответствие реальному адресу соцсетей.

«Если пользователь решит зайти на страницу "хейтера", то обнаружит, что личная страница обидчика закрыта. При этом в описании профиля есть ссылка, которая якобы перенаправляет на аккаунт в другой социальной сети. Но стоит перейти по ней и авторизоваться — мошенник тут же получит доступ к странице жертвы и сможет использовать её для обмана других пользователей», — пояснил Вураско.

* организация признана экстремистской, её деятельность запрещена на территории России.

Все права защищены