

Персональные данные

Не передавайте свои персональные данные незнакомым людям, включая **адрес, номер телефона, пароли, одноразовые коды и любую другую личную информацию**, – даже если собеседник представляется специалистом службы поддержки или продавцом маркетплейса.

* * * * *



Служба поддержки

Если подозреваете, что столкнулись с мошенническим ресурсом – **напишите в службу поддержки маркетплейса** в чате приложения или на сайте, специалисты помогут разобраться в ситуации.



Отличия официальных ресурсов от скам-сайтов

- * Скам-сайты часто *маскируются под маркет-плейс* или проводят фейковые розыгрыши на ресурсе, выдающем себя за официальный.
- * Внешне скам-сайт может копировать настоящий, но он будет отличаться незначительными деталями: *лишней буквой в названии сайта или нестандартной доменной зоной.*
- * На официальном сайте *вы всегда сможете изменить фильтр и перейти в другие разделы.* На скам-ресурсе чаще всего действия ограничиваются одной страницей.

Ссылки от незнакомцев

- * Не переходите по ссылкам от незнакомых людей в мессенджерах или почте, а также всегда обращайтесь внимание на адрес отправителя.
- * Маркетплейс *не устраивает закрытых распродаж* или розыгрыши скидок, не отправляет *ссылки на оплату товаров в личные сообщения*.
- * Также остерегайтесь *предложений о работе с чрезмерно высоким доходом* – скорее всего, пишут мошенники.

Надежный пароль и двухфакторная аутентификация

Важно придумать *надежный пароль* и по возможности *включить двухфакторную аутентификацию* для входа в личный кабинет на маркетплейсах.

Также *не стоит привязывать к профилю основную банковскую карту*. Лучше привязать ту, на которую будете переводить нужную сумму для покупки.

Угрозы «серых» SIM-карт и VPN-сервисов



Дело в том, что *«серые» SIM-карты могут быть зарегистрированы на подставное физическое или юридическое лицо, то есть на мошенников.*

Что касается *VPN-сервисов, из-за них может произойти утечка персональных данных в открытый доступ.* Либо разработчик VPN-сервиса передаст ваши данные третьим лицам, среди которых могут оказаться злоумышленники.

Сомнительные предложения об удаленной работе в ИТ

Злоумышленники начали размещать в интернете от имени российских ИТ-компаний поддельные предложения об удаленной работе.



Большая часть подобных предложений публикуется в профильных Telegram-каналах с вакансиями.

Если пользователя заинтересовало подобное приложение, мошенники предлагают ему перейти по ссылке, чтобы заполнить Google-форму. В ней он оставляет свои контактные данные.

Несуществующая «Единая медицинская служба»

Мошенники начали представляться сотрудниками «Единой медицинской службы». Однако такой организации не существует.



Злоумышленники звонят потенциальной жертве, чтобы поинтересоваться у нее, когда она проходила флюорографию. Если человек отвечает, что обследование он прошел в 2024 году, аферисты сообщают ему, что в системе организации произошел сбой, поэтому в ее базе остались результаты только за 2022 год. В связи с этим мошенники просят человека продиктовать СНИЛС или код из SMS.

Цель таких манипуляций - получить доступ к аккаунту пользователя на портале «Госуслуги».

Угрозы «серых» SIM-карт и VPN-сервисов

Эксперты РОЦИТ напоминают:

чтобы обезопасить свои персональные данные и деньги, *не стоит использовать «серые» SIM-карты и VPN-сервисы* для совершения покупок, входа в банковские приложения, на портал «Госуслуги» и иные ресурсы, где *содержится ваша чувствительная информация.*

Сомнительные предложения об удаленной работе в ИТ



Бывает, что аферисты предлагают человеку сразу же связаться с HR-менеджером, чтобы пройти собеседование.

Затем, когда оно успешно пройдено, с человеком уже связывается якобы сотрудник бухгалтерии ИТ-компании. Он предлагает будущему работнику привязать телефонный номер корпоративной SIM-карты к личному кабинету банка, чтобы тот сразу начал получать зарплату с первого дня трудовой деятельности.

Если человек это делает, мошенники незамедлительно крадут его деньги с банковского счета.

МОШЕННИКИ НЕ ДРЕМЛЮТ: НОВЫЕ СХЕМЫ ОТ ЗЛОУМЫШЛЕННИКОВ

Комментируют эксперты РОЦИТ



© РОЦИТ