«Вы выиграли приз от мобильного приложения»

Надежда, Обнинск

Учу английский в одном из мобильных приложений. Но там можно заниматься бесплатно только по 5 минут каждые 10 часов. Иногда минуты дарят бонусом.

Недавно в приложении вылез рекламный баннер с сообщением: «Вы выиграли приз, откройте и посмотрите, что там». Я подумала – скорее всего, еще бонусные минуты дают, и нажала.

На экране появились коробки и надо было угадать, в какой из них приз. Всего давали три попытки. И вот я выиграла 3060$. Затем открылось окно с поздравлениями. Еще появился чат, где другие пользователи радовались, что тоже получили деньги в этом розыгрыше. Кто-то мало, кто-то много, но даже те, кто ничего не выиграл, радовались за остальных.

Участники обсуждали, кто как забирал приз. Я вообще-то сразу подозревала, что это развод, но когда увидела, что за вывод денег надо платить комиссию, сомнений не осталось. Ничего нажимать не стала, все закрыла. Как говорится, бесплатный сыр бывает только в мышеловке.

Заскринила фото «представителя розыгрыша» из чата. С помощью поиска по картинке узнала, что это фото, которое под разными именами используют еще в нескольких сомнительных историях. Опять же признак обмана.

Баннеры в моем приложении для изучения языков – это место для рекламы, и оказалось, что один из баннеров проплатили мошенники. Сейчас в большинстве бесплатных приложений приходится смотреть рекламные ролики. Вот и вылезает всякая дрянь. Не хочешь – плати за премиум-аккаунт.

Желаю всем быть внимательнее с баннерами и всплывающими окнами, чтобы не угодить к мошенникам.

Совет эксперта по противодействию мошенничеству:

Обычно аферисты рассылают людям письма счастья о беспроигрышных лотереях по электронной почте и в мессенджерах. Но все чаще они ищут потенциальных жертв несколько иначе – выкупают рекламные баннеры на различных сайтах и в популярных мобильных приложениях.

Сами сайты и приложения могут быть вполне безобидными – их разработчики не задаются целью обмануть пользователей и украсть деньги. Но они живут за счет продажи рекламы и не всегда тщательно проверяют своих рекламодателей.

Киберпреступники рассчитывают, что баннер внутри знакомой программы не вызовет у людей никаких подозрений. Пользователи поверят обещаниям призов и перейдут по ссылке. А оказавшись на мошенническом сайте, клюнут на сказочные выигрыши и фейковые отзывы восторженных счастливцев.

Как правило, перед получением приза требуется оплатить небольшую комиссию. А для этого – ввести полные реквизиты своей банковской карты на фишинговой странице.

Если бы Надежда не распознала обман и последовала инструкции аферистов, то открыла бы им доступ ко всем деньгам на своей карте.

Но даже просто кликать на подозрительные рекламные баннеры опасно – можно скачать вирус, который крадет с устройств логины и пароли от онлайн-банка и перехватывает сообщения с кодами подтверждения операций.

Чтобы не потерять деньги, важно всегда сохранять бдительность и следовать правилам кибербезопасности:

- Скачивайте приложения только из официальных магазинов, таких как Google Play и App Store. Предварительно изучите, как давно появилось приложение, какой у него рейтинг и сколько пользователей. Если программа существует уже несколько лет, у нее высокие оценки и сотни тысяч скачиваний, можно рассчитывать на ее безопасность. И наоборот – не стоит скачивать приложение, которое создано совсем недавно, набрало пару сотен пользователей, и те не слишком им довольны. Конечно, могут быть исключения – лучше дополнительно почитать комментарии и отзывы на независимых форумах.

- После установки продолжайте следить за поведением программы. Если заметите странности вроде запроса новых данных или подозрительных рекламных баннеров, лучше удалить это приложение и поискать безопасный аналог. О недобросовестной работе программы стоит написать отзыв в магазине приложений.

- Установите антивирус на все устройства, которыми пользуетесь, и регулярно его обновляйте. Но даже после этого не стоит терять бдительность – хакеры постоянно изобретают новые способы атак и защита все же может пропустить вредоносную программу. И уж точно антивирус не спасет, если вы сами передадите мошенникам свои конфиденциальные данные. Важно самому всегда быть начеку.

- Не спешите кликать по рекламным баннерам, не переходите по ссылкам от незнакомцев и не вводите данные банковской карты на подозрительных страницах.