«Заработай на айфон всего за неделю!»

Паша, Белгород

Мой одноклассник однажды нарвался на мошенников. Он упрашивал родителей купить ему новый айфон, но его мама сказала, что слишком дорого, максимум прошлогодний купят. И то, если хорошо четверть закончит.

Короче он стал искать, где купить новый, но дешевле, и нашел интересное объявление. Типа можно быстро заработать на новый айфон, всего за неделю. Надо зарегиться на сайте и писать отзывы ко всяким товарам, скачивать приложения и проходить опросы. Ну все изи. Начал скачивать, другие задания выполнять. И хоба, в личном кабинете накапало 37 тыщ рублей дней за пять. Он подумал, еще немного и реально купит айфон. Но когда решил снять эти деньги, у него ничего не получилось. Там надо было ввести номер телефона, ему пришла смска со ссылкой, он кликнул и у него баланс телефона сразу в минус 200 рублей ушел. Личный кабинет на том сайте залочился, а все, что он там накопил, пропало. Я потом на этот сайт тоже попробовал зайти, а он уже не работает.

Совет эксперта по противодействию мошенничеству:

Мошенники часто заманивают в свои схемы «супервыгодными» предложениями. Обещают быстрое обогащение и легкий заработок. Но в итоге в плюсе остаются только сами махинаторы.

На этот раз они решили не просто выманить чужие деньги, но еще и заполучить бесплатную рабочую силу. Мошенники используют человека в своих целях: нагнать просмотры на различные сайты или быстро собрать отзывы для продвижения товаров или услуг в интернете.

Человек выполняет несложные задания и думает, что получит за это денежное вознаграждение. Но в его личном кабинете копятся баллы, как в онлайн-игре, а не рубли, и получить их он не сможет. Аккаунт блокируют, когда человек пытается вывести свой «заработок».

На прощание аферисты снимают деньги с баланса его мобильного телефона: присылают СМС со ссылкой, и если по ней перейти, человек невольно подтвердит списание.

Махинаторы могут также предложить, например, оплатить небольшую комиссию для вывода денег из личного кабинета. После того как пользователь введет данные своей банковской карты для оплаты комиссии на фишинговой странице, преступники получат доступ к счету и смогут списать все, что там есть.

В итоге желание быстро заработать оборачивается потерей денег и времени.

Чтобы не попасться на удочку онлайн-аферистов, важно соблюдать правила кибергигиены:

- Не доверяйте объявлениям о быстром обогащении — это явный признак мошенничества.

- Не оставляйте на сомнительных сайтах личные данные (ФИО, номер паспорта и мобильного телефона), не вводите полные реквизиты банковской карты (номер, срок действия, трехзначный код с обратной стороны), а также пароли и коды из сообщений от банка.

- Прежде чем оплачивать что-либо в интернете, сначала убедитесь, что перед вами не фишинговая страница. Мошенники часто копируют сайты известных онлайн-магазинов, банков и других популярных ресурсов.

- Не переходите по подозрительным ссылкам из сообщений от незнакомцев.

- Настройте антивирусы на всех гаджетах, которыми пользуетесь. На телефонах, компьютерах или планшетах маленьких детей можно установить программы родительского контроля, чтобы обезопасить их от посещения сомнительных сайтов.

- Не храните большие суммы на карте, которой регулярно расплачиваетесь в интернете. Лучше использовать отдельную карту для онлайн-шопинга и переводить на нее только сумму покупки. Родители могут ограничить сумму или количество операций по банковской карте своего ребенка — так у мошенников будет гораздо меньше шансов завладеть всеми его деньгами.