«Хорошая работа для вас. Включите демонстрацию экрана»

Анна, Смоленск

Подозреваю, что мне звонили мошенники, но в чем суть схемы так и не поняла, помогите разобраться. Звонок был с незнакомого номера, человек обратился ко мне по имени-отчеству, представился сотрудником одной известной компании и предложил неплохой вариант подработки. Нужно писать небольшие тексты для их сайта, затраты по времени небольшие – где-то полчаса в день, а заработок – около 30 тысяч в месяц.

Предложение меня очень заинтересовало, так как я сейчас в декрете и дополнительный заработок мне не помешал бы. Но ни на какие уточняющие вопросы звонивший отвечать не стал. Сказал, что теперь нам обязательно нужно устроить собеседование по видеосвязи, на котором я и получу все ответы.

Он тут же спросил, какой у меня смартфон и оперативная система. На что я ответила, что телефон у меня старый и для видеосвязи я пользуюсь только стационарным компьютером. После этого мой собеседник резко утратил ко мне интерес, сказал «вы нам не подходите» и бросил трубку. Связи между операционной системой телефона и написанием текстов маловато, так что уверена, что это был развод. Но в чем именно был подвох? Помогите разобраться.

Совет эксперта по противодействию мошенничеству:

Все верно, это новая схема мошенничества. Сначала мошенники настаивают на том, что общение может продолжаться только по видеосвязи, а затем под разными предлогами просят включить демонстрацию экрана смартфона.

Сами аферисты в это время уже сидят на сайте банка, в котором у человека есть карта, и рассчитывают по номеру его телефона или все той же карты, попасть в личный кабинет. Они планируют сбросить старый пароль и установить новый. Но для этого им нужны коды, которые придут на смартфон человека. И именно для этого они просят включить демонстрацию экрана – чтобы разглядеть уведомление от

банка. Если человек следует инструкциям собеседника, то мошенники получают доступ к его мобильному банку и опустошают банковские счета.

Чтобы схема сработала, у мошенников должно быть довольно много сведений о человеке, которому они звонят. Попробовать сменить пароль и получить доступ к чужому личному кабинету на сайте банка можно, если мошенники уже знают, в частности, номер карты своей жертвы. Эту информацию они могут найти в открытом доступе – например, если вы сами публиковали номер карты для какого-нибудь сбора денег. Либо получить из слитых или украденных баз данных. О том, чем грозят утечки персональных данных и как себя обезопасить, читайте в материалах «Мои персональные данные украли. Что делать?» и «Кто и как охотится за вашими банковскими картами».

Чтобы защитить свои финансы, можно завести отдельный номер телефона и электронную почту только для работы с онлайн-банком и подтверждения финансовых операций и не использовать их ни для каких других целей.

Не устанавливайте по просьбе незнакомцев никакие приложения и не общайтесь с ними через сервисы видеосвязи с опцией демонстрации экрана. Если в результате такой беседы вы потеряете деньги, банк не обязан ничего возмещать, так как вы сами по неосторожности выдали злоумышленникам секретную информацию.

На большинстве телефонов можно отключить отображение содержания уведомлений – что же в них написано, вы узнаете, только когда откроете сообщение.