«Хотите много зарабатывать онлайн? Скачайте программу»

Решила подзаработать в декрете и стала искать в интернете удаленку. Разместила резюме на популярном сайте вакансий. Скоро позвонила девушка и сказала, что ищет операторов колл-центра в свой магазин по продаже косметики. Предложила хорошую зарплату, и работать всего три часа в день. Как раз то, что мне нужно.

Стали обсуждать детали, она попросила скачать на телефон несколько программ для работы — чтобы вести базу клиентов, записывать звонки и еще что-то, уже не помню точно. По телефону сказала названия программ, и я их скачала в официальном плей маркете.

А через некоторое время мой телефон заглючил и почему-то сам стал открывать всякие приложения, как будто кто-то за меня им управлял. От банка пришло сообщение, что кто-то пытается перевести деньги с моей карты. Я запаниковала, выключила телефон.

Хорошо, что муж был дома и смог посидеть с ребенком, а я с паспортом побежала в ближайшее отделение банка. Там мне сказали, что я скорее всего скачала вирус, который украл мой пароль от онлайн-банка, и у меня пытались снять деньги. Но видимо там что-то засбоило у самих мошенников, и они не успели ничего снять.

На всякий случай сотрудница временно заблокировала мои карты и доступ к онлайн-банку. А мне посоветовали почистить телефон, в смысле удалить все эти новые приложения, скачать антивирус, а потом поменять везде пароли. Вот тебе и заработала.

Совет эксперта по противодействию мошенничеству:

Удаленная работа становится все более популярной, и мошенники этим пользуются. Они находят контакты людей на сайтах по поиску вакансий, обзванивают соискателей и предлагают им установить мобильные приложения для организации удаленной работы. На самом деле эти программы открывают киберпреступникам дистанционный доступ к гаджетам пользователей, а это позволяет им добраться и до банковских счетов.

Опасность схемы в том, что даже бдительный человек не сразу распознает мошенничество, ведь у него не требуют никаких конфиденциальных данных или денег. Наоборот, предлагают зарплату, а программы просят скачать из официального магазина приложений.

Почти все эти программы безопасны, а некоторые даже могут быть знакомы претенденту на работу. Это также вызывает доверие.

Но одно из приложений, которые преступники предлагают установить на смартфон, дает им удаленный доступ к гаджету соискателя. Если им удастся выудить данные для входа в онлайн-банк или банковское мобильное приложение, они смогут украсть у человека все деньги или даже оформить кредит от его имени.

Чтобы узнать логины и пароли, а также коды из сообщений от банка, хакеры могут зашить в программу вирус-шпион. Часто преступники присылают ссылку для скачивания этой программы, и по ней пользователь попадает на поддельный сайт, который похож на страницу официального магазина приложений.

Иногда вредоносная программа и правда оказывается размещена в известных каталогах приложений, поскольку там не всегда успевают сразу же проверять все загруженные разработчиками программы.

А в некоторых случаях преступники используют совершенно легальные приложения для удаленного управления компьютерами и смартфонами. Как правило, такие приложения стараются защитить пользователей от несанкционированного доступа. Например, присылают код, который нужно ввести перед началом работы. В таких случаях мошенники под различными предлогами стараются выманить у владельца смартфона этот код.

Важно понимать, что банки не возвращают деньги, если человек сам сообщил преступникам конфиденциальную информацию, ввел ее на мошенническом сайте или загрузил на свое устройство программу, которая открывает доступ к его счетам.

Нина правильно сделала, что выключила смартфон: программа удаленного доступа перестала работать. Хотя вирус и опасное приложение никуда не делись.

Затем стоило бы немедленно позвонить в банк (например, с домашнего номера или телефона мужа), чтобы сообщить

о произошедшем и проконсультироваться со специалистом банка. Ведь каждая минута повышает шансы преступников украсть деньги, если им удалось узнать реквизиты счетов и карт.

Как правило, банк сразу же блокирует карты или исходящие операции по ним, отключает дистанционный доступ к счетам через личный кабинет на сайте и мобильное приложение.

А после этого действительно нужно идти в отделение и писать заявления: о перевыпуске карт и о несогласии с операциями, если мошенники все же успели их провести.

И конечно, нужно удалить все приложения, которые были скачаны по просьбе преступников, проверить телефон на вирусы и обновить защиту.

Логины и пароли стоит поменять не только для онлайн- и мобильного банка, но и в первую очередь для электронной почты. Ведь на нее может приходить важная информация от банка, например отчет об операциях и остатке на счете или ссылки и коды для доступа к личному кабинету.

Обезопасить деньги помогут правила кибергигиены:

Установите антивирусы на всех устройствах, которыми вы пользуетесь. Это поможет вам оградить их от вредоносных программ, которые могут встретиться даже в официальных магазинах приложений. Регулярно обновляйте антивирусную защиту.

Не переходите по сомнительным ссылкам от незнакомцев. И не скачивайте приложения, пока не выясните, что именно они делают, как отзываются о них пользователи.

Прежде чем выполнять просьбы неизвестных компаний, например потенциальных работодателей, проверяйте информацию о них. Найдите в интернете официальный сайт организации, почитайте отзывы, пробейте компанию в СМИ — вдруг она замешана в скандалах. Если организация зарегистрирована буквально пару недель назад и про нее еще нет информации, с ней тоже лучше не связываться. Такие фирмы-однодневки чаще всего создают мошенники.

Никому никогда не передавайте пароли и коды из сообщений от банков, полные реквизиты банковской карты, включая срок действия

и трехзначный код с оборота. И не вводите эти данные на сомнительных сайтах, не привязывайте карту к неизвестным приложениям.