«Введите номер карты, а три цифры с оборота мы подсмотрим сами»

Кристина, Выборг

Моя свекровь Надежда Сергеевна пыталась устроиться на работу и чуть не осталась без денег. Дело было так: она нашла неплохую вакансию на сайте для поиска работы. Фирма по подбору персонала искала менеджера по обработке анкет для крупного банка. Свекровь откликнулась — работа удаленная и деньги для нашего города хорошие.

Получила приглашение на онлайн-собеседование. Там были стандартные вопросы: где работала раньше, умеет ли обращаться с компьютером, какие программы знает и на каком уровне. А потом попросили прямо во время собеседования заполнить небольшую анкету и прислали ссылку на нее. Якобы они сразу онлайн проверят данные по какой-то базе в целях безопасности.

Нужно было сообщить телефон, место жительства, еще что-то и реквизиты банковской карты, на которую будут перечислять зарплату. Никаких подозрений это не вызвало — ведь просили только номер и имя владельца.

Она все заполнила. При этом собеседование не прекращалось — они продолжали общаться по видеосвязи. Ей сказали, что «карта не найдена», может, она ошиблась в цифрах. Свекровь вбила данные еще раз — тот же результат. Ей предложили использовать карту другого банка, если она есть. Новая карта их устроила. После этого ей пообещали перезвонить, и собеседование закончилось.

Буквально через пять минут с первой карты кто-то попытался списать деньги, но операция не прошла — банк посчитал ее подозрительной. Свекровь поняла, что дело нечисто, и сама догадалась заблокировать вторую карту.

В общем, все закончилось относительно хорошо, только карты пришлось выпускать заново. Но удивляет вот что: как мошенникам практически удалось добраться до денег свекрови, хотя они знали только номер карты и имя владельца? Ведь везде пишут, что эти данные можно передавать без опаски. Код с оборота она же не выдавала!

Совет эксперта по противодействию мошенничеству:

Сообщать посторонним номер карты и имя на ней действительно можно без риска — списать деньги лишь по этим реквизитам никому не удастся. А вот раскрывать коды из уведомлений от банка, срок действия карты и три цифры с ее оборота нельзя никому.

Но многие уже знают об этом, и, чтобы не вызывать подозрений, хитрые мошенники запрашивают у людей лишь «безопасные» данные, а секретную информацию выведывают с помощью разных ухищрений.

Вероятно, Надежда Сергеевна во время видеособеседования брала свою карту в руки и засветила обе ее стороны перед камерой, когда заполняла анкету.

Если вы случайно выдали кому-то секретные платежные данные или ввели их на подозрительном сайте, нужно срочно блокировать карту, как и сделала Надежда Сергеевна. Быстрее всего отключить карту можно в приложении банка, в личном кабинете на официальном сайте или по телефону горячей линии. После этого пластик придется перевыпустить.

Когда вы потеряли карту, а потом по счастливому стечению обстоятельств вам ее вернули, не спешите радоваться. Есть риск, что кто-то скопировал ваши реквизиты и попытается их использовать. В этом случае карту тоже лучше заблокировать и перевыпустить.

Если вы наткнулись на фальшивого работодателя на сайте — агрегаторе вакансий, стоит написать в поддержку этого портала и рассказать о мошенниках. Чем больше жалоб на них придет от соискателей, тем быстрее обманщиков удалят с сайта. И тем меньше людей лишатся своих денег.

Как не попасть в ловушку

Даже крупные порталы с вакансиями не всегда успевают быстро распознать фейковые конторы. Так что при поиске работы будьте бдительны:

1.Не верьте предложениям легкого заработка за необременительные или туманные обязанности.
2.Прежде чем идти на виртуальное собеседование в какую-либо организацию, убедитесь, что она действительно существует:

зарегистрирована как юридическое лицо, у нее есть сайт, о ней можно найти отзывы в интернете. Свяжитесь с ее кадровой службой и узнайте, правда ли они ищут сотрудников.

3. На онлайн-встрече не соглашайтесь включать демонстрацию экрана смартфона. Если собеседник будет видеть ваш экран, а во время разговора вы получите оповещение от банка с секретным кодом, есть риск остаться без денег.

4. Не оставляйте никому свои паспортные и платежные данные, пока не убедитесь, что ваш собеседник — действительно тот, за кого себя выдает. Помните, что настоящий работодатель не будет запрашивать банковские реквизиты, пока вы не заключите с ним договор. Трудовое соглашение можно подписать на бумаге от руки или с помощью электронной цифровой подписи, но точно не по видео во время собеседования.

5. Не продолжайте общение с теми, кто просит вас:

- оплатить регистрацию на сайте, который якобы потребуется вам для работы;
- отправить какую-то сумму в качестве гарантии, что вы не пропадете и вовремя выполните первое задание;
- перевести деньги за обучение или какие-то еще услуги.

Столкнулись с подобным? Это точно мошенники!