«Дайте реквизиты карты — будем перечислять вам большую зарплату»

Алла, Нефтеюганск

Моя фирма начала сокращать штат, многих уже уволили, и я решила подыскать запасные варианты на случай, если и мою ставку уберут. Написала знакомым, повесила резюме со своими контактами на самых известных сайтах с вакансиями.

Вскоре мне позвонил рекрутер из фирмы, которая ищет сотрудников для разных организаций. Сказал, что одна крупная компания открывает в нашем городе филиал и набирает туда штат. У них есть вакансия, для которой я как раз подхожу. Должность такая же, а условия даже лучше – зарплата больше, да еще соцпакет.

Рекрутер предупредил, что надо будет пройти несколько собеседований. Сначала подготовительное интервью – с их фирмой – а потом уже с будущим начальником. Ездить никуда не нужно – все по видеосвязи. И еще надо сделать тестовое задание – написать пару деловых писем и небольшой рассказ о том, как я вижу свою дальнейшую карьеру.

На все про все у нас ушла пара недель. Потом рекрутер сказал, что и мое тестовое работодателям понравилось, и сама я произвела приятное впечатление, так что меня берут – офис уже скоро открывается.

А пока нужно оформить договор: для этого я должна прислать данные паспорта, СНИЛС, ИНН, заполнить анкету с личными данными. Поскольку компания солидная, она тщательно проверяет будущих сотрудников, так что меня попросили предоставить информацию и о ближайших родственниках.

Договор я почитала – все как обещали: приличная белая зарплата, отпуск, премии по итогам года, медстраховка. Потом прислали отдельную форму, в ней нужно было заполнить реквизиты карты, на которую будут перечислять зарплату.

И вот здесь начались странности: в тот же вечер стали приходить СМС, как будто с моей карты кто-то старается что-то списать. Но денег, к счастью, на ней почти не было – я как раз оплатила счета за квартиру и поездку в отпуск. Связалась с банком – и мне подтвердили, что были попытки списания с моего счета. Сотрудница порекомендовала заблокировать и перевыпустить карту.

Как только я это сделала, почти сразу же позвонил рекрутер и спросил, нет ли у меня карты другого банка – и назвал крупный госбанк. Сказал, что у компании, которая меня берет, в ней зарплатный проект и им удобнее туда перечислять. Но меня так насторожили эти попытки снять деньги с моей карты, что я ответила: нет, у меня всего одна – зарплатная.

Рекрутер обещал позже со мной связаться, но так и не появился. На мои звонки и письма не отвечал. Тогда я решила позвонить в головной офис компании, которая якобы набирала сотрудников в новое подразделение в нашем городе. Мне сказали, что планов расширения у них нет и, скорее всего, меня кто-то обманул. Я расстроилась, конечно, что с новой работой не вышло. Но и обрадовалась, что мошенникам не удалось меня обокрасть.

Совет эксперта по противодействию мошенничеству:

Обычно мошенники стараются провернуть все быстро – за один телефонный звонок под различными предлогами выманить данные карты, чтобы украсть с нее все деньги. Но на этот раз они решили, что на кону большой куш и надо действовать очень аккуратно, чтобы не вызвать подозрений у потенциальной жертвы.

Они использовали психологические уловки, чтобы поймать человека на крючок. Сначала заинтриговали его привлекательными перспективами, затем имитировали реальный процесс рекрутинга – просили выполнить тестовое задание, проводили несколько интервью. А после этого обрадовали, сообщив, что кандидат принят на престижную работу с огромной зарплатой, и попросили заполнить данные, которые всегда нужны при трудоустройстве.

Реалистичность процесса найма и эйфория от того, что все испытания успешно пройдены, усыпили бдительность соискателя. И, судя по всему, Алла не заметила, что ее просят сообщить не только номер карты и название банка, но и конфиденциальные данные – срок действия карты и три цифры с оборота. Ведь все прикрывалось

легендой, что это необходимо для перечисления зарплаты. Эти секретные данные – ключ к счету, с которого преступники хотели украсть все деньги.

Если бы на счету Аллы были деньги и мошенникам удалось бы их украсть, то банк ничего не компенсировал бы. Ведь она сама передала мошенникам секретную информацию.

Порой аферисты просят «будущего сотрудника» скачать программу для работы, которая на самом деле дает им удаленный доступ к устройству жертвы, в том числе к мобильному или онлайн-банку.

У Аллы мошенники выманили не только реквизиты карты, но и персональные данные – номера паспорта, СНИЛС, ИНН, а также информацию о родственниках. Эти сведения они, скорее всего, попытаются использовать в новых схемах социальной инженерии или перепродадут другим аферистам. Так что теперь ей и ее близким нужно быть еще более бдительными.

Как не попасться на уловки обманщиков?

- Важно следовать правилам безопасности:

- Никому ни в коем случае не сообщайте конфиденциальные данные банковской карты: трехзначный CVC/CVV-код и срок действия – их запрашивают только мошенники. Храните в тайне пароли от мобильного и онлайн-банка, ПИН-коды карты, коды из банковских уведомлений.

- Если с вами на связь вышел представитель известной компании с привлекательным предложением, не спешите выполнять его инструкции и тем более передавать личные сведения и документы. Мошенники довольно часто выдают себя за представителей крупных компаний. Уточните ФИО и должность собеседника и перепроверьте информацию: зайдите на официальный сайт организации, найдите ее контакты и позвоните сами. Спросите, действительно ли у них работает этот сотрудник и правда ли они ищут кандидатов на предложенную вакансию.

Если общение идет по электронной почте, то для начала сверьте доменный адрес отправителя (после символа @) с официальным сайтом компании. Если они не совпадают, просто удалите письмо.

- Когда получаете предложение от кадрового агентства-посредника или от неизвестного работодателя, найдите организацию в базе налоговой и проверьте, когда она создана и какой у нее вид деятельности. Возможно, окажется, что это фирма-однодневка. Пробейте компанию в СМИ – вдруг она замешана в скандалах, почитайте отзывы о ней в интернете.

- Не переходите по ссылкам от незнакомцев и не скачивайте программы по их требованию.

- По возможности не публикуйте свои персональные данные в открытом доступе, в том числе на сайтах объявлений и в социальных сетях – мошенники используют эту информацию, чтобы выйти с вами на связь и применить свои схемы обмана.

- Установите антивирусы на все устройства, которыми пользуетесь, и регулярно их обновляйте.