

кадр из фильма «Иван Васильевич меняет профессию» / 1973

Золотые обещания: мошенники наловчились красть данные банковских карт во время собеседования

Александр Кудрявцев

27 января 21:40 Общество

Из-за кризиса, вызванного пандемией, и недобросовестного отношения работодателей некоторые люди остались без дохода или понесли ощутимые убытки. На 20 января в стране зарегистрировано 2,6 миллиона безработных. Неудивительно, что количество резюме на сайтах по размещению вакансий неуклонно растет. Этим быстро научились пользоваться мошенники. Корреспондент «Вечерней Москвы» выяснил, как работает новый способ наживы на пострадавших от пандемии.

Павел Скрябин (имя и фамилия изменены по просьбе героя. — «*ВМ*») разместил в интернете объявление о поиске работы в удаленном формате и свое резюме. Дистанционный формат был очень важен для соискателя. Через несколько дней мужчине позвонили из крупной компании. Потенциальный работодатель обещал хорошие условия, удобный график и высокую заработную плату. Он уговорил Павла установить на свой

смартфон приложение. Программа была в официальном цифровом магазине, поэтому соискатель и не стал сомневаться.

На следующий день мужчина обнаружил, что с его счета исчезла крупная сумма денег. Его адвокат обратился в консалтинговую компанию в сфере IT-безопасности, чтобы разобраться в случившемся.

— Приложение, которое установил потерпевший, помогло мошенникам получить доступ к его банковскому аккаунту. Программа, похоже, была связана с сервисом приема и отправки СМС-сообщений с телефона. Вероятно, мошенник просто сбросил пароль от личного кабинета клиента, перехватил секретный код доступа и таким образом завладел электронным счетом и вывел с него средства, — рассказал директор технического департамента крупной консалтинговой компании в сфере IT-безопасности Федор Музалевский.



Фото: pixabay.com

Он добавил, что такая схема мошенничества еще не получила широкого распространения, но уже есть первые пострадавшие от рук злоумышленников. Новизна подхода заключается в том, что злоумышленники совмещают вредоносное программное обеспечение с навыками социальной инженерии (психологическое манипулирование людьми. — «*ВМ*»).

— Они подгоняют вас. Торопливость — отличительная черта злоумышленников. Ни один работодатель не будет просить вас ставить приложение прямо сейчас, пока идет телефонный звонок. Это классический ход. Злоумышленники надеются, что вы поторопитесь и не заметите подвоха, — добавил Федор Музалевский.

Ситуация с коронавирусной инфекцией в мире привела к серьезным изменениям в привычках людей, считает заслуженный юрист России Иван Соловьев. Еще недавно редкий удаленный режим работы теперь многим знаком и удобен. Люди стали чаще покупать товары онлайн. Электронным переводом денег жители пользуются охотнее, чем наличными. Это в свою очередь привело к росту количества дистанционных мошенничеств более чем на 70 процентов.

— Бесконтактный обман несет в себе меньше рисков быть задержанным с поличным в момент совершения преступления. Кроме того, в сети легче скрыть следы совершенных противоправных деяний. Поэтому преступники сегодня используют весь диапазон возможностей, предоставляемых всемирной сетью, — сообщил Иван Соловьев

Знание — сила

Защититься от мошенников помогут бдительность и информированность. Руководитель пресс-службы крупного сайта по поиску работы Александр Джабаров рассказал, что обычно представители компаний не предлагают что-либо скачать или установить во время собеседования. Подобные просьбы как раз характерны для мошенников. Если вы оказались в похожей ситуации, для начала точно узнайте, кто вам звонит. Попросите собеседника представиться полностью, узнайте должность и наименование компании. Затем можно попросить связаться с вами позднее, сославшись на занятость. А в это время проверьте потенциального работодателя. Подробности о фирме можно узнать в интернете. Достаточно найти адрес и телефон. После позвоните в компанию и уточните, ведет ли она еще свою деятельность.

— Чтобы обезопасить себя, соискатель может вести коммуникацию не напрямую, а через мессенджер на сайте по поиску работы. Тогда он будет точно знать, что ведет разговор действительно с работодателем, который нашел его резюме на электронной площадке, — добавил Александр Джабаров.

По его словам, на сайтах по поиску работы можно проверить фирму. Администрация ресурса в ручном и полуавтоматическом режиме обновляет данные о компаниях. Проверенные организации будут иметь соответствующую отметку. Какого-то общего для всей России реестра благонадежных работодателей в свободном доступе нет, хотя в интернете представлено множество сервисов по поиску информации о различных фирмах. Там в отзывах можно найти предупреждение, если представители компании ведут себя недобросовестно.

Еще обезопасить себя от уловок мошенников можно на эмоциональном уровне. Психолог Леонид Китаев-Смык утверждает, что злоумышленники зачастую стараются взволновать жертву. Сообщают о трагической новости или, наоборот, сказочном выигрыше. В обоих случаях они надеются, что человеком в принятии решений будут руководить эмоции.

— Люди сейчас все время находятся в стрессовом состоянии. Кто-то потерял работу из-за пандемии коронавируса. Растут цены, родственники лежат в больницах. Неизвестно, когда это закончится. Еще волнение добавляют тревожные сообщения по телевизору и в интер- нете. В такое время люди неосознанно надеются на помощь и легче доверяются другим. Этим и пользуются мошенники, — рассказал психолог Леонид Китаев-Смык.

Минимизировать риски

Если вас обманули мошенники, нужно сразу заблокировать свои банковские счета, советует адвокат Алексей Гавришев. Преступники, получив доступ к одной платежной

карте, смогут добраться и до других. После нужно обратиться в полицию. Сейчас это проще сделать благодаря онлайн-сервисам.

— На сайте Министерства внутренних дел России есть определенная форма. Ее легче заполнить, чем ехать в отделение и писать заявление. Это обращение тоже официальное. Оно может стать поводом для начала расследования, — подчеркнул Алексей Гавришев.

Он добавил, что к обращению нужно приложить скриншоты (снимки экрана телефона. — «*ВМ*») с перепиской и уведомлениями от приложения. Еще следствию может помочь запись телефонного разговора с мошенниками. Полицейским может понадобиться и ваш смартфон. Эксперты проанализируют вредоносное приложение. Они просмотрят его логи (архивные записи о всех действиях программы. — «*ВМ*»). Информация поможет им поймать мошенников. Еще Алексей Гавришев посоветовал обратиться в полицию, даже если преступникам не удалось вас обмануть.

— Эта информация может быть полезна полицейским. Сообщения о попытках мошенничества помогают выстроить алгоритм поиска и поимки преступников, — добавил заслуженный юрист России Иван Соловьев.



Фото: pixabay.com

Богатая фантазия

Понятно, что на одной схеме выдумки «разводил» не заканчиваются. Недавно появилась информация о еще одном новом методе обмана. Подробности схемы рассказали эксперты крупной компании, занимающейся вопросами кибербезопасности. Мошенники наживаются на экономных интернет-пользователях. Злоумышленники размещают на онлайн-площадках объявления о продаже различных товаров по заниженной цене. Когда

находится покупатель, аферисты отправляют ему ссылку на собственный сайт. Только страница эта выглядит так, будто она принадлежит популярной службе доставки. Ничего не подозревающий покупатель вводит данные своей кредитной карты и переводит деньги. В результате мошенники получают и средства жертвы, и доступ к банковскому счету.

Эта схема набирает популярность в Европе и Соединенных Штатах Америки. В декабре прошлого года эксперты обнаружили уже порядка 3000 поддельных сайтов. Еще преступники используют новые технологии на основе искусственного интеллекта. Есть программа, которая позволяет подделать голос любого человека.

— Это нейросеть. Искусственный интеллект анализирует несколько записей разговора человека. После программа может говорить его голосом. Аферисты могут подделать речь вашего родственника, друга или начальника, — рассказал ведущий эксперт крупной консалтинговой компании в сфере IT-безопасности Сергей Волокитин.

Он добавил, что вышеназванные программы редко используются при обмане обычных жителей. Притворяться родственниками невыгодно для мошенников, потому что люди стали гораздо реже верить такому обману. Такие технологии представляют опасность для руководителей корпораций. Однако крупные компании уже ищут способы защиты. Российские и зарубежные научные центры из сферы кибербезопасности уже ведут разработки систем, которые смогут распознать поддельный голос. После эти технологии будут защищать крупные компании и банки. Последние заботятся не только о собственном капитале, но и о средствах клиентов.

— Эта функция доступна всем клиентам банков. Вы заранее ограничиваете максимальную сумму переводов или снятия наличных в месяц.

Так мошенники не смогут присвоить все ваши деньги, даже если получат доступ к счету. Ведь чтобы снять ограничение, нужно обратиться в банк и назвать секретное слово, — добавил Сергей Волокитин.

Еще клиенты крупных банков могут усилить защиту своего личного кабинета, настроить авторизацию по отпечатку пальца. Кроме того, компании внедряют новые технологии для защиты клиентов. Например, есть система на базе искусственного интеллекта, которая постоянно анализирует денежные операции пользователей. Программа фиксирует все переводы и списания средств. Она может заблокировать операцию, которая вызывает подозрения. Особое внимание банки уделяют клиентам из групп риска. Например, при установке мобильного приложения на смартфон пожилого человека программа не активируется сразу.

ПРИЗНАКИ ОБМАНА

— Собеседник постоянно торопит вас и мотивирует действовать прямо сейчас, не откладывая.

— Вам предлагают установить приложение на смартфон прямо во время разговора или перейти по ссылке на подозрительный сайт.

— Звонящий отказывается сообщить свои имя, фамилию, должность и рабочий номер телефона.

— Вас просят совершить со счетом какие-либо операции, например перевести средства, ввести код или отправить СМС-сообщение.

— Вам звонят с номера телефона, который не определяется.

— Вас просят оплатить какие-либо расходы или комиссии за перевод выигрыша или для получения приза.

— Сообщение якобы от банка приходит вам в новый чат, где не отображаются ранее присланные уведомления об операциях.

— Собеседник просит вас назвать свои персональные данные, например номер паспорта.

— В тексте сообщения допущены грубые грамматические ошибки, а некоторые русские буквы заменены на похожие из латинского алфавита.

ЦИТАТА

Юрий Титов, руководитель пресс-службы департамента региональной безопасности и противодействия коррупции Москвы:

— Чтобы не стать жертвой злоумышленников, настоятельно рекомендуем никогда не устанавливать на свой телефон непроверенные приложения. Не сообщать свои персональные данные в разговоре. При малейшем сомнении в намерениях собеседника прерывайте разговор. Не дайте себя обмануть. В случае, если вы стали свидетелем или жертвой мошенничества, незамедлительно обращайтесь в полицию. Свое временно принятые меры помогают найти злоумышленников и привлечь их к ответственности.

КОММЕНТАРИИ ЭКСПЕРТОВ

Никита Масленников, экономист:

— Мошенники нацелились на безработных, которых стало больше из-за ситуации с коронавирусом в мире. Большую роль сыграло уменьшение работы в сером секторе бизнеса. Люди, которые были трудоустроены неофициально, потеряли свои места и теперь готовы ухватиться за любую возможность. Конечно, мошенников привлекает сложившаяся ситуация. Многие ищут дополнительный доход, даже имея основное место работы.

Виталий Терентьев, эксперт по кибербезопасности крупного портала по поиску работы:

— Во время телефонного разговора с рекрутером вас должны насторожить просьбы что-то скачать, установить или сообщить свои персональные данные, например серию и номер паспорта. Такую информацию ни в коем случае нельзя предоставлять на первых этапах собеседования. И все рекрутеры компаний об этом знают. Ваши персональные данные понадобятся только на последнем этапе переговоров, для проверки со стороны службы безопасности или уже непосредственно перед трудоустройством. На очной встрече вам предложат подписать согласие на обработку персональных данных. Только после этого можно их разглашать.

Виктор Карасев, руководитель курсов компьютерной грамотности Литературного института имени Алексея Горького:

— Есть косвенные признаки, по которым можно определить, что приложение выполняет какие-то другие функции, кроме официально заявленных. Например, следует насторожиться, если программа запрашивает доступ к СМС-сообщениям. Злоумышленникам это нужно, чтобы перехватывать коды доступа, которые приходят

пользователю при входе в банковский аккаунт. Вообще с разрешениями надо быть внимательнее. Если приложение для заметок почему-то пытается подключиться к камере, то стоит насторожиться.