Соколова А.Н., старший преподаватель кафедры «Экономическая безопасность, учет и право» ФГБОУ ВО ДГТУ», Ростов-на-Дону, Россия**;**
Шумилина В.Е., к.э.н., доцент, кафедры «Экономическая безопасность, учет и право», Донской государственный технический университет, Ростов-на-Дону, Россия
Тупакова К.Д., студент 3 курса кафедры «Экономическая безопасность, учет и права» ДГТУ, Ростов – на – Дону, Россия;

МОБИЛЬНЫЕ МОШЕННИЧЕСТВА КАК УГРОЗА ЭКОНОМИЧЕСКОЙ ЖИЗНИ СТРАНЫ

Аннотация. Данная статья рассматривает наиболее популярные схемы совершения мошеннических операций, которые напрямую угрожают безопасности экономической жизни целого государства. Демонстрируются способы того, с помощью каких инструментов и манипуляций мошенники добиваются своей корыстной преступной цели. Рассматриваются действия, которые необходимы для защиты от мошенников и минимизации рисков попасться на их мошеннические схемы.

Ключевые слова: мобильное мошенничество, телефон, средства сотовой связи, мошеннические схемы, корыстные побуждения, жертва, абонент.

Sokolova A. N., Senior lecturer of the Department «Economic Security, accounting and law», FGBOU DSTU , Rostov-on-don, Russia;
Shumilina V. E., associate Professor of «Economic safety, accounting and Law» of the «Donskoy state technical University», Rostov-on-Don, Russia;
Tupakova K.D.,student of the Department of «Economic Security, Accounting and Law» DGTU, Rostov-on-Don, Russia;

MOBILE FRAUD AS A THREAT TO THE COUNTRY'S ECONOMIC LIFE

Annotation. This article examines the most popular fraud schemes that directly threaten the economic security of an entire nation. It demonstrates ways in which the tools and manipulation are used by fraudsters to achieve their selfish criminal purpose. The actions that are necessary to protect against fraudsters and minimise the risks of falling for their schemes are discussed.

Keywords: mobile fraud, telephone, cellular means, fraudulent schemes, self-interest, victim, subscriber.

В наше время преступность, которая совершается из корыстных побуждений, достигла недостижимого апогея за все времена существования человечества. Её доля превышает 90% от общего количества зарегистрированных преступлений в странах с развитой экономикой и более 60% в развивающихся странах. В нашей стране каждое 3-е преступление, которое преследуется Уголовным кодексом РФ, характеризуется корыстными помыслами. Наиболее распространенными преступлениями из числа корыстных являются преступления против собственности, совершаемые посредством различных форм хищений чужого имущества. Их главная особенность в том, что они не только опасны для общества, но и вносят дезорганизацию в экономическую жизнь страны, создают возможности для паразитического обогащения одних за счет других, чем создают угрозу существования целого государства.

Одним из самых популярных видов хищения чужого имущества является мошенничество. Оно, как биологический вирус, распространился во все сферы деятельности каждого человека. На это влияет стремительное и интенсивное развитие компьютерных технологий и телекоммуникации. Данные факторы являются главной чертой современного технологически развитого общества. Мобильная система связи, которая возникла в 80-ых годах прошлого века, стремительно зарекомендовала себя и распространилась по всему земному шару. По статистическим данным на 2017 год, около 6 млрд человек пользуются мобильной связью, но фактическое число их – около 4,1 млрд человек, т.к. один пользователь может являться абонентом сразу нескольких операторов.

На заре своего появления телефон стал способом преступного обогащения в среде мошенников и разного рода криминала, а сотовый (или мобильный) - в особенности. Вместе со свободным оборотом на рынке сотовых телефонов появились разнообразные схемы мошенничества, которые напрямую стали

связаны с ними. Злоумышленник всегда старается найти способом обогатиться за счет высокодоходного бизнеса и его клиентов. Мошенничество в сфере телефонной связи отличается по способам и степени изощренности, по степени общественной опасности их деяний. С развитием компьютерных технологий, развитием научно-технического прогресса арсенал возможностей и способов у мошенников неустанно пополняется и модернизируется.

Согласно международной статистике ежегодные совокупные потериоператоров связи и абонентов от телефонного мошенничества составляют примерно $10-40 млрд. Собрать точную цифру убытка довольно проблематично, т.к. каждый оператор не захочет называть конкретную сумму убытка из-за мошенников. Это может навредить репутации такой кампании, подорвать ее авторитет, как стабильного и надежного оператора сотовой связи. И зачастую, люди, которых обманули на сумму 500-1000 рублей, не обращаются в правоохранительные органы для попытки вернуть свои украденные средства. По данным МВД России, каждый пятый из ста обладателей сотовых телефонов становился жертвой телефонного мошенничества.

Конкретно на территории нашей страны мобильное мошенничество стало процветать не так давно, примерно с 2008 года. В качестве основного инструмента для мошенников является мобильный телефон. Популярность данного криминального феномена объясняется следующим: широкая распространенность и относительная доступность для большинства населения услуг сотовой связи и средств общения внутри нее. Жертвой может оказаться любой человек:

- бизнесмен;
- чиновник;
- служащий банка;
- продавец и все остальные.

Для того, чтобы вступить в контакт с жертвой, телефонные мошенники используют два способа:

- телефонный звонок – такой способ позволяет напрямую манипулировать и управлять человеком, но имеет один изъян: стоит задать один правильный вопрос (каждый вопрос разнится в зависимости от конкретного случая) и мошенника можно будет рассекретить;

- СМС-сообщения – способ общения с жертвой вслепую. Такие сообщения может получить большинство из нас в надежде, что адресат будет доверчивым получателем. Примером данных сообщений много, например: «вы являетесь победителем, пришлите смс с кодом на этот номер, и заберите свой приз», «наша кампания ООО «М» проводит СМС опрос, для участия в нем вы можете, отправив ответное сообщение на этот номер».

Главная задача телефонного мошенника – застать свою жертву врасплох и заставить ее, добровольно, передать свои денежные средства. Согласно статистики данных МВД России популярными в наше время являются следующие схемы:

-шантаж, угроза близкими. Мошенник звонит своей потенциальной жертве и представляет работником правоохранительных органов. Преступник сообщает человеку, что его близкий, друг, знакомый – кто угодно, попал в страшное происшествие (ДТП со смертельным исходом, убийство по неосторожности, распространение наркотических веществ, хранение наркотических веществ и т.д.) и сообщает, что жертва может помочь закрыть дело за взятку в особо крупном размере. Деньги необходимо найти срочно, иначе потом будет поздно. Главной особенностью данного способа мошенничества являются 2 момента: неожиданность информации для человека и количество времени, которое предоставляет мошенник жертве. Эти 2 психологических способа в совокупности полностью дезориентируют человека и заставляют идти на поводу у преступника. Общественная опасность подобных преступлений заключается в том, что, помимо

причинения материального ущерба потерпевшим, дискредитируются правоохранительные органы, в частности полиция;

- СМС-сообщения на телефон. Мошенник пишет на телефон жертве от имени друга, родственника, члена семьи просьбу о том, что ему срочно нужны деньги. Все обстоятельства он обязуется объяснить позже.

- телефонный номер (ссылка): платный номер или интернет-ссылка. Один переход или звонок способен снять большую сумму денег, например: жертве приходит СМС-сообщение с просьбой найти редкую группу крови для ребенка. В самом сообщении просят перезвонить по определенному номеру или прислать ответное СМС-сообщение. В данном случае звонки автоматически снимают денежные средства со счета звонящего, а отправка СМС имеет повышенную стоимость. Или другой случай: абонент получает от мошенников SMS-сообщение. В нем сообщается о том, что ему прислали поздравления, которые оставили на сайте. На него оставляется ссылка, чтобы наша потенциальная жертва смогла открыть ее и перейти по ней. После перехода по ссылке на мобильном телефоне нашего абонента автоматически оформляются платные подписки на разные сервисы. Одним из возможных вариантов развития такого события может быть вирус, который цепляет мобильный телефон жертвы.В результате этого, в будущем, происходит ежедневное списание средств с его телефонного счета;

- код от «оператора связи». Данный способом мошенничества завязан на том, что вам в СМС-сообщения приходит предложение подключить выгодную услугу. Для этого необходимо всего лишь ввести код, который на самом деле спишет средства со счёта. На мобильный телефон жертвы приходит звонок от«сотрудника службы технической поддержки оператора сотовой связи» (мошенник) с предложением подключить совершенно новую и эксклюзивную услугу, которая в разыулучшить качество связи абонента. Для этого на номер жертвы высылается сообщение с кодом, которое просят продиктовать. Данная махинация позволит преступнику перевести все денежные средства своей жертвы себе на счета;

- штрафные санкции и угроза отключения номера. В данном случае здесь все прозрачно и выявить мошенничество можно, немного разбираясь в специфике работы мобильных операторов связи. Потенциальной жертве звонит мошенник, представляясь сотрудником технической службы определенного оператора. Он уведомляет абонента о том, что тот не внес своевременно уплату за свой тариф. В следствие этого потенциальной жертве необходимо возместить убыток оператору связи, заплатив штраф в определенном размере, купив карты экспресс-оплаты и сообщив их коды. Случаи мошенничества данного вида могут быть разные: поменял тарифный план, не оповестив при этом оператора связи, воспользовался услугами роуминга без предупреждения и т.д.

- «слежка» за людьми. В виду большой любопытности людей за чужой жизнью, мошенники разработали новую схему мошенничества. Они предлагаю потенциальной услуге жертву, которая позволит получить полный доступ к СМС-сообщениям и звонкам другого человека. Для этого необходимо отправить сообщение стоимостью от 10 до 30 руб. на указанный короткий номер и вписать в предлагаемую форму номер телефона абонента. После того, как пользователь отправляет SMS, с его счета списывается сумма гораздо большая той, что была указана мошенниками, - до 500 руб., а интересующая информация так и не поступает;

- СМС-сообщение о блокировке банковской карты. В СМС-сообщения потенциальной жертве приходит уведомление о том, что их банковская карта заблокирована. Для ознакомления со всеми подробностями ей предлагается позвонить, по указанному в сообщении, номеру. Наша потенциальная жертва звонит, и в ответ получает информацию мошенника о том, что на сервере их банка произошел сбой, поэтому они просят предоставить PIN-код карты и ее цифры, которые находятся на лицевой стороне. После получения данной информации мошенники спокойным образом выводят все денежные средства со счета этой карты.

Мы рассмотрели самые распространенные способы мошенничества, но это не значит, что на этом их список закончился. Люди, которые преследуют цель – хищение чужого имущества – изобретательны и предприимчивы. Существуют еще множество способов того, как мошенники вымогали личные финансовые средства доверчивых граждан, их просто невозможно перечислить все. Но раз существует способ обмана людей, значит есть способы, которые помогут предотвратить случай наступления мобильного мошенничества. Из перечисленных выше примеров, можно сформировать основные моменты, на которые давят мошенники:

- Ощущение надвигающейся опасности в сочетании с тем, что у человека нет времени на бездействие. Это психологический метод воздействия на жертву, когда ее активно подталкивают к активным действиям, которые выгодны телефонному мошеннику. В таком случае всегда стоит не поддаваться на провокации такого человека, необходимо остановиться и задуматься. Любой официальный представитель крупной организации, кампании всегда сможет ответить на ваши вопросы и не будет торопить с преждевременными действиями;
- Эмпатия. Мошенники зачастую просят помочь им в ходе телефонного разговора. Если вы чувствуете вину за то, что сомневаетесь в реальной причине обращения к вам, это должно стать первым звонком. Мошенники могут притвориться сотрудниками благотворительной организации или придумать другую историю. Для того, чтобы убедить жертву, ониначинают упоминать недавнюю природную катастрофу или другую актуальную проблему;
- Обещания. Обычно это касается выигрышей в лотерее, автомобилей в каком-то конкурсе или путевке на море, полученные через радиостанцию, о которой жертва никогда и нигде не слышала. Перспектива получить награду может подтолкнуть вас к выполнению просьбы мошенника. В таком случае необходимо быть предельно внимательным к тому, что вам обещают.

Теперь необходимо рассмотреть способы защиты от мобильного мошенничества, которые помогут минимизировать шансы быть обманутыми:

- Сложные пароли. Необходимо использовать для защиты своих личных данных пароли, которые буду представлять из себяслучайный набор символов, но не только буквы, но и различные цифры, специальные символы;
- Длинный PIN-код. Необходимо использовать разнообразный, не однотипный набор цифр, который должен состоять из большого набора таких символов. Например, вместо четырехзначного ПИН-кода установите на экран блокировки ПИН-код из шести знаков. Не используйте в качестве своего личного пароля важные знаменательные даты, т.к. эти данные можно узнать о вас из интернета, к чему часто прибегают мошенники.
- Установитеприложение, блокирующее звонки. Такие приложения защищают ваш телефон от звонков, нелегально выполняемых роботами, и прочих типов телефонного мошенничества. Они предоставляют вам возможность лично проверять входящие номера в случае, если позвонят действительно люди, от которых ожидается звонок.
- Не вступайте в разговор и положите трубку. Участие в разговоре в любом виде может спровоцировать еще больше звонков. Не нажимайте на кнопки для навигации по автоматизированному меню и не отвечайте живым операторам, если заподозрили неладное.

Таким образом, можно сделать вывод, что сфера мобильного мошенничества многогранна и очень разнообразна. В данной статье мы рассмотрели далеко не все способы мошеннических схем злоумышленников, поэтому всем людям необходимо самостоятельно обновлять свои знания на тему такого рода преступлений. В наше время необходимо всегда быть бдительными, поскольку такого рода мошенники подрывают финансовое благосостояние не только конкретного гражданина, но и всего государства. От их деятельности страдают не только люди, но и крупные частные или государственные кампании.

Литература

1. Лазарева И.В. Расследование преступлений, связанных с несанкционированным доступом к сети сотовой радиотелефонной связи: автореф. дис. ... канд. юрид. наук. Хабаровск, 2017.
2. Ударцев С.Ю. Раскрытие хищений средств сотовой связи подразделениями уголовного розыска. Хабаровск, 2018.
3. Расследование и раскрытие преступлений, совершенных посредством смс-сообщений: метод. рекомендации / Н.А. Жукова и др. М., 2019.
4. Ударцев С.Ю., Давыдов С. И. Способы хищений средств сотовой связи, совершаемых путем мошенничества // Проблемы теории и практики оперативно-розыскной деятельности криминальной милиции: межвуз. сб. науч. тр. Барнаул, 2018.
5. Шумилина, В. Е. Экономическое мошенничество как угроза обеспечения экономической безопасности хозяйствующих субъектов / В. Е. Шумилина, А. М. Бокова // Управление безопасностью бизнеса в современных условиях. – Москва : AUSPUBLISHERS, 2021. – С. 92-101.
6. Шумилина, В. Е. Экономическая безопасность предприятий малого и среднего бизнеса / В. Е. Шумилина, А. А. Борзых // Управление безопасностью бизнеса в современных условиях. – Москва : AUSPUBLISHERS, 2021. – С. 74-83.
7. Шумилина, В. Е. Обеспечение экономической безопасности хозяйствующего субъекта / В. Е. Шумилина, Ю. Г. Стороженко // Управление безопасностью бизнеса в современных условиях. – Москва : AUSPUBLISHERS, 2021. – С. 56-64.
8. Шумилин, П. Е. Влияние корпоративного мошенничества на бизнес и экономическую безопасность страны в целом / П. Е. Шумилин, П. С. Нежижимова // : Современные проблемы экономической безопасности, учета и права в Российской Федерации. Том 2, 11 января

2018 года – 31 2019 года, 2019. – С. 5. – DOI 10.26526/conferencearticle_5c50608a3442c1.05921536.

References

1. Lazareva I.V. Investigation of crimes related to unauthorized access to the network of cellular radiotelephone communications: Ph.D. dis. ... cand. legal Sciences. Khabarovsk, 2017.
2. Udartsev S.Yu. Disclosure of theft of cellular communications by criminal investigation units. Khabarovsk, 2018.
3. Investigation and disclosure of crimes committed through SMS messages: method. recommendations / N.A. Zhukova et al. M., 2019.
4. Udartsev S.Yu., Davydov S.I. Methods of theft of cellular communication means committed by fraud // Problems of the theory and practice of the operational-search activity of the criminal police: interuniversity. Sat. scientific tr. Barnaul, 2018.
5. Shumilina, V. E. Economic fraud as a threat to ensuring the economic security of business entities / V. E. Shumilina, A. M. Bokova // Management of business security in modern conditions. - Moscow: AUSPUBLISHERS, 2021. - P. 92-101.
6. Shumilina, V. E. Economic security of small and medium-sized businesses / V. E. Shumilina, A. A. Borzykh // Management of business security in modern conditions. - Moscow: AUSPUBLISHERS, 2021. - S. 74-83.
7. Shumilina, V. E. Ensuring the economic security of an economic entity / V. E. Shumilina, Yu. G. Storozhenko // Management of business security in modern conditions. - Moscow: AUSPUBLISHERS, 2021. - P. 56-64.
8. Shumilin, P. E. Influence of corporate fraud on business and economic security of the country as a whole / P. E. Shumilin, P. S. Nezhizhimova // Modern problems of economic security, accounting and law in the Russian

Federation. Volume 2, January 11, 2018 - January 31, 2019, 2019. - P. 5. - DOI 10.26526/conferencearticle_5c50608a3442c1.05921536.