УДК 316.774

ПРИВЫЧКИ СОВРЕМЕННОГО МОЛОДОГО ПОЛЬЗОВАТЕЛЯ СЕРВИСА ОНЛАЙН-ПЛАТЕЖЕЙ

© **Юдалевич Н. В., 2022**
Иркутский государственный университет, г. Иркутск

В данной статье анализируется текущая ситуация с онлайн-платежами, рассматриваются привычки людей, предпочитающих онлайн-платежи, выявляются угрозы в виде попадания на сайты мошенников и вырабатываются рекомендации по избеганию потери средств при попадании на сайты мошенников.

Ключевые слова: онлайн-платежи, онлайн-покупки, мошенники, смс-уведомления, push-уведомления, сайты мошенников

В настоящее время, когда цифровизация экономики уже стала не только реальностью, но и обыденностью, как никогда важно обращать внимание на те угрозы, которые помимо всех очевидных плюсов и удобств, она в себе несёт.

Все мы уже привыкли к онлайн-платежам и всё реже можно встретить человека, расплачивающегося наличкой. Наличка стала редкостью. И если раньше основной угрозой для нашего кошелька было то, что его могут физически у нас украсть либо отнять силой, то сейчас акценты сместились на обеспечение безопасности наших виртуальных денег.

Многие считают, что хранение в надежном месте пластиковой карты или мобильного телефона полностью оградит от попыток мошенников лишь нас средств. Разумеется, использование всевозможных паролей и пин-кодов в какой-то степени ограждает наш кошелёк от кражи средств, но, как показывает практика, зачастую этого бывает недостаточно.

И в данной статье мы рассмотрим привычки современного пользователя онлайн-платежей и попробуем проанализировать причины проблем, возникающих при онлайн-платежах.

Итак, нами был проведён опрос среди российских пользователей, среди которых оказалось 62 % женщин и 38 % мужчин. Основной возраст опрашиваемых составил 18–25 лет — 76,6 %, 8 % — люди в возрасте до 18 лет, остальные возрастные группы (старше 25 лет) в нашем опросе составили в сумме 15 %.

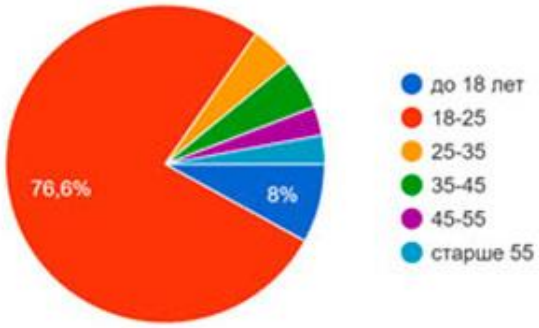

Рис. 1. Возрастное распределение участников опроса

То есть, мы можем говорить о том, что в нашем опросе участвовала молодежь, которая наиболее часто прибегает к безналичному расчёту и предпочитает его наличному. Так на вопрос как часто опрашиваемые используют наличные средства для совершения платежей 41,6 % ответили, что только там, где не принимают безнал, 35 % указали, что используют наличку очень редко, 20,4 % — 50 на 50, в половине случаев используют наличку, в половине — безнал. И лишь 2,9 % всегда пользуются только наличкой. Данные показывают, что подавляющее большинство участников опроса предпочитают безналичный расчет.

Рис. 2. Структура использования налички и безнала

При совершении безналичных платежей плательщик либо пользуется терминалом в магазине, либо совершает платежи в Интернет. Первый способ представляется более защищенным и, следовательно, безопасным, поскольку при получении оборудования (терминалов) владелец

магазина (или любой торговой точки) проходит процесс идентификации и подписи пакета документов, разрешающих им соответствующую деятельность.

Напротив, когда мы совершаем платежи в Интернет, следует обращать внимание на то, на каком сайте совершается покупка, на сколько сайт надежен и заслуживает доверия. Мы разделили сайты на три типа — официальные сайты компаний, проверенные известные маркет-плейсы, приложения для телефона (также для первых двух типов) и любые другие сайты.

Выяснилось, что на сайтах компаний покупают 56,9 % опрошенных, на проверенных маркет-плейсах 49,6 %, пользуются приложениями для покупок на телефоне 61,3 % и лишь 8 % используют непроверенные сайты.

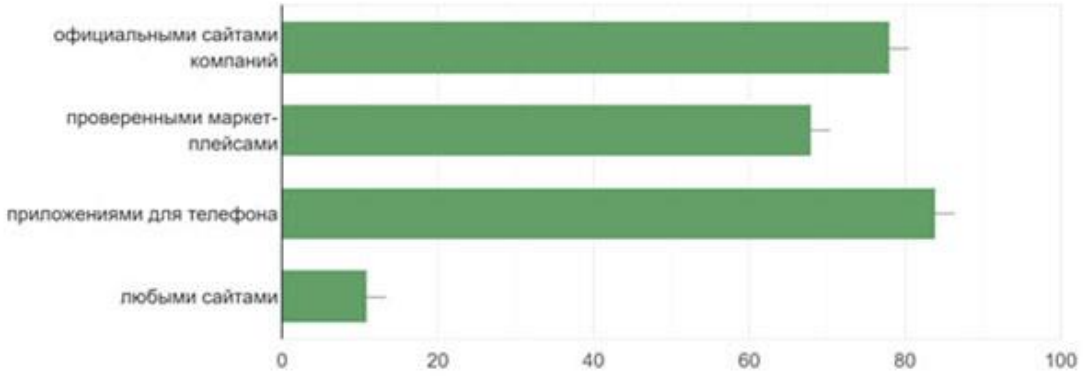

Рис. 3. Использование различных источников для совершения платежей онлайн

По идее, это должно говорить о том, что основная масса участников опроса полностью защищена от мошенничества при совершении онлайн-платежа. Тем не менее, 24,8 % опрошенных показывают, что становились жертвой мошенников, когда при совершении платежа с них сняли деньги, но не оказали услугу или не прислали товар.

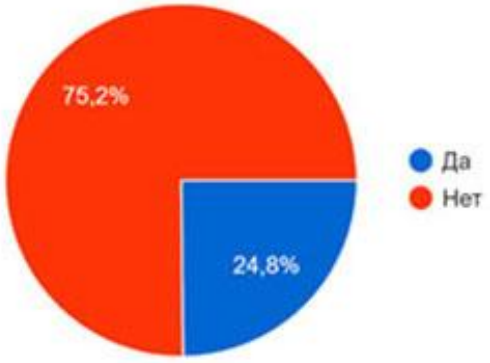

Рис. 4. Доля опрошенных — тех, кто сталкивался с сайтами мошенников

Почему так много пользователей становятся жертвами сайтов мошенников, учитывая тот факт, что наши участники опроса — молодежь, то есть люди, использующие Интернет и онлайн-платежи постоянно и в достаточно большом объёме.

Безусловно, при совершении платежа на непроверенном сайте следует соблюдать некоторые меры безопасности, в частности, проверять, от кого пришел счёт на оплату (смс или push-уведомление), а также, какая сумма будет снята со счёта плательщика.

По результатам опроса 75,2 % утверждают, что всегда внимательно смотрят какая сумма, и от чьего имени будет снята с их счёта, 24,1 % смотрят иногда и 0,7 % никогда не смотрят. Это говорит о том, что четверть опрошенных подвергаются риску снятия у них любой суммы каждый раз, когда не смотрят, кто и какую сумму снимает с их счёта.

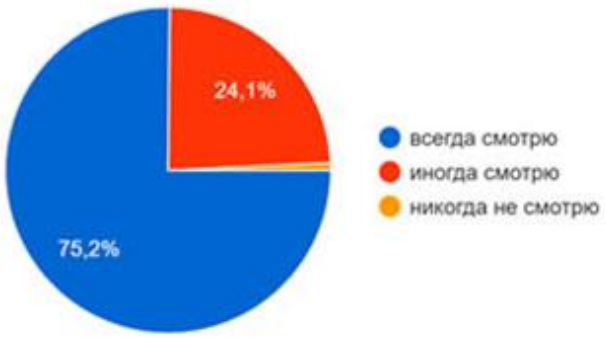

Рис. 4. Показатели осмотрительности опрошенных в отношении того, какая сумма и от имени кого снимается со счёта плательщика при совершении онлайн-платежа

Рис. 5. Проверка остатка на счёте после совершения покупки

Также важным, на наш взгляд, показателем является то, проверяют ли опрошенные остаток на счёте после каждой совершенной покупки. С одной стороны, это относится к показателям бережливости плательщиков, но с другой может предупредить повторное использование сайта мошенников, поскольку мошенники часто применяют предложение повторного платежа при удачном списании средств у неосмотрительного покупателя.

В январе 2022 года поисковик для покупки жд билетов выдавал в первых строках поиска поддельный сайт с названием rzd.group. Ничего не подозревающий пользователь заходил на него, видел логотип РЖД (чуть измененный, но с изменениями, незаметными обычному потребителю). Далее следовал выбор билетов с базой данных, которую мошенники воровали в реальном времени у РЖД. И когда наступал момент оплаты, и человек, не проверив от кого и в каком размере пришел запрос на оплату, вводил код подтверждения, ему выдавалось сообщение о том, что оплата якобы не прошла и предлагалось совершить платеж с использованием карты другого банка (см. рис.6)

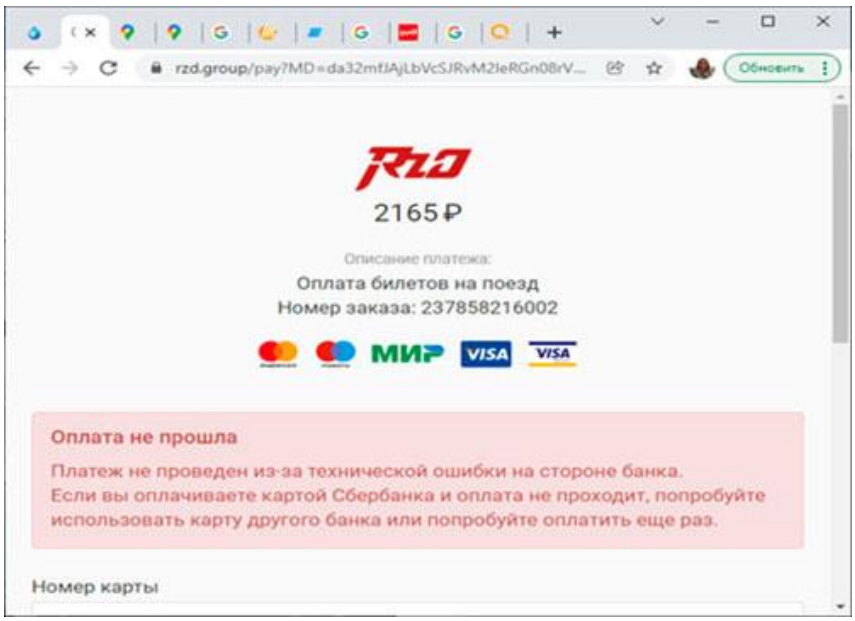

Рис. 6. Сообщение с сайта мошенников после оплаты услуги

Поэтому очень важна проверка данных стороны, запросившей оплату. Данную информацию пользователь получает либо в виде смс-сообщения, либо в виде push-уведомления, либо вообще никак.

При получении смс-сообщения, оно появляется на телефоне и далее хранится в разделе смс, где их можно прочитать в любое время. В отличие от смс для push-уведомлений нет встроенного приложения и практический у всех они после показа помещаются в раздел оповещений телефона и их полный текст можно увидеть лишь зайдя в приложение банка. Но самый плохой сценарий развития событий — это когда оповещения в принципе не приходят, поскольку тогда плательщик вообще не может узнать, кому и какую сумму он на самом деле переводит. И по результатам нашего опроса получилось, что 48,2 % получают push-уведомления, 46 % — смс-оповещения и 5,8 % вообще не получают никаких уведомлений, что, очевидно, способствует процветанию деятельности мошенников.

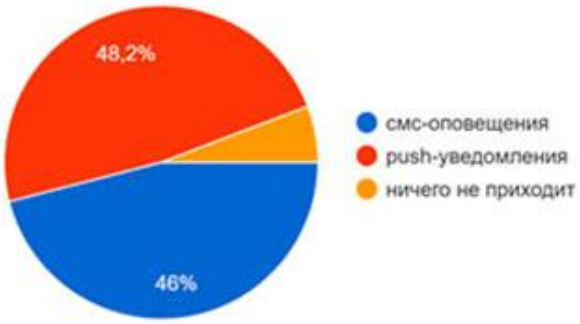

Рис. 7. Соотношение разных видов банковских оповещений при совершении онлайн-покупок.

Что же делать если человек попал в ситуацию, когда с него сняли некую ощутимую сумму на сайте мошенников? В соответствии с Российским законодательством человек может подать заявление в полицию о факте мошенничества. Это можно и нужно делать, хотя шансов возврата денежных средств обычно немного, поскольку схемы работы мошенников очень часто меняются и постоянно придумываются все более новые.

При обращении в банк вам сообщат, что у банка нет возможности опротестовать оспариваемые платежи. Также согласно Правилам предоставления и использования банковских карт Клиент обязан соблюдать сохранность карты и ее реквизитов, и правильно введенный ПИН при совершении операции, а также оформленный в сети Интернет заказ предприятию торговли (услуг), с указанием в нем реквизитов Карты (в том числе таких, как: номер и срок действия Карты, коды CVC2/CVV2/ППК и/или логин и пароль 3D-Secure) являются для Банка распоряжением Клиента списать сумму операции с карточного счета. Операции, совершенные с помощью CVC/CVV/ППК/3DS, считаются совершенными Держателем и не могут быть оспорены. То есть, лицо, которое ввело правильный код подтверждения

тем самым полностью согласилось с проведением платежа и несёт за это ответственность.

Компания, сайт которой подделали мошенники сообщит, что без обращения в полицию, без подачи туда заявления о мошенничестве они, равно как и банк, не имеют юридического основания начинать какие-либо действия. Любая другая компания, задействованная в процессе, сообщит потерпевшему то же самое.

Банки рекомендуют использовать только проверенные приложения из известных источников или известные и проверенные сайты компаний (например, сайт Аэрофлота или S7 для покупки авиабилетов, сайт «River gauche» для покупки косметики соответствующих брендов и т.п.). Но, к сожалению, это не всегда возможно, хотя и вполне разумно.

Еще один вариант для сохранения средств в безопасности от онлайн-мошенников, который рекомендуют банки, это хранить все средства на внутреннем счёте, а на самой карте хранить лишь сумму, необходимую для текущего платежа. Это точно обезопасит вас от рассмотренного выше вида мошенничества, но потребует усилий по переводу средств каждый раз для совершения платежа. Иными словами, вы должны решить, какой суммой согласны рискнуть, оставляя ее на карте.

В этой связи мы поинтересовались, какую сумму наши участники опроса считают безопасным хранить на карте для совершения обычных платежей. В итоге лишь 2,9 % следуют безопасному сценарию и для каждого платежа переводят деньги с внутреннего счета на карту. Еще одна категория — 1,5 % — хранит максимум 500р. 7,3 % считают безопасным хранить 500–1 000 р., по 28,5 % 1 000–5 000р. и 5 000–15 000р., 21,9 % — больше 15 000р. и 9,5 % хранят на карте все средства, что у них есть. Отсюда видно, какую сумму не боятся потерять те или иные категории опрошенных, потому что при нахождении на карте определенного количества средств означает, что попадание на сайт мошенников в сумме с невнимательностью при проверке суммы платежа и того, кто его запрашивает, позволит вышеуказанным мошенникам лишить вас любой суммы в пределах того, что находится на карте.

Рис. 8. Количество средств, хранимых на карте участниками опроса

Итак, из описанного выше можно сделать выводы. Дабы не стать жертвой онлайн-мошенников и сохранить свои средства от посягательств, во-первых, конечно, проверять кто запросил оплату и в каком размере, во-вторых, использовать проверенные и известные приложения и официальные сайты компаний, а также известные маркетплейсы, и, в-третьих, хранить все средства на внутреннем счете банка, и не лениться переводить нужные средства на карту для совершения платежа. ■

The habits of the modern young consumer of online payments

This article analyzes the current situation with online payments, discusses the habits of people who prefer online payments, identifies threats in the form of getting to the sites of fraudsters and makes recommendations to avoid losing funds when getting to the sites of fraudsters.

Keywords: online payments, online purchases, fraudsters, SMS notifications, push notifications, fraudster sites