Научная статья
УДК 343.9

МОБИЛЬНЫЕ ЛОВУШКИ: КАК СОВРЕМЕННЫЕ ТЕХНОЛОГИИ СТАНОВЯТСЯ ИНСТРУМЕНТАМИ ХИЩЕНИЙ

Устиния Игоревна МИЛЮТИНА
Санкт-Петербургский юридический институт (филиал)
Университета Прокуратуры Российской Федерации, Санкт-Петербург, Россия
milyutina.ustiniya@mail.ru

Научный руководитель доцент кафедры уголовного процесса и криминалистики Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент **Мария Александровна Григорьева**, mgrek@inbox.ru

Аннотация. Статья посвящена исследованию способов хищения, совершаемых с использованием средств мобильной связи. Автор акцентирует внимание на наиболее часто используемых криминальными операторами схемах манипуляции жертвами и получения доступа к их финансовым ресурсам.

Ключевые слова: хищение, звонок, SMS-сообщение, денежные средства, социальная инженерия, жертва.

MOBILE TRAPS: HOW MODERN TECHNOLOGIES ARE BECOMING TOOLS OF THEFT

Ustiniya I. MILYUTINA
St. Petersburg Law Institute (branch)
University of the Prosecutor’s Office of the Russian Federation milyutina.ustiniya@mail.ru

Scientific adviser — Associate Professor at the Department of Civil law disciplines, St. Petersburg Law Institute (branch) of the University of the Prosecutor's Office of the Russian Federation, candidate of Legal Sciences, Associate Professor
M. A. Grigoryeva, mgrek@inbox.ru

Abstract. The article is devoted to the study of methods of theft committed with the use of mobile communication means. The author focuses on the most common schemes used by criminal operators to manipulate victims and gain access to their financial resources.

Keywords: theft, call, text message, money, social engineering, victim.

Феноменальный научно-технический прогресс XX века, как и любое достижение человечества, имеет обратную сторону медали – практически каждое полезное изобретение может быть использовано злоумышленниками в противоправных целях. В частности, современные средства мобильной связи не только обеспечивают возможность мгновенной передачи голосовой информации, но и открывают доступ к персональным данным и банковским счетам пользователей, что создаёт новые возможности для разработки мошеннических схем.

По данным Генеральной прокуратуры Российской Федерации число преступлений, совершенных с использованием сети Интернет и средств мобильной связи, выросло в 2023 году на 39,3% по сравнению с аналогичным периодом прошлого года[1].

Ежегодный рост преступлений данной категории связан с относительной простотой совершения хищений денежных средств в телекоммуникационных сетях, так как большинство атак можно проводить удаленно и для них не требуется специальное оборудование или высокий уровень технических знаний. Лишь понимание принципа работы социальной инженерии, искусство убеждать и умение манипулировать людьми становятся ключевыми факторами для злоумышленников. Они могут использовать различные методы, такие как фишинг, смс-мошенничество или подмена идентификации, чтобы обманом получить доступ к личной информации жертв.

Так, все способы хищений, совершаемых с использованием средств сотовой IP-телефонии можно классифицировать на две большие группы:

- совершаемые посредством телефонного звонка;

- совершаемые посредством отправления SMS-сообщения[2].

Главной задачей «мобильных мошенников» является склонение жертвы к добровольной передаче своих денежных средств. Для достижения этой цели применяются разнообразные схемы.

---

[1] О преступлениях, совершенных в сфере информационных технологий // Генеральная прокуратура Российской Федерации : офиц. сайт. URL: https://epp.genproc.gov.ru/web/proc_pvfo/mass-media/news/news-regional?item=91381247 (дата обращения: 20.09.2024).

[2] Лабутин А. А. «Мобильные» мошенничества: основные способы совершения // Вестник Казанского юридического института МВД России. 2013. №12.

1. Телефонный звонок:

- **голосовой спам** - один из наиболее распространённых видов голосового мошенничества, нацеленный на большие группы клиентов мобильного оператора. Мошенники получают списки телефонных номеров из утекших баз данных или просто купленных онлайн. В основном они используют автодозвоны для генерации большого количества звонков и используют предварительно записанные сообщения (робозвонки), которые в дальнейшем могут быть переадресованы оперативным агентам преступного колл-центра для взаимодействия с жертвами. Благодаря низкой стоимости и масштабируемости систем вызова злоумышленники могут совершать миллионы звонков и легко расширять экосистему мошенничества;

- **телемаркетинг** - это метод прямого маркетинга, при котором продавец через телефонный звонок склоняет путём обмана клиентов покупать товары или услуги, представленные криминальным оператором через журналы, ссылки, сайты;

- при **голосовом фишинге** (также известном как *вишинг*) вызывающий абонент имитирует законную организацию или физическое лицо и пытается получить доступ к персональной и финансовой информации с помощью методов социальной инженерии. Подделка идентификатора (номера телефона или IP-адреса) вызывающего абонента часто используется мошенниками для сокрытия своей реальной личности и затрудняет блокировку спам-звонков. Чаще всего встречаются звонки якобы от банков, мобильных операторов, правоохранительных органов, иных государственных служб, которые под разным предлогом пытаются получить от жертвы конфиденциальную информацию. Чаще всего речь идёт о банковских данных и паролях. Например, «представитель» сотового оператора сообщает, что у жертвы истёк срок договора на оказание услуг сотовой связи, его необходимо продлить через сайт государственных услуг, иначе абонент может остаться без связи, в результате чего злоумышленником устанавливается переадресации с номера, открывается вся информация, привязанная к номеру телефона;

- при звонках от **технической поддержки** вымогатели пытаются убедить

людей в том, что их компьютер заражен вредоносным ПО (в основном путем обмана с целью установки инструментов удаленного доступа) и запрашивают платеж для решения так называемой проблемы;

- при **мошенничестве с авансовым платежом** жертву обманом заставляют произвести некоторый авансовый платеж или, например, оплатить подоходный налог, чтобы иметь возможность получить более крупную сумму денег, например, фиктивный лотерейный приз. Аналогичной является **афера с бесплатными круизами**, когда мошенники рекламируют возможность бесплатного круиза, но позже требуют дополнительных платежей;

- отдельно стоит выделить **звонки от банков,** которые начинаются, например, с заманчивого предложения снизить процентные ставки по кредитной карте или аккумулировании всех кредитов на одном счету для более выгодного их погашения. Затем звонок переключается на живого агента, который запрашивает номер кредитной карты и срок ее действия, имя, адрес, а в некоторых случаях даже номер социального страхования. Другой случай, когда поступает звонок якобы от сотрудника банка, который сообщает, что банком была замечена угроза списания денежных средств с банковского счёта, и для того, чтобы их обезопасить, нужно перевести деньги на «безопасный» счёт, номер которого продиктован «сотрудником» банка. Так, в сентябре 2024 года известная народная артистка России, эстрадная певица Лариса Долина попалась на уловку мошенников по продаже квартиры и переводе денежных средств на «безопасный» счёт в размере 200 млн рублей[3];

- **звонок с использованием искусственного интеллекта** позволяет злоумышленникам выдавать себя за друзей и знакомых потенциальной жертвы, вводя в заблуждение путём обмана. Для этого требуется всего за три секунды аудиозаписи, чтобы “клонировать” голос человека для использования в мошеннических звонках. Мошенники могут найти аудиоклип в Интернете (или через вашу голосовую почту) а затем использовать этот клон для активации устройств

[3] Осторожно, мошенники: эксперт объяснила схему обмана Ларисы Долиной // ТАСС : информ. агентство России : сайт. Москва. Обновляется в течение суток. URL: https://tass.ru/obschestvo/21922273 (дата обращения: 23.09.2024).

с голосовым управлением, создания фальшивых видеороликов, проведения голосового фишинга.

Нельзя не отметить угрозу существования **deepfake** (англ. - глубокая подделка) суть которой заключается в осуществлении видео-звонка от сгенерированного компьютером лица, которое накладывается на другого человека. Таким образом один из офисов многонациональной компании в Гонконге стал жертвой аферы злоумышленника с использованием видеотехнологии deepfake, который выдал себя за руководителя и выманил у компании 200 миллионов гонконгских долларов (25,6 миллиона долларов)[4].

2. SMS-сообщения строятся по такому же принципу и в целом схожи с другими способами дистанционных хищений денежных средств с помощью мобильной связи. Они часто содержат заманчивые предложения или угрозы, чтобы вызвать у жертвы чувство срочности и решимости:

- **смишинг (SMS + phishing)** – это форма фишинговой атаки, использующая короткие сообщения (SMS) о том, что украдена учётная запись или заморожен номер банковского счёта. Прикрепленная ссылка направляет на веб-сайт для «проверки» информации о счёте. В ходе кибератаки хакер обманным путем заставляет жертву раскрыть конфиденциальную информацию, чтобы использовать ее для своих злонамеренных действий.

- **ошибочный перевод средств**: просят вернуть деньги, а потом дополнительно снимают сумму по чеку[5]. Абоненту поступает SMS-сообщение о том, что через «мобильный банк» ему случайно был осуществлен перевод денежных средств. Вскоре после этого поступает звонок с просьбой перевести эти деньги обратно тем же способом;

- сообщения от **транспортных компаний или службы доставки.** В условиях пандемии Covid-19 большое количество людей пострадало от ложных сообщений об изменениях условий доставки заказанных товаров, её переносе и

[4] Deepfake video call scam cons company out of $25 million. [Электронный ресурс] // URL: https://readwrite.com/deepfake-video-call-scam-cons-company-out-of-25-million/ (дата обращения: 22.09.2024).
[5] Лабутин А. А. «Мобильные» мошенничества: основные способы совершения // Вестник Казанского юридического института МВД России. 2013. №12.

т.п. В сообщении прикреплялась ссылка для ознакомления, подтверждения, уточнения информации, переходя на которую, пострадавший оказывался на мошенническом сайте, запрашивающем личную информацию или предоплату за доставку посылки;

- **сообщения от банков**, например, с использованием подменной идентификации от номера 900. Пользователю сообщается, что его банковский счёт был заблокирован при обнаружении угрозы из безопасных соображений. Чтобы восстановить доступ необходимо перейти по ссылке или позвонить по номеру телефона, после чего произойдет хищение денежных средств;

- **сервисы подписки**, такие как Netflix, Okko и другие стали частой мишенью текстовых мошенников. В ходе этих мошеннических действий абонент получаете текстовое сообщение, в котором утверждается, что его учетная запись заблокирована из-за неуплаты или что у него есть деньги, ожидающие из-за “переплаты”. Для их получения опять же прикрепляется ссылка, переходя на которую можно стать жертвой хищения;

- сообщение **о необходимости установления двухфакторной аутентификации**, которая добавляет дополнительный уровень безопасности учетным записям в приложениях, социальный сетях или мессенджерах. Она работает путем отправки короткого кода на мобильное устройство, как только обнаруживается попытка входа в учетную запись. С использованием подменной идентификации криминальный оператор подделывают номер общеизвестной компании (например, telegram) и отправят сообщение, в котором сообщает, что техническая поддержка приложения обнаружила “подозрительную активность при входе” в учетную запись. Чтобы избежать блокировки учетной записи, просят отправить им свой код двухфакторной аутентификации. Отправив его, абонент предоставляет доступ к своей учетной записи.

Новая схема дистанционного мошенничества с использование мобильных средств связи была выявлена в Вологодской области. Потерпевшие в разное время на различных интернет-платформах размещали объявления о пропаже своих вещей. По телефону с ними связывалась неизвестная женщина, представлявшаяся работником ломбарда или заверявшая, что нашла потерянную вещь,

после чего SMS-сообщением отправляла номер телефона, на который необходимо перевести предоплату вознаграждения за найденную вещь, после чего больше не выходила на связь. В результате оперативно-розыскных мероприятий была найдена подозреваемая, в отношении которой возбуждено уголовное дело по ч. 2 ст. 159 УК РФ, предусматривающей ответственность за мошенничество, совершенное с причинением значительного ущерба гражданину[6].

В заключение, необходимо подчеркнуть, что мошенничество с использованием средств мобильной связи представляет собой серьезную угрозу для финансовой безопасности граждан и требует комплексного подхода к решению данной проблемы. Учитывая тот факт, что арсенал мошеннических сценариев постоянно обновляется и расширяется, в работе были представлены не все, но наиболее часто встречающиеся способы хищений.

Ежегодный рост числа подобных преступлений подчеркивает важность повышения осведомленности населения о методах защиты от действий мошенников, а также необходимости активного сотрудничества между правоохранительными органами, финансовыми учреждениями и технологическими компаниями.

Список источников

1. Лабутин А. А. «Мобильные» мошенничества: основные способы совершения // Вестник Казанского юридического института МВД России. - 2013. - №12.
2. О преступлениях, совершенных в сфере информационных технологий // Генеральная прокуратура Российской Федерации : офиц. сайт. URL: https://epp.genproc.gov.ru/web/proc_pvfo/mass-media/news/news-regional?item=91381247 (дата обращения: 20.09.2024).
3. Осторожно, мошенники: эксперт объяснила схему обмана Ларисы Доли-

[6] Сотрудники областного уголовного розыска раскрыли серию дистанционных мошенничеств // Управление МВД России по Вологодской области : офиц. сайт. URL: https://35.мвд.рф/news/item/12919870/ (дата обращения: 23.09.2024)

ной // ТАСС : информ. агентство России : сайт. Москва. Обновляется в течение суток. URL: https://tass.ru/obschestvo/21922273 (дата обращения: 23.09.2024).

4. Сотрудники областного уголовного розыска раскрыли серию дистанционных мошенничеств // Управление МВД России по Вологодской области : офиц. сайт. URL: https://35.мвд.рф/news/item/12919870/ (дата обращения: 23.09.2024)
5. Deepfake video call scam cons company out of $25 million. [Электронный ресурс] // URL: https://readwrite.com/deepfake-video-call-scam-cons-company-out-of-25-million/ (дата обращения: 22.09.2024).

Информация об авторах

У.И. МИЛЮТИНА — студент 5 курса.

Information about authors

U.I. MILYUTINA — 5th year student.