Научно-теоретическая статья
УДК 316.663.5
DOI: 10.24412/2078-9238-2024-452-81-89

ЯЗЫК ОБМАНА: СХЕМА СЦЕНАРИЯ И ПРИЧИНЫ ВОВЛЕЧЕНИЯ ЖЕРТВ В СИТУАЦИИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Змазнева О. А.

Московский политехнический университет,
Москва, Россия,
ozmazneva@gmail.com

Аннотация. Современный человек большое количество времени проводит в открытом публичном медиапространстве, например в социальных сетях, где он оставляет цифровой след, не задумываясь, каким образом и кем может быть использована предоставленная им о себе информация, зачастую содержащая конфиденциальные данные. В статье рассматриваются роли участников мошеннических действий в ситуации телефонных переговоров, анализируется типовой сценарий игры «Жертва – Спасатель» и схема этапов вовлечения жертвы в диалог и склонения ее к принятию незамедлительного, выгодного для злоумышленника решения, а также описываются некоторые основные причины вовлечения потенциальных жертв в предлагаемые мошенниками игры. В исследовании автор опирается на метод транзактного (трансакционного) анализа Э. Берна, работы социолога М. Кастельса, социального психолога Р. Чалдини, исследования зарубежных ученых, а также использует статистические данные ВЦИОМ за 2021/2024 годы.

Ключевые слова: телефонные мошенники, транзактный/трансакционный анализ, спам, жертва мошеннических действий

Для цитирования: Змазнева О. А. Язык обмана: схема сценария и причины вовлечения жертв в ситуации телефонного мошенничества // Вестник МГПУ. Серия «Философские науки». 2024. № 4 (52). С. 81–89. DOI: 10.24412/2078-9238-2024-452-81-89

Благодарности: автор благодарит студентов факультета информационных технологий Московского политехнического университета за искреннее обсуждение интересующих их проблем — именно во время этих дискуссий и появилась идея этой статьи.

Scientific and theoretical article
UDC 316.663.5
DOI: 10.24412/2078-9238-2024-452-81-89

THE LANGUAGE OF DECEPTION: THE SCHEME OF THE SCENARIO AND THE REASONS FOR THE INVOLVEMENT OF VICTIMS IN A SITUATION OF TELEPHONE FRAUD

Olesya A. Zmazneva

Moscow Polytechnical University,
Moscow, Russia,
ozmazneva@gmail.com

Abstract. Modern people spend a lot of time in the open public media space, for example, on social networks, where they leave a digital footprint, without thinking about how and by whom the information they provide about themselves, often containing confidential data, can be used. The article examines the roles of participants in fraudulent actions in the situation of telephone conversations, analyzes the typical scenario of the game "Victim – Rescuer" and the scheme of stages of involving the victim in a dialogue and persuading her to make an immediate, beneficial decision for the attacker, and also describes some of the main reasons for involving potential victims in the games offered by scammers. In the study, the author relies on the method of transactional analysis by E. Bern, the work of sociologist M. Castells, social psychologist R. Cialdini, research by foreign scientists, and also uses statistical data from WCIOM 2021/2024.

Keywords: phone scammers, transactional analysis, spam, victim of fraud

For citation: Zmazneva, O. A. (2024). The language of deception: the scheme of the scenario and the reasons for the involvement of victims in a situation of telephone fraud. *MCU Journal of Philosophical Sciences, 4* (52), 81–89. https://doi.org/10.24412/2078-9238-2024-452-81-89

Acknowledgements: the author thank the students of the Faculty of Information Technology of Moscow Polytechnic University for discussing topical issues and related problems — it was during these discussions that the idea for this article appeared.

Введение

Значимые изменения в коммуникации, которые мы наблюдаем в течение нескольких десятилетий, воздействуют на все сферы человеческой жизни, на модели поведения человека в обществе и на его мышление. Новая технологическая парадигма в области информационно-коммуникационных технологий (ИКТ) задает новые коммуникативные сценарии.

Как отмечает Мануэль Кастельс, «быстрое распространение Интернета с середины 90-х годов стало результатом сочетания трех факторов:

1. Технологическое открытие Всемирной паутины.

2. Институциональные изменения в управлении Интернетом, находящимся под общим управлением глобального интернет-сообщества, но приватизированным и разрешающим как коммерческое, так и коллективное использование.

3. Глобальные перемены в культуре и социальном поведении: индивидуализация и осетевление» [Кастельс, 2020, с. 6–17].

Одним из ключевых изменений в культуре является «сдвиг от массовой коммуникации, основанной на массмедиа, к массовой самокоммуникации, основанной на Интернете» [Кастельс, 2020, с. 17]. Действительно, современный человек проводит большое количество времени в Интернете и социальных сетях, где оставляет значительный цифровой след, в том числе и персональные данные, которые могут быть использованы и в мошеннических целях.

По данным Всероссийского центра изучения общественного мнения (ВЦИОМ), число жертв телефонного мошенничества растет с каждым годом: в ходе опроса, проведенного в феврале 2024 года, «67 % россиян признались, что за последние полгода – год получали фейковые звонки, тогда как еще в 2021 года о таком опыте могли рассказать чуть больше половины наших сограждан (57 %, + 1 п.п. за три года)»[1].

Один из основных критериев выбора жертвы — это место проживания. «Наиболее подвержены телефонному мошенничеству жители обеих столиц: с ним сталкивались 85 % москвичей и петербуржцев…»[2]. Сделаем предположение, что жители двух этих крупных городов предоставляют Сети информацию о себе в большем объеме, чем, скажем, жители сельских населенных пунктов. Заметим, что даже по предварительнму просмотру и несложному анализу публикаций в социальных сетях: фотографиям, местам посещения, статусам и прочему — можно, во-первых, собрать персональную информацию о потенциальной жертве, во-вторых, получить представление о ее/его привычках и, в-третьих, сделать предварительную оценку ее/его платежеспособности.

Стандартные роли участников типовых коммуникативных актов в сценарии телефонного мошенничества можно обозначить как «Жертва» и «Помощник»/«Спасатель».

Проанализируем пример типового сценария. При анализе будем частично опираться на схему, предложенную в свое время для транзактного (трансакционного) анализа психотерапевтом Эриком Берном [Берн, 2019]. В нашем анализе используем параметры: «Тезис декларируемый», «Цели: демонстрируемая и реальная» (дифференциация целей отсутствует в схеме Берна), «Роли», «Примеры», «Этапы («Ходы» у Э. Берна)». Сценарий сопроводим рекомендациями.

Сценарий: «Звонок от представителя банка».

---

[1] Телефонное мошенничество: мониторинг. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring (дата обращения: 15.09.2024).

[2] Там же.

Тезис декларируемый: *Банк реагирует на подозрительные действия и защищает клиента.*

Цель демонстрируемая: *Защита клиента.*

Цель реальная: *Создание доверительных отношений и получение данных для вывода/перевода денег; для перевода/личной передачи денег.*

Роли: *«Представитель банка» — Спасатель.*

Адресант/Клиент — потенциальная Жертва.

Этапы: *Знакомство – вброс информации о потенциальной угрозе – предложение помощи / уговоры / запугивание / шантаж: «Вы переводили деньги на преступные цели».*

Пример: Во время разговора «сотрудник банка» — мошенник может сообщить, что карта адресата заблокирована или что произошла подозрительная транзакция. Он попытается получить личные данные, такие как номер карты или код безопасности.

Реакция на тезис декларируемый: *Сотрудники банка обычно не звонят клиентам. Если адресат незадолго до звонка не совершал какую-либо крупную транзакцию, которая требует подтверждения, продолжать коммуникацию нет необходимости.*

Распознавание этапов, их анализ: *какие эмоции и состояния собеседник на разных этапах диалога пытается вызвать у адресата и почему?*

Пример анализа:

Знакомство: сотрудник банка называет клиента по имени-отчеству (владеет персональной информацией, использует официальный стиль в общении, говорит уверенно, быстро и эмоционально — пытается вызвать у клиента состояние доверия и паники — Зачем? — (чтобы не было времени рассуждать логично и распознать мошенника).

Вброс информации о потенциальной угрозе — предложение помощи / уговоры / запугивание / шантаж — предложение помощи: «Вы переводили деньги на преступные цели — поэтому вы уже являетесь соучастником преступления. Мы хотим вам помочь…».

Причины вовлечения жертв в мошеннические сценарии

Случаи телефонного мошенничества становятся все более распространенным явлением, и понимание причин, по которым получатели сообщений вовлекаются в предлагаемые сценарии, имеет важное значение для разработки эффективных мер профилактики — работы с потенциальными жертвами из групп риска.

Роберт Чалдини, социальный психолог, автор ряда работ по техникам убеждения, в том числе бестселлеров «Психология влияния» и «Техники пре-убеждения» отмечает, что все методы и техники убеждения и пре-убеждения (в данном случае речь идет о подготовительной работе перед непосредственным

озвучиванием просьбы/требования) в той или иной степени базируются на взаимности, благорасположении, социальном доказательстве, авторитете, дефиците и последовательности [Чалдини, 2018].

Р. Чалдини отдельно отмечает, что «особого внимания в силу его глубокого и широкого воздействия на аудиторию» располагает «авторитетный коммуникатор»: «Когда говорит признанный эксперт по конкретной теме, люди, как правило, поддаются убеждению» [Чалдини, 2018, с. 237]. Не менее важен в контексте нашей темы и комментарий автора: «Это особенно верно, когда слушатель не знает, что ему делать» [Чалдини, 2018, с. 237].

Злоумышленники в ряде типовых сценариев используют схему с «авторитетным коммуникатором». В его роли выступает мошенник, который может представиться как «руководитель организации», где работает адресат сообщения; «сотрудник банка», в котором у жертвы открыт счет, «представитель органов власти»: сотрудник полиции, налоговой инспекции; представители сферы услуг и пр. В ряде случаев злоумышленники могут имитировать голоса близких родственников. В самом начале разговора злоумышленники создают эмоциональную (стрессовую) коммуникативную ситуацию, которая может сопровождаться истерикой и плачем («Вам звонят из больницы, где в реанимации находится ваш родственник…»), криками, использованием ненормативной лексики, различными фразами, выражающими угрозы, шантаж. Одна из задач, которая реализуется при создании такого эмоционального фона, — поставить жертву в условия немедленного принятия решения. Следовательно, создание образа авторитетного коммуникатора и условий для паники — это обязательные условия проведения телефонных переговоров в сценарии «Спасатель – Жертва».

Схема этапов типового разговора злоумышленника с потенциальной жертвой может быть представлена следующим образом:

1. Злоумышленник (Спасатель) представляется (называет фамилию, имя, отчество, место работы, должность. Может также быть названа фамилия лица, от имени которого Спасатель ведет переговоры (например, «руководитель службы безопасности» — от имени «директора компании»).

2. Сообщает некую информацию, которая призвана подтвердить наличие у злоумышленника доступа к персональным/конфиденциальным данным Жертвы (например, «сотрудник банка» говорит о том, что только что была проведена транзакция и называет сумму и данные о получателе перевода) и тем самым поместить его в ранг авторитетного источника информации и вызвать доверие у адресата.

3. Далее, в случае, если Жертва на предыдущих этапах реагирует эмоционально и включается в диалог, используются методы уговоров, запугивания, шантажа и пр. Основное требование злоумышленника, предъявляемое Жертве, — принять решение незамедлительно, чтобы Жертва не имела возможности проанализировать ситуацию и понять настоящее положение дела. Дополнительными приемами создания образа «авторитетного коммуникатора»

являются уверенный голос, ссылка на знакомые Жертве имена, упоминание некоторых действий Жертвы в прошлом и пр. Использование технологий дипфейка сейчас уже выводит мошенников на более сложный для распознавания простыми методами уровень (так, известен случай, когда мошенник по просьбе реального сотрудника банка пройти идентификацию подключился со сгенерированным нейросетями видеоизображением и смог, подтвердив таким образом личность, вывести со счетов деньги клиента, чье видеоизображение ему удалось воспроизвести с помощью цифровых технологий.

Еще один аргумент в арсенале злоумышленников — это «свидетельство силы социального доказательства». Р. Чалдини отмечает, что «люди считают приемлемым для себя верить, чувствовать или делать что-то в той мере, в какой верят, чувствуют или делают это другие люди, особенно схожие с ними» [Чалдини, 2018, с. 232]. В связи с этим злоумышленник в роли, например, «представителя службы безопасности компании», в которой работает Жертва, может упомянуть, что многие ее/его коллеги уже выполнили те действия, которые сейчас предлагается выполнить и Жертве. При этом есть необходимое условие — неразглашение только что полученной информации.

Проанализируем основные причины, по которым Жертвы вовлекаются в сценарии, предлагаемые злоумышленниками, условно ранжируя их от наименее частотных к наиболее распространенным.

1. Низкий уровень осведомленности получателей сообщений о сценариях действий мошенников.

Многие адресаты не осведомлены в достаточной степени о существовании телефонных мошенничеств и не осознают опасности, с которой могут столкнуться. Отсутствие информации приводит к тому, что жертвы не могут распознать мошеннические схемы.

2. Социальная изолированность.

Ряд исследователей наблюдает прямую корреляцию между изолированностью/асоциальностью человека и его уязвимостью перед действиями мошенников. В частности, Дж. Лим отмечает рост мошеннических действий во время пандемии — в период принудительной изоляции людей [Lim]. В условиях социальной изоляции и/или одиночества человек склонен доверять скорее, если мошеннику удается с первых слов убедить Жертву в проявлении заботы о ней. В качестве подтверждения приведем цитату из исследования ВЦИОМ 2021 года: «Три четверти россиян (76 %) поддержали бы разговор с незнакомым человеком, вызвавшим у них симпатию, 20 % не стали бы поддерживать разговор»[3].

Проблема социализированности/асоциальности представляется здесь заслуживающей более детального рассмотрения, что может стать темой для следующих исследований.

---

[3] Телефонное мошенничество: мониторинг. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring (дата обращения 15.09.2024).

3. Эмоциональная уязвимость.

Эмоции играют ключевую роль в процессе принятия решений. Мошенники часто используют манипуляции, чтобы вызвать у адресата чувство страха или срочности для принятии быстрого решения. С другой стороны, как отмечает ряд исследователей, мошенники стремятся завоевать доверие адресата, для чего используют обращение по имени / имени-отчеству, ссылаются на рекомендацию авторитетного для адресата человека («Ваш руководитель — Ф. И. О. — передал нашей службе безопасности ваши контакты…» [Парсонс, 2018].

4. Социальное давление.

Получатели сообщений могут вступать в диалог с мошенниками из-за давления — не только прямого, но и косвенного — со стороны окружающих. Например, если в окружении потенциальной жертвы, в частности, в комментариях к опубликованным в социальных сетях постам, кто-либо расскажет о том, как он получил выигрыш, это может подтолкнуть жертву к тому, чтобы тоже попытаться «поймать удачу». Социальное давление может существенно влиять на поведение человека, на его подверженность воздействию, в том числе и негативному, давать ему оценку, а, как мы знаем, «моральная оценка — решающий аспект действия в социальных системах» [Чалдини, 2024, с. 262].

5. Доверие к авторитетам.

Один из самых распространенных приемов мошенников — обращение по имени / имени-отчеству и самопрезентация в качестве сотрудника известных жертве компаний или государственных организаций с целью вызвать у жертвы доверие. По данным ряда исследований, люди склонны доверять звонкам от тех, кто представляется официальными лицами [Чалдини, 2024].

6. Низкий уровень финансовой грамотности.

Недостаток знаний в области финансов может привести к тому, что получатели сообщений не понимают, как работают финансовые системы, какие риски существуют, как обезопасить свои средства и пр.

7. Стереотипные представления об образе мошенника.

Многие люди имеют устаревшие представления о том, как выглядит мошенничество, что делает их более уязвимыми к современным схемам. Стереотипы о мошенниках часто не соответствуют реальности и могут привести к ошибкам в оценке ситуации.

8. Погоня за легким заработком.

Наиболее распространенной причиной подверженности мошенничеству является желание быстрого обогащения. Мошенники активно используют эту особенность человеческой психологии для вовлечения жертв в свою игру. Идея о том, что можно легко и быстро заработать деньги, всегда была привлекательной для человека, но с появлением Интернета и социальных сетей, где в том числе пропагандируются разные способы и возможности для быстрого обогащения, эта мысль приобретает новые формы.

9. Дефицит / страх потери.

«Наше нежелание лишиться чего-то ценного — ключевой фактор. В конце концов потеря — это высшая форма дефицита, делающая ценный предмет или возможность недостижимыми» [Чалдини, 2018, с. 242]. Злоумышленники в первую очередь работают с эмоциями Жертвы — поэтому стремятся создать ситуацию паники и усилить ее описаниями возможных потерь, «если не предпринять здесь и сейчас» ряд «предупреждающих мер».

Заключение

Подверженность вовлечению в диалог с телефонными мошенниками обусловлена множеством факторов, включая низкий уровень осведомленности потенциальной жертвы о сценариях, которые используют злоумышленники, эмоциональную уязвимость, желание быстрого обогащения и страх потери. Понимание этих причин может помочь в разработке более эффективных стратегий профилактики, в частности подготовки и проведения образовательных программ среди наиболее уязвимых групп потенциальных жертв мошеннических действий.

Список источников

1. Кастельс М. Власть коммуникации. М.: ВШЭ, 2020. 591 с.

2. Берн Э. Игры, в которые играют люди. Люди, которые играют в игры. М.: Бомбора, 2019. 560 с.

3. Чалдини Р. Психология влияния. М.: Эксмо, 2018. 416 с.

4. Парсонс Т. О структуре социального действия. М.: Академический Проект, 2018. 435 с.

5. Чалдини Р. Техники пре-убеждения: как получить согласие оппонента еще до начала переговоров. М.: Эксмо, 2024. 400 с.

6. Lim J. Cover study: Consumers more vulnerable to scams during pandemic // The Edge Malaysia. October 7. URL: https://www.theedgemarkets.com/article/cover-story-consumers-more-vulnerable-scams-during-pandemic

7. Bidgoli M., Grossklags J. Hello. This ist he IRS calling: “A case study on scams, extortion, impersonation, and phone spoofing” // APWG Symposium on Electronic Crime Research (eCrime). Scottsdale, AZ, USA, 2017. P. 57–69. DOI: 10.1109/ECRIME.2017.7945055.

8. Button M. M., Nicholls C. M. N., Kerr J., Owen R. Online frauds: Learning from victims why they fall for these scams // Australian and New Zealand Journal of Criminology. 2014. Vol. 47, № 3. P. 391–408. DOI: 10.1177/000486581452122

9. Телефонное мошенничество: мониторинг. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring (дата обращения: 15.09.2024).

10. Одиночество и как с ним бороться. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/odinochestvo-i-kak-s-nim-borotsja (дата обращения: 19.09.2024).

References

1. Kastel's, M. (2020). *The power of communication.* Moscow, VSE. (In Russian).
2, Bern, E. (2019). *Games people play. People who play games.* Moscow, Bombora.
3. Chaldini, R. (2018). *Psychology of influence.* Moscow, Eksmo.
4. Parsons, T. (2018). *On the structure of social action.* Moscow, Academic project.
5. Chaldini, R. (2024). *Pre-persuasion techniques: how to get your opponent's consent before negotiations even begin.* Moscow, Eksmo.
6. Lim, J. Cover study: Consumers more vulnerable to scams during pandemic. *The Edge Malaysia, October 7.* Retrieved from https://www.theedgemarkets.com/article/cover-story-consumers-more-vulnerable-scams-during-pandemic
7. Bidgoli, M., Grossklags, J. (2017) *Hello. This ist he IRS calling: "A case study on scams, extortion, impersonation, and phone spoofing".* APWG Symposium on Electronic Crime Research (eCrime), Scottsdale, AZ, USA, pp. 57–69. https://doi.org/10.1109/ECRIME. 2017. 7945055
8. Button, M. M., Nicholls, C. M. N., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian and New Zealand Journal of Criminology, 47*, 3. 391–408, 2014. https://doi.org/10.1177/000486581452122
9. Telephone fraud: monitoring. Retrieved from https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring
10. Loneliness and how to deal with it. Retrieved from https://wciom.ru/analytical-reviews/analiticheskii-obzor/odinochestvo-i-kak-s-nim-borotsja

Информация об авторе / Information about the author:

Змазнева Олеся Анатольевна — доцент кафедры инфокогнитивных технологий Московского политехнического университета, кандидат филологических наук, доцент; руководитель модуля SoftSkills факультета информационных технологий МПУ; руководитель и модератор научно-популярного проекта «Наука без границ», Москва, Россия.

Zmazneva Olesya A. — Associate Professor, Ph.D. Moscow polytechnical university, IT faculty, infocognitive department. The Head of SoftSkills Module in the MPU IT Department's programs. The director and the moderator of "Science without borders" project, Moscow, Russia.

ozmazneva@gmail.com