УДК 159.9.07, 316.624

ЖЕРТВЫ КИБЕРМОШЕННИКОВ: ОТ ДОВЕРЧИВОСТИ К РАЗОБЛАЧЕНИЮ

Медяник О.В.

доцент кафедры управления рисками и страхования,

Санкт-Петербургский государственный университет,

Санкт-Петербург, Россия

Легостаева Н.И.

старший научный сотрудник факультета социологии,

Санкт-Петербургский государственный университет,

Санкт-Петербург, Россия

Медяник С.И.

инженер-исследователь,

Санкт-Петербургский государственный университет,

Санкт-Петербург, Россия

Аннотация: Стремительное развитие цифровых средств массовой коммуникации породило такое сложное и опасное явление как кибермошенничество, которое можно сравнить с цифровой раковой опухолью современного общества. В данной работе авторы представляют результаты качественного исследования, которое было проведено в октябре 2024 года. Основными результатами интервью с 21 участником исследования стали следующие: 1) доверчивость, склонность к авторитету, эмоциональность, страх - доминирующие психологические факторы, которые делают людей

наиболее уязвимыми к финансовому мошенничеству; 2) фишинговые сайты, мошенничество с трудоустройством, мошенничество в сфере здравоохранения, романтическое мошенничество - основные виды мошенничества, с которыми столкнулись участники исследования; 3) чрезмерное давление на авторитет, создание ситуации дефицита времени, неграмотная речь собеседника, ошибки в оформлении сайта – основные паттерны-подсказчики для участников исследования, которые помогли им распознать кибермошенника.

Ключевые слова: кибермошенничество, психологические особенности жертв, фишинговые сайты, мошенничество с трудоустройством, мошенничество в сфере здравоохранения, романтическое мошенничество.

Благодарности: Исследование выполнено за счет гранта Российского научного фонда № 23-28-00701, «Поведенческие стратегии потребителей финансовых услуг в условиях кибермошенничества: междисциплинарный анализ», https://rscf.ru/project/23-28-00701/

VICTIMS OF CYBERFRAUD: FROM TRUST TO EXPOSURE

Medyanik O.V.

Associate Professor at the Department of Risk Management and Insurance,

Saint Petersburg State University,

Saint Petersburg, Russia

Legostayeva N.I.

Senior Researcher at the Department of Sociology,

Saint Petersburg State University,

Saint Petersburg, Russia

Medyanik S.I.

Research engineer,

Saint Petersburg State University,

Saint Petersburg, Russia

Abstract. The rapid development of digital mass media has given rise to such a complex and dangerous phenomenon as cyber fraud, which can be compared to a digital cancer of modern society. In this paper, the authors present the results of a qualitative study that was conducted in October 2024. The main findings from interviews with 21 study participants were as follows: 1) gullibility, tendency towards authority, emotionality, fear - the dominant psychological factors that make people most vulnerable to financial fraud; 2) phishing sites, employment scams, health care scams, romance scams were the main types of scams that the study participants encountered; 3) excessive pressure on authority, creating a situation of time shortage, illiterate speech of the interlocutor, errors in the design of the site - the main patterns-hints for the study participants that helped them to recognize a cyber fraudster.

Keywords: cyber fraud, psychological characteristics of victims, phishing sites, employment fraud, health care fraud, romance fraud

Acknowledgement: The study was supported by grant No. 23-28-00701 from the Russian Science Foundation, “Behavioral strategies of financial services consumers in the context of cyber fraud: an interdisciplinary analysis”, https://rscf.ru/project/23-28-00701/

Социальные сети и мессенджеры сегодня являются неотъемлемой составляющей повседневной жизни людей, но с их развитием стремительно

растет уровень киберпреступлений, совершаемых злоумышленниками. Существует множество определений кибермошенничества, но одним из универсальных является определение, которое дали Whitty M.T. и Joinson A.N., обозначив его как «любое мошенничество, использующее технологии массовой коммуникации для выманивания у людей денег» [15].

Потенциальной жертвой мошенников может стать любой человек, однако, многие исследователи, опираясь на социально-демографические характеристики, выделяют среди наиболее уязвимых групп населения пожилых людей, подростков, людей с низким уровнем образования [3; 4; 8; 11; 12]. Другие авторы относят к группе риска людей в возрасте 20 – 29 лет [1]. Напротив, в исследовании Whitty M.T. подтвердились гипотезы о том, что мужчины и образованные люди чаще подвергались мошенничеству, чем женщины и менее образованные люди [7; 13].

Ряд исследований посвящен не только половозрастным различиям потенциальных жертв, но и психологическим особенностям пострадавших от действий злоумышленников. Многие авторы отмечают, что более импульсивные и невротичные люди чаще подвергаются кибермошенничеству [7]. Другие исследователи утверждают, что у жертв киберпреступников повышенный уровень доверчивости к окружающим [6]. Ряд авторов, используя рамки теорий повседневной деятельности и самоконтроля, изучали как уровень самоконтроля коррелирует с вероятностью мошенничества [8]. Отдельной группой стоят исследования, в которых авторы изучают социально-демографические и психологические особенности жертв по видам мошенничества: молодежь и женщины более подвержены фишингу [5], жертвы романтического мошенничества более импульсивны и склонны идеализировать своих партнеров [14].

Авторы Parti K. и Tahir F. в ходе проведения интервью с жертвами мошенников пожилого возраста сделали вывод, что киберпреступления - один из видов преступлений, о которых реже всего сообщается, поскольку жертвы злоумышленников испытывают чувство вины, стыда, смущения, потери доверия к правоохраниельным органам, а также психологическое состояние жертв пожилого возраста ухудшается по причине обвинений со стороны членов семьи, отсутствия ИКТ-компетенций, страхом потерять контроль над активами (финансы, социальный статус) [10]. В других исследованиях так же подчеркивается нежелание жертв обращаться в правоохранительные органы по причине избегания стресса и низкой вероятности установления личности кибермошенника [2].

Принимая во внимание вышесказанное и постулат о том, что жертвой кибермошенников может стать любой человек, авторы данной работы в гайд полустандартизированного интервью не включили информацию о возрасте, образовании, месте работы, месте проживания, уровне дохода в семье. В исследовании приняли участие 21 человек (16 женщин и 5 мужчин), которые сами столкнулись со случаем мошенничества, либо их родные, знакомые, коллеги по работе стали жертвами мошенничества. Особенности данной выборки состояли в том, что женщины намного охотнее мужчин отвечали на вопросы и давали короткие комментарии, но при этом необходимо отметить, что эмоциональная напряженность и проявление агрессии были выше у женщин. Объединяющей чертой мужчин и женщин выступало их нежелание давать развернутые и длинные комментарии в процессе интервьюирования. Гайд интервью включил в себя следующие вопросы: «Как бы Вы оценили свои знания о финансовом мошенничестве и методах защиты от него?», «Насколько Вы уверены в своей способности распознать и противостоять различным мошенническим схемам?», ««Как Вы думаете, какие психологические факторы делают людей наиболее уязвимыми к финансовому

мошенничеству?», «С какими видами мошенничества сталкивались Вы или Ваши близкие, знакомые или коллеги по работе?», «Когда Вы или Ваши близкие, знакомые или коллеги по работе столкнулись с попыткой финансового мошенничества, удалось ли распознать его?», «Как Вам или Вашим близким, знакомым или коллегам по работе удалось распознать мошенников? Что подсказало, что эти люди - мошенники?».

На вопрос «Как бы Вы оценили свои знания о финансовом мошенничестве и методах защиты от него?» половина информантов (11 человек) ответили, что их знания находятся на высоком уровне, были получены следующие ответы: «я много знаю о финансовом мошенничестве, сейчас часто говорят про мошенников и передачи показывают», «до того, как я и моя семья не столкнулась с мошенниками, я знала мало, теперь я знаю очень много», «да, про них уже все и всем известно», «я много читал про них, по телевизору говорят быть осторожными, и в банках тоже информация висит». Из них 3 участника исследования сказали, что их знания находятся на очень высоком уровне: «теперь я сам могу вас проконсультировать», «я – профи и меня не проведешь», «я стала специалистом по распознанию преступников из своего горького опыта». 6 информантов сообщили о среднем уровне знаний: «того, что я знаю хватает, но можно еще поучиться новым знаниям», «знаний хватает, чтобы не брать трубку от незнакомого номера и не разговаривать с ним», «думаю, что знаний хватает, сегодня тема мошенников часто обсуждается в СМИ и в сетях». Среди ответивших были и такие, которые оценили свой уровень знаний на низком уровне (3 информанта): «я волнуюсь за свою маму, что я не смогу ее защитить», «моих знаний не хватает, чтобы я смогла себя защитить», «мне не хватает информации, не хочу попасть на их удочку еще раз».

На вопрос интервьюера о том, насколько участник исследования уверен в своей способности распознать и противостоять различным мошенническим

схемам уверенных ответов среди информантов было намного меньше. 8 участников исследования отвечали следующим образом: «думаю, что распознаю, но не совсем уверен», «после моего опыта я узнаю мошенника, но они придумывают новые схемы», «сложно распознать, что ты в западне», «я была уверена, что меня не проведешь, но они очень подкованы на язык». 8 информантов ответили, что их умение распознать мошенника находится на высоком уровне: «теперь я не попадусь на их уловки», «мне моих знаний итак достаточно», «я могу дать отпор и учу своих близких, как это делать». Трое участников исследования оценили свои умения в процессе противостояния мошенникам на очень высоком уровне: «что там их распознавать, звонит с незнакомого номера и представляется МВД или банком – кладу трубку и все», «мне не страшны никакие их разговоры-уговоры», «я не разговариваю с этими “липовыми” специалистами, я все про них знаю».

На вопрос «Как Вы думаете, какие психологические факторы делают людей наиболее уязвимыми к финансовому мошенничеству?» большинство информантов говорили о доверчивости и склонности к авторитету: «доверчив наш народ, привыкли уши развешивать и верить первому встречному», «многие давят на статус, свое высокое положение в обществе, ФСБ, там, МВД», «звонят и говорят, что с работы, начальство, как тут не поверить», «много лет покупали все в интернете, все было хорошо, заплатил-получил, но теперь появились сайты-подделки, сразу не разберешь, что к чему». Так же участники исследования часто упоминали в своих ответах эмоциональность: «я так обрадовалась новогодним скидкам на одном сайте, что не посмотрела отзывы и перевела деньги», «мне написали в WhatsApp, что я стала победительницей в конкурсе от одного магазина, надо было пройти по ссылке и заполнить форму, я была очень рада, потому что никогда ничего не выигрывала». Среди других ответов участники исследования упоминали код воздействия «страх»: «мне позвонили и сказали, что моя родственница попала

в беду, я испугалась, звонили с разных номеров и нужна была срочно помощь в виде денег», «по телефону сказали, что все мои деньги пропадут, если я их не переведу на застрахованный счет», «мне сказали, что меня уволят с работы, если я не сообщу сотрудникам ФСБ информацию, которую они спрашивают и других работников нашей организации в рамках официальной проверки». Так же участники исследования говорили о недостатке финансовой грамотности: «взрослым не хватает знаний, что уже говорить о пожилых, молодым проще, они все время в Интернете и больше понимают», «в наше время не было такого, этому не учили, теперь надо обучать».

Чаще всего участники исследования сталкивались с мошенничеством через фишинговые сайты при попытках покупки различных товаров и услуг (11 информантов), так же в процессе интервьюирования 7 человек указали на случаи столкновения с мошенничеством в профессиональной сфере, когда им поступил звонок по телефону или сообщение в Telegram, а потом звонок из мессенджера от якобы руководства. 6 участников исследования указали на случаи столкновения с мошенничеством в здравоохранении, но здесь надо указать, что чаще всего эти случаи пересекались с мошенничеством через фишинговые сайты, когда информанты пытались приобрести лекарственные препараты. Только трое участников исследования указали на случаи романтического обмана, когда информанты знакомились в социальных сетях и мессенджерах с людьми, с которыми продолжали переписку, и в результате общения участники исследования несли финансовые и репутационные потери.

Интересными представляются результаты на вопрос «Когда Вы или Ваши близкие, знакомые, коллеги по работе столкнулись с попыткой финансового мошенничества, удалось ли распознать его?», 18 участников исследования утвердительно ответили на данный вопрос: «конечно, я сразу поняла, что меня пытаются обмануть», «сначала я стала им отвечать, но потом прекратила переписку», «с работы по почте меня предупредили, что

мошенники могут связаться со мной, и когда мне позвонили и сообщили о важном следствии, то я положила трубку», «я смотрела передачи про мошенников и сразу поняла, что меня пытаются обмануть и украсть мои деньги». Только трое признались, что им не удалось распознать мошенников: «я поняла, что со мной что-то случилось, когда было уже поздно», «там невозможно понять, вы сами бы ничего не поняли, я была в полном ужасе», «после того, как я перевела деньги, я еще надеялась, что посылка придет, звонила по телефону и писала, но номер был все время занят, и никто не отвечал на сообщения».

На вопрос «Как Вам или Вашим близким, знакомым, коллегам по работе удалось распознать мошенников? Что подсказало, что эти люди – мошенники?» информанты чаще всего указывали на чрезмерное давление на авторитет и создание ситуации дефицита времени: «вот, это их “быстрее-быстрее”, “надо делать срочно”, меня и смутило», «по телевизору говорили, что мошенники представляются сотрудниками банков и МВД, а они никогда по телефону разговаривать не будут, поэтому я и положила трубку», «они говорят никому не сообщать, секретно, по закону меня могут наказать за то, что я кому-то расскажу, а меня коллеги по работе предупредили, что это уже обман». Среди других паттернов-подсказок участники исследования отмечали речь собеседника: «мне странным показался акцент и гэканье», «я стала задавать много вопросов, и тогда звонящий стал ругаться, изменился тон голоса». Так же участники исследования говорили о недочетах в оформлении сайта: «не всегда открывалась картинка на сайте», «оплата была не через сайт, а через ссылку в WhatsApp», «звонили потом по номеру телефона, который был указан на сайте, а он не работает».

В результате проведенного исследования авторы сделали вывод, что информанты высоко оценивают уровень своих знаний о финансовом мошенничестве и методах защиты от него, при этом уровень уверенности в

том, что они могут распознать и противостоять различным мошенническим схемам был намного меньше. Доминирующими психологическими факторами, которые делают людей наиболее уязвимыми к финансовому мошенничеству, были названы доверчивость и склонность к авторитету, эмоциональность, страх и недостаточный уровень знаний по вопросам финансовой грамотности. Основными видами мошенничества, с которыми столкнулись участники исследования, были названы фишинговые сайты, мошенничество с трудоустройством, мошенничество в сфере здравоохранения, романтическое мошенничество. Подавляющее большинство участников исследования сказали, что при столкновении с попыткой финансового мошенничества им удалось его распознать. Данный вывод представляется интересным и перекликается с результатами исследования Whitty M., в котором автор говорит о том, что жертвы кибермошенников верили, что они контролируют исход событий [7; 13], а также с выводами Parti K. и Tahir F. о том, что жертвы испытывают когнитивный диссонанс и отрицают виктимизацию [10]. Основными паттернами-подсказчиками для участников исследования в том, что они, их близкие или коллеги по работе столкнулись с мошенником, выступили чрезмерное давление на авторитет, создание ситуации дефицита времени, особенности речи собеседника, ошибки в оформлении сайта. Конечно, авторы признают ограничения исследования, которые выражаются в отсутствии разграничения информантов на тех, кто лично перенес ситуацию столкновения с мошенниками и тех, у кого близкие, знакомые или коллеги по работе стали жертвами кибермошенников, но это ограничение было связано с тем, что тема кибермошенничества, по-прежнему, остается табуированной и сложной для обсуждения для жертв злоумышленников. В перспективе авторы планируют провести серию интервью с экспертами в области банковского и инвестиционного сектора с целью разработки практических инструментов, которые помогут гражданам

Российской Федерации эффективно и в кратчайшие сроки распознавать мошеннические схемы и им противостоять.

Библиографический список:

1. Akhtar N., Kerim B., Perwej Y., Tiwari A., Praveen S. A comprehensive overview of privacy and data security for cloud storage // International Journal of Scientific Research in Science Engineering and Technology. - 2021. – Т. 8. – №. 5. – С. 113-152 p.
2. Asiama A.A., Zhong H. Victims rational decision: A theoretical and empirical explanation of dark figures in crime statistics // Cogent Social Sciences. – 2022. – Т. 8. – №. 1. – С. 1-15
3. Bergmann M.C., Dreißigacker A., von Skarczinski B., Wollinger G.R. Cyber-dependent crime victimization: the same risk for everyone? // Cyberpsychology, Behavior, and Social Networking. - 2018. - Т. 21. - № 2. С. 84-90.
4. Burnes D., Henderson Jr. C.R., Sheppard C., Zhao R., Pillemer K., Lachs M.S. Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis // American journal of public health. – 2017. – Т. 107. – №. 8. – С. e13-e21.
5. Darwish A., El Zarka A., Akoul F. Towards understanding phishing victims' profile // International Conference on Computer Systems and Industrial Informatics. - IEEE, 2012. – С. 1-5.
6. Fischer P., Lea S.E.G., Evans K.M. Why do individuals respond to fraudulent scam communi- cation and lose money? The psychological determinants of scam compliance // Journal of Applied Social Psychology. - 2013. Т. 43. - № 10. – С. 2060–2072.
7. Halevi T., Lewis J., Memon N. Phishing, personality traits and Facebook //arXiv preprint arXiv:1301.7643. – 2013.

8. Holtfreter K., Reisig M.D., Pratt T.C. Low self-control, routine activities, and fraud victimization. Criminology. - 2008. – Т. 46. - № 1. – С. 189–220.
9. Holtfreter K., Reisig M.D., Mears D.P., Wolfe S.E. Financial exploitation of the elderly in a consumer context. - US Department of Justice, Office of Justice Programs, National Institute of Justice, 2014.
10. Parti K., Tahir F. “If We Don’t Listen to Them, We Make Them Lose More than Money:” Exploring Reasons for Underreporting and the Needs of Older Scam Victims // Social Sciences. – 2023. – Т. 12. – № 5. – С. 264
11. Ross M., Grossmann I., Schryer, E. Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud // Perspectives on Psychological Science. - 2014. – Т. 9. - № 4. – С. 427-442.
12. Titus R.M., Gover A.R. Personal fraud: The victims and the scams // Crime Prevention Studies. - 2001. – Т. 12. – С. 133–151.
13. Whitty M.T. Is there a scam for everyone? Psychologically profiling cyberscam victims // European Journal on Criminal Policy and Research. – 2020. – Т. 26. – №. 3. – С. 399-409.
14. Whitty M.T., Buchanan T. The online dating romance scam: a serious crime // Cyberpsychology. Behavior, and Social Networking. - 2012. – Т. 15. – С. 181–183.
15. Whitty M.T., Joinson A.N. Truth, lies, and trust on internet. London: Routledge, Psychology Press, 2008. – 184 с.

Оригинальность 75%