УДК 32:159.9

Н.Р. Красовская, А.А. Гуляев

К ВОПРОСУ О КИБЕРМОШЕННИЧЕСТВЕ

Кибермошенничество – сравнительно новый феномен, представляющий собой активные действия в онлайн-формате с целью получения выгоды посредством манипуляций сознанием человека. Кибермошенничество появилось и развивается в Интернет-пространстве. Современная информационная эпоха с приходом в мир пандемии обусловила распространение манипуляций сознанием людей в беспрецедентных масштабах. В Интернет-пространстве кибермошенничество связано с похищением и использованием личных данных человека для совершения экономических преступлений, а также используется и в других сферах – политике, рекламе.

Ключевые слова: когнитивный хакинг, фишинг, спуфинг, когнитивное искажение, социальная инженерия, кибермошенничество, манипуляция

DOI: 10.35634/2587-9030-2022-6-1-133-138

Ссылка на статью:
Красовская Н.Р., Гуляев А.А. К вопросу о кибермошенничестве // Вестн. Удм. ун-та. Социология. Политология. Международные отношения. 2022. Т. 6, вып. 1. С. 133–138. https://doi.org/10.35634/2587-9030-2022-6-1-133-138

Введение

О значимости киберпространства как среды, имеющей специфические эффективные инструменты влияния на все сферы жизни, в том числе политику, рекламу, экономику, международные отношения, в последнее время говорится все чаще. Особую роль в этом сыграл 2020 год, отмеченный ситуацией пандемии и небывалых по масштабу и последствиям ограничений и изменений.

Сегодня киберпространство – неотъемлемая часть и факт повседневной жизни; огромное количество действий совершается в виртуальном формате. Все более острой проблемой в складывающихся условиях становится кибербезопасность. Угрозы сохранности информации в интернете, шпионажа, саботажа и мошенничества растут вместе с активизацией этого сектора. Наблюдаемый в киберпространстве прогрессирующий рост самых разных нарушений, злоупотреблений, преступлений определяется тем, что идентичность и границы здесь размыты, становится легче скрыть личность и источник нападения и проще передать ложную информацию.

Мошенничество по определению Уголовного кодекса Российской Федерации – это хищение чужого имущества, приобретение права на чужое имущество путем обмана или злоупотребления доверием. Мошенники – категория преступников, нацеленных на завладение чужим имуществом обманным путем, не прибегая к использованию открытого насилия и угроз. Их даже называют «элитой» криминального мира, так как основные средства их преступных деяний – хитрость, находчивость и изобретательность, а не непосредственное насилие и агрессия [9].

В современной России мошенничество – одно из самых часто совершаемых преступлений; чаще происходят только кражи. За время действия ограничений, связанных с эпидемией коронавируса, краж стало меньше на 9 %, в то время как случаи мошенничества увеличились на 36 %.

Рост произошел исключительно за счет телефонного и Интернет-мошенничества. По сравнению с первым полугодием 2019 года, в 2020 году число случаев такого мошенничества увеличилось на 76 %. При этом раскрываемость таких преступлений составляет не более 23 % [7].

Кибермошенники (отдельные личности или группы киберпреступников) используют различные способы, стратегии, возможности информационных технологий и Интернет в преступных целях. В их числе информационно-психологическое воздействие, дозирование (сокрытие) информации, распространение среди пользователей социальных сетей слухов, паники, введение в заблуждение. Целенаправленное планирование ситуации информационно-психологического шока у отдельного человека или большой группы людей создает благоприятные условия влияния на поведение потенциальной жертвы.

Исследователи и эксперты отмечают, что изначально тема киберпреступлений стала актуальной на фоне бурного роста популярности соцсетей. Ситуация пандемии и вынужденной физической изоляции основной части населения создала благоприятные условия, провоцирующие её рост [3].

Фишинг

Обзор данных открытых источников по проблеме показывает, что в 2020 году пользователи Интернета, как компании, так и граждане, нередко сами сообщали мошенникам свои личные данные, в том числе давая доступ к своим счетам. Фишинг – способ Интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей. Для этого проводится, например, массовая рассылка электронных писем от имени популярных брендов, а также личных сообщений посредством различных сервисов, прежде всего от имени банков, в том числе через социальные сети (например, Фейсбук, Инстаграм). В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить пользователя ввести на этой странице свой логин и пароль, которые он обычно использует для доступа, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам [5].

Фишинг относится к технологиям из сферы социальной инженерии. Он опирается на факт незнания пользователем основ информационной безопасности. Реальные сервисы не рассылают письма с просьбами сообщить свои личные данные; такие письма и сообщения приходят только от кибермошенников. В практике кибермошенников есть и другие приемы, например, в сообщениях в социальных сетях они могут попросить помочь сохранить их денежные средства (якобы у них трудные обстоятельства) посредством перевода на банковскую карту потенциальной жертвы, чтобы потом часть средств осталась у пользователя в качестве вознаграждения за помощь. Злоумышленники подыскивают самыми разные, правдоподобные на первый взгляд причины, по которым они вознамерились перевести на банковскую карту объекта манипуляции денежные средства. Например, объекту сообщают, что он является однофамильцем умершего богатого человека, не имевшего наследников. Далее предлагают представиться его родственником и получить наследство, позже разделив его с автором сообщения. Автор письма, потенциальный кибермошенник, может объяснить свои действия тем, что он является сотрудником банка, где хранятся депозиты умершего однофамильца, не имевшего наследников. Этот «сотрудник» переживает, что депозиты достанутся руководству банка, поэтому за помощью обращается к потенциальной жертве. Цель всех этих рассылок и сообщений – узнать данные банковской карты или счета, которыми можно воспользоваться для снятия денежных средств с карты или счета потенциальной жертвы кибермошенничества [4]. Как следует из источников МВД, в 2020 году в России зарегистрировано 510,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Это на 73,4 % больше по сравнению с 2019 годом. Число преступлений с пластиковыми картами выросло более чем в 5 раз [8].

Новые схемы телефонного мошенничества в России появляются чуть ли не еженедельно. В большинстве из них мошенники наживаются за счет доверчивости граждан, однако появляются и такие схемы, при которых удается обмануть даже тех, кто привык проверять входящие номера [2].

По данным наблюдений Webroot за 2019 год, фишинг стал более персонализированным: злоумышленники, могут отслеживать при помощи специальных программ деятельность конкретного пользователя в Интернете, предлагая актуальную для него информацию, например, о распродаже вместе со ссылкой и адресом, похожим на реальный сайт магазина. Как отмечает Ironscales, почти четверть вредоносных электронных писем теперь содержит ссылки на фишинговые сайты. Тенденция продолжилась, и в июле 2020 года был поставлен рекорд по фишингу среди клиентов российских банков [3]. Кибермошенники используют определенные эволюционные особенности нашего мозга, которые связаны с когнитивными искажениями [9]. Когнитивные искажения – это ошибки в восприятии и мышлении, обусловленные наличием субъективных предубеждений и стереотипов, социальных, моральных и эмоциональных причин, сбоями в обработке и анализе информации, физическими ограничениями и особенностями строения человеческого мозга. Всего насчитывают более 200 когнитивных искажений.

Когнитивные искажения

В данное время достаточно часто встречаются такие когнитивные искажения, как «нулевой риск» и эффект «плохих новостей». В силу эволюционных причин, люди больше прислушиваются к плохим новостям, чем к хорошим, и стремятся к минимальному риску для собственного здоровья и благополучия, что дает основу для действий кибермошенников. Когнитивные искажения использу-

ются не только при кибермошенничестве, но также и при осуществлении информационных атак с целью нагнетания социального напряжения в обществе. Плохие новости мы бессознательно считаем более достоверными. Отсюда недоверие к официальным СМИ, которые пытаются донести положительную информацию, и активное распространение негативной информацией, когда пользователи становятся добровольными акторами информационных войн.

Возникновение когнитивных искажений связано с ограниченным использованием возможностей мозга человека, с тем, что человек сосредотачивается лишь на одном аспекте сложной проблемы и оказывается не в состоянии трезво оценить эту проблему как целое. В обычных условиях механизм принятия решения снижает уровень тревоги, экономит время, ресурсы и позволяет человеку начать действовать: эволюционном плане от быстроты реакции человека на ситуацию зависело его выживание. При недостаточном количестве информации, как правило, возникает эмоциональное напряжение. Это состояние человека сильно затрудняет принятие взвешенных решений, становясь причиной скоропалительных действий, что также относится к числу когнитивных искажений. В современном мире на нас обрушивается очень много информации, с которой мозгу трудно справляться. Механизм отсекания лишнего – для увеличения скорости или для снижения нагрузки – один из приемлемых выходов для мозга. В результате наше восприятие действительности подогнано под некие шаблоны, алгоритмизировано. Это может стать причиной ошибок в итоговых суждениях, обусловленных неизбежными когнитивными искажениями.

«Когнитивный хакинг»

«Взлом сознания» или «когнитивный хакинг» получил широкое распространение в рамках непрерывно ведущихся на разных уровнях современных информационных войн. «Когнитивный хакинг» – понятие, которым обозначают вредоносные действия, нацеленные на манипулирование восприятием и мышлением. Когнитивные уловки (в сфере познавательной активности) помогают создавать и использовать специфические состояния психики, при которых контроль снижается, а степень податливости воздействию извне, наоборот, увеличивается. Например, часто встречается психологический прием «слепота внимания», при котором избыточное количество деталей, к примеру, сообщения о распродаже, предупреждения о якобы несанкционированном переводе средств или краже данных, способствует тому, чтобы человек не заметил главного – поддельного адреса в ссылке, который может отличаться всего на один знак от реального [3].

Методы когнитивного хакинга применяют не только киберпреступники, но и недобросовестные корпорации, рекламодатели, политики, СМИ при помощи кампаний по дезинформации или распространению на Интернет-платформах контента, меняющего восприятие действительности пользователями. В последнее время все больше специалистов в области IT-безопасности и психологии обращает внимание на растущее число случаев, когда злоумышленники успешно обходят технические способы защиты в киберпространстве, используя психологические манипуляции. Цель таких атак – изменение человеческого поведения или отношения к каким-то явлениям или действиям; часто они совершаются при помощи распространения дезинформации или подтасовки фактов.

Спуфинг

Широкое распространение в современном киберпространстве получила еще одна форма социальной манипуляции – спуфинг. При спуфинге вредоносная программа маскируется под легальную и, таким образом, получает у потребителя данные его банковских карт, счетов, значимой информации либо напрямую запрашивая их, либо скрыто извлекая их из приложений на смартфоне. Описан серьезный и показательный случай спуфинга в области политики, когда Джон Подеста, сотрудник избирательного штаба Хиллари Клинтон, в марте 2016 года поддался на поддельное уведомление о нарушении безопасности якобы от Google. Введя свои учетные данные на фейковой странице, он собственноручно открыл злоумышленникам доступ к секретным данным [3].

Случаи активного использования этой технологии наблюдаются и в нашей стране. По данным специалистов Центра реагирования на инциденты кибербезопасности CERT-GIB, в августе 2020 кибератакам с использованием спуфинга (подмены адреса) электронной почты подверглись три крупные благотворительные организации. От лица руководителей благотворительных фондов злоумышленники отправляли поддельные письма их коллегам, например, из финансового отдела, с просьбой

срочно оплатить лечение кого-то из подопечных организации. В частности, сотрудникам Фонда Хабенского пришло письмо от хакеров, в котором директор якобы просил немедленно осуществить перевод средств, собранных для одного из подопечных фонда, на указанные реквизиты [6].

Заключение

Специалист по кибербезопасности американско-израильской компании Ironscales, вице-президент Иэн Бакстер отмечает, что в настоящее время значительно чаще, чем прежде, злоумышленники при кибератаках опираются на психологические закономерности поведения пользователей. Только понимая, как именно злоумышленники дурачат «объект» своего корыстного интереса, специалисты могут ликвидировать пробелы в системах безопасности и снижать риски обмана [3].

Огромное значение для предотвращения случаев кибермошенничества также имеет социальная активность в затруднительной ситуации. Как правило, киберпреступникам удается обмануть потенциальную жертву, когда она изолирована от других в силу разных причин. Если у человека блокирована возможность получить квалифицированный совет, помощь других людей, то киберпреступникам удается направлять действия жертвы, достигая нужной цели. Основным способом профилактики киберпреступлений является информирование населения всех возрастов с помощью различных каналов о видах преступных ситуаций, особенностях их развития, поведении мошенников. Важно показать, что при попытках злоумышленников получить значимую личную информацию целесообразно придерживаться следующих способов преодоления манипуляции: необходимо остановиться, сделать паузу, осмотреться, не совершать скоропалительных действий, найти возможность прояснить, уточнить ситуацию, посоветоваться с другими людьми. Эти шаги могут предотвратить совершение кибермошенничества.

По данным статистики в сфере Интернет-преступности, Россия стала одним из лидеров по числу кибератак. За ней следуют США, Китай и Индия) [1].

В целом, тенденция роста киберпреступлений и кибермошенничества прослеживается и в мировой практике. Анализ современного состояния киберпреступности фиксирует её устойчивый рост, требуя адекватной реакции общества.

Опыт общения, навыки восприятия и анализа информации на предмет доверия легче формируются у молодежной аудитории. Тем не менее важно включить информацию о кибербезопасности в школьный курс «Основы безопасности жизнедеятельности». У активных пользователей социальных сетей накапливается умение понимать, исходит информация из заслуживающего доверия источника или нет. Люди старших возрастных категорий, как правило, менее осведомлены об изменениях и новшествах, что делает их более уязвимыми для мошенников. Войдя в доверие к будущей жертве, застав ее врасплох, киберпреступники успешно достигают корыстных целей, лишают потерпевших денежных средств и собственности. Масштабы материального ущерба при этом более чем впечатляют. Психологический ущерб непосредственно оценить невозможно. Поэтому подготовка к жизни с широким применением Интернет-ресурсов должна найти свое отражение на всех доступных уровнях, для всех возрастных категорий. Сегодня для России кибермошенничество становится одним из самых заметных вызовов, что делает задачу борьбы с этой угрозой в современном обществе все более значимой.

СПИСОК ЛИТЕРАТУРЫ

1. Kiberprestupleniya – problema 21 veka. Mezhdunarodnaya Akademiya issledovaniya lzhi. – URL: https://blog.studylie.ru/kiberprestuplenija-problema-21-veka/ (accessed: 10.10.2019).
2. Klon v telefone: moshenniki zvonyat s nomerov gosorganov i bankov // Izvestiya. – URL: https://iz.ru/1118164/marta-litvinova/klon-na-telefone-moshenniki-zvoniat-s-nomerov-gosorganov-i-bankov?utm_source=mail_json (accessed: 02.02.2021).
3. Kognitivnyy khaking vykhodit na tropu kibervoyny // Kommersant'. – URL: https://www.kommersant.ru/doc/447364130 (accessed: 08. 02. 2020).
4. Serieva, M. M. Kiberprestupnost' kak novaya kriminal'naya ugroza / M. M. Serieva // Novyy yuridicheskiy vestnik. – 2017. – № 1 (1). – S. 104–106. – URL: https://moluch.ru/th/9/archive/66/2365/ (accessed: 26.01.2021).
5. Tokaeva, Yu. V. Osnovnye skhemy sovershеniya kibermoshennichestva i vozmozhnosti protivodeystviya so storony vnutrennego kontrolya / Yu. V. Tokaeva, T. P. Krivetskaya // Uchetno-analiticheskoe obespechenie – informatsionnaya osnova ekonomicheskoy bezopasnosti khozyaystvuyushchikh sub"ektov: mezhvuz. sb. nauchnykh tr. i re-zul'tatov sovmestnykh nauchno-issledovatel'skikh proektov: v 2-kh chastyakh. – Moskva, 2017. – S. 365–369.

6. Chernousov, I. Spetsialisty fiksiruyut rost moshennichestva v adres blagotvoritel'nykh fondov / I. Cherno-usov // Rossiyskaya gazeta. – 2020. – URL: https://rg.ru/2020/08/19/specialisty-fiksiruiut-rost-kiberatak-na-blagotvoritelnye-organizacii.html (accessed: 02.02.2021).
7. Chislo del o moshennichestve rekordno vyroslo na fone pandemii. – URL: https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d (accessed: 02.02.2021).
8. Chislo prestupleniy s plastikovymi kartami v Rossii vyroslo // Izvestiya. – 2021. – URL: https://news.mail.ru/incident/45082201/?frommail=1 (accessed: 02.02.2021).
9. Yurochkin, N. S. Kibermoshennichestvo: kharakteristika, priemy i metody ego sovershenniya / N. S. Yurochkin // Tavricheskiy nauchnyy obozrevatel'. – 2016. – № 12 (17), ch. 2. – S. 124–128.

Поступила в редакцию 27.05.2021

Красовская Наталия Рудольфовна, кандидат психологических наук,
доцент кафедры социальной психологии и виктимологии
ФГБОУ ВО «Новосибирский государственный педагогический университет»
630126, Россия, г. Новосибирск, ул. Вилюйская, 28
E-mail: krasovskaya.mcm@gmail.com

Гуляев Андрей Анатольевич, кандидат философских наук
АНО Центр народной дипломатии
125009, Россия, г. Москва, Георгиевский пер., 1 (стр. 1)
E-mail: andrey.gulyaev1966@yandex.ru

N.R. Krasovskaya, A.A. Gulyaev
ON THE ISSUE OF CYBER FRAUD

DOI: 10.35634/2587-9030-2022-6-1-133-138

Cyber fraud is a relatively new phenomenon, which is an active action in the Internet in order to obtain benefits through the manipulation of human consciousness. Cyber fraud has appeared and is developing in the Internet space. The modern information age, with the advent of the pandemic in the world, has caused the spread of cyber fraud and manipulation of people's minds on an unprecedented scale. In the Internet space, cyber fraud is associated not only with the theft and use of personal data of a person for committing economic crimes, but is also used in other areas – politics, advertising.

Keywords: cognitive hacking, phishing, spoofing, cognitive distortion, social engineering, cyber fraud, manipulation.

REFERENCES

1. Kiberprestupleniya – problema 21 veka [Cybercrime – the problem of the XXI century]. Mezhdunarodnaya akademiya issledovaniya lzhi 10.10.2019. [Ehlektronnyj resurs]. – Rezhim dostupa: https://blog.studylie.ru/kiberprestuplenija-problema-21-veka/
2. Klon v telefone: moshenniki zvonyat s nomerov gosorganov i bankov [Clone in the phone: scammers call from numbers of government agencies and banks] // Izvestiya 02.02.2021. [Elektronnyj resurs]. – Rezhim dostupa: https://iz.ru/1118164/marta-litvinova/klon-na-telefone-moshenniki-zvoniat-s-nomerov-gosorganov-i-bankov
3. Kognitivnyj haking vyhodit na tropu kibervojny [Cognitive hacking enters the path of cyber warfare] // "Kommersant" ot 30.08.2020. [Elektronnyj resurs]. – Rezhim dostupa: https://www.kommersant.ru/doc/4473641
4. Serieva M.M. Kiberprestupnost' kak novaya kriminal'naya ugroza [Cybercrime as a new criminal threat] // Novyj yuridicheskij vestnik. 2017. № 1 (1). S. 104-106. URL: https://moluch.ru/th/9/archive/66/2365/
5. Tokaeva Yu.V., Kriveckaya T.P. Osnovnye skhemy sovershenniya kibermoshennichestva i vozmozhnosti protivodejstviya so storony vnutrennego kontrolya [The main schemes of cyberbullying and the possibility of counteraction by internal control] // Uchetno-analiticheskoe obespechenie - informacionnaya osnova ekonomicheskoj bezopasnosti hozyajstvuyushchih sub"ektov. Mezhvuzovskij sbornik nauchnyh trudov i rezul'tatov sovmestnyh nauchno-issledovatel'skih proektov: v 2-h chastyah. Moskva, 2017. S. 365 – 369.
6. Chernousov I. Specialisty fiksiruyut rost moshennichestva v adres blagotvoritel'nyh fondov [Experts record an increase in fraud against charitable foundations] // Rossijskaya gazeta 19.08.2020. [Elektronnyj resurs]. – Rezhim dostupa: https://rg.ru/2020/08/19/specialisty-fiksiruiut-rost-kiberatak-na-blagotvoritelnye-organizacii.html
7. Chislo del o moshennichestve rekordno vyroslo na fone pandemii [The number of fraud cases has grown record high amid the pandemic] // RBK 31.08.2021. [Elektronnyj resurs]. – Rezhim dostupa: https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d

8. Chislo prestuplenij s plastikovymi kartami v Rossii vyroslo v 5,5 raza [The number of crimes with plastic cards in Russia has increased 5.5 times] // Izvestiya 01.02.2021. [Elektronnyj resurs]. – Rezhim dostupa: https://news.mail.ru/incident/45082201/
9. Yurochkin N.S. Kibermoshennichestvo: harakteristika, priemy i metody ego sovershenіya [Cyber fraud: characteristics, techniques and methods of its commission] // Tavricheskij nauchnyj obozrevatel'. 2016. № 12 (17). Chast' 2. S. 124–128.

For citation:
Krasovskaya N.R., Gulyaev A.A. On the issue of cyber fraud // Bulletin of Udmurt University. Sociology. Political Science. International Relations. 2022. Vol. 6, iss. 1. P. 133–138. https://doi.org/10.35634/2587-9030-2022-6-1-133-138 (In Russ.).

Received 27.05.2021

Krasovskaya N.R., Candidate of Psychology, Associate Professor
at Department of Social Psychology and Victimology
Novosibirsk State Pedagogical University
Vilyuiskaya st., 28, Novosibirsk, Russia, 630126
E-mail: krasovskaya.mcm@gmail.com

Gulyaev Andrey Anatolyevich, Candidate of Philosophy
Center for People's Diplomacy
Georgievsky lane, 1/1, Moscow, Russia, 125009
E-mail: andrey.gulyaev1966@yandex.ru