УДК 336.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ И КИБЕРМОШЕННИЧЕСТВО: ТРЕНДЫ, СХЕМЫ И СПОСОБЫ БОРЬБЫ

Анненкова Екатерина Александровна, к.э.н., доцент
Саратовская государственная юридическая академия
Annenkova Ekaterina Aleksandrovna, PhD, Associate Professor
Saratov State Law Academy, gea555@mail.ru

Аннотация. В статье рассматриваются вопросы социальной инженерии: понятие, характерные элементы. Анализируются основные схемы кибермошенничесв: телефонное, фишинг. Отмечается активное применение дипфейк-технологий. Кроме того, приводятся примеры способов борьбы с кибермошенничесвтом.

Ключевые слова: кибермошенничество, киберпреступления, дропперство, фишинг, социальная инженерия

Одним из самых распространенных инструментов злоумышленников на сегодняшний момент остается социальная инженерия. По сути она представляет собой психологическое манипулирование жертвой с целью совершить определенные действия в интересах мошенника для хищения личных или финансовых данных. Причем, на уловки мошенников попадаются как физические, так и юридические лица.

По данным Банка России несмотря на снижение киберперступлений в 2025 г. по сравнению с 2024 г. на 18%, выросли суммы. Все чаще стали совершаться преступления в данной области на крупные суммы. Всего за девять месяцев 2025 г. кибермошенники похитили 6,9 млрд. руб. [1].

Злоумышленники маскируют свои сценарии под актуальную новостную ленту. Например, когда актуальной новостью было распространение короновирусной инфекции, то мошенники всячески использовали ее. С 2023 г. стали использовать тему специальной военной операции. Есть темы, которые повторяются ежегодно. Это может быть сдача налоговой декларации, оповещения от службы судебных приставов под новогодние праздники, начало учебного года и т.д.

Телефоны остаются одним из основных инструментов в мошеннических схемах. С помощью них мошенники путем психологического давления или манипулирования выманивают личную или финансовую информацию, либо заставляют владельца, например, банковской карты, самостоятельно перевести денежные средства злоумышленникам.

В качестве основных критериев социальной инженерии нами были выделены следующие:

1) обман или злоупотребление доверием. Мошенники могут представиться сотрудником правоохранительных органов или представителем банка;

2) психологическое давление, которое может проявляться двояко. С одной стороны, они могут угрожать, запугивать, торопить, не давать связаться с родственниками и выйти из-под их контроля. С другой стороны, могут ввести в состояние эйфории;

3) манипулирование.

Стоит отметить, что мошенники следят за изменениями не только в банковской сфере, но и изучают новейшие разработки в области техники и технологиях. В последнее время стали активно использовать дипфейк-технологии. С помощью нейросети мошенники создают реалистичное изображение, образ человека и рассылают его друзьям, коллегам и родственникам через мессенджеры или социальные сети. Нередки случаи, когда от имени знаменитого блогера рассылают видео, в котором герой с голосом, не отличимым от оригинала, рассказывает историю о том, как с ним что-то случилось, и он просит о помощи. Для создания видео мошенники используют фото и видео из открытых источников, которые они получают путем взлома его социальных сетей или мессенджеров. Однако, дипфейки не лишены недостатков. Так, их характеризует:

1) монотонная речь;

2) дефекты звука и видео;

3) несвойственная мимика.

Добиться успеха мошенникам помогают следующие факторы:

1) эффект неожиданности. Как правило, жертвы мошенников теряются, когда им, например, звонит человек и представляется сотрудником правоохранительных органов. Играет важное значение и время, когда мошенники звонят. К примеру, ранним утром и поздним вечером любой человек наиболее уязвим и не может быстро и здраво принимать решения;

2) сильные эмоции. Особенно ярко они проявляются, когда речь заходит о близких родственниках. Используются не только негативные эмоции (страх, стыд, паника), но и положительные (радость, надежда, доверие). Например, после слов «Вам положена социальная выплата…» или «Вы выиграли…» наступает радость и надежда на получение денежных средств. Таким образом мошенники активизируют базовые эмоции и используют быструю необдуманную реакцию жертвы. При этом главной задачей является вывести человека из состояния равновесия и отключить критическое мышление;

3) психологическое давление и создание паники;

4) актуальность темы.

Еще одним инструментом, в котором активно применяются методы социальной инженерии, является фишинг. Мошенники имитируют сайты известных компаний. Помимо сбора личной или финансовой информации, с помощью фишинговых сайтов, так осуществляется взлом, к примеру портала госуслуги. Внешне такие сайты практически ничем не отличаются от оригинала. В качестве признаков, которые отличают фишинговый сайт от официального, можно выделить следующие:

1) дополнительные символы или буквы в адресной строке. Например, вместо gosuslugi.ru используется gosuslugis.ru;

2) отсутствие обозначение «закрытого замка» или протокола https;

3) в тексте присутствуют орфографические ошибки;

4) дизайн сайта отличается, например, по цветовой гамме;
5) предложение скачать какой-либо файл или установить программу.

Самыми популярными схемами являются:

1) интернет-магазины и аукционы;
2) онлайн-опросы и конкурсы;
3) восстановление положительной кредитной истории;
4) предложения о работе с высоким доходом;
5) кредиты на очень выгодных условиях;
6) различные сборы на лечение детей, животных, пожертвования;
7) инвестиции с высокой доходностью.

Распространенным заблуждением является точка зрения о том, что жертвами мошенников становятся лишь пожилые доверчивые люди. Ими может стать любой человек, независимо от возраста и уровня образования. Ежегодно Банк России проводит социологические опросы населения об уровне удовлетворенности оказанных финансово-кредитными организациями услуг. Каждый третий из опрошенных так или иначе сталкивался с кибермошенничеством. 9% всех респондентов не только стали жертвами, но и лишились своих денежных средств. По итогам хищения денежных средств чаще всего обращаются в обслуживающий банк (42,8% опрошенных), в полицию (30%), никуда не обращаются (18,3%) и в иные организации: Банк России, Роспотребнадзор и др. (8,9%). По сравнению с предыдущим годом число обращений в банк увеличилось на 9%, в полицию – 2%, одновременно в банк и полицию – на 10% (34% опрошенных) [1]. На 4 % сократилось число тех, кто никуда не обратился. Среди них граждане, у кого сумма похищенных денежных средств составила менее 20 тыс. руб. На основании такого масштабного исследования составляется портрет пострадавшего. Так, по итогам 2024 г. чаще всего жертвами кибермошенников становились работающие женщины со средним уровнем дохода в возрасте от 25 до 44 лет, проживающие в городе. В особой группе риска экономически активные граждане, которые часто используют платежные сервисы, в том числе с применением новейших технологий.

Наиболее острой проблемой кибермошенничества сегодня является вовлечение в дропперство. Чаще всего в качестве дропперов используются школьники или студенты, люди, приехавшие учиться или работать из небольших населенных пунктов, люди с тяжелым материальным положением (например, имеющие много кредитов), а также уязвимые слои населения (сироты, пенсионеры, безработные и т.д.). По сути дропы выступают в качестве посредников, которые помогают кибермошенникам вывести денежные средства с помощью своей банковской карты. Они становятся соучастниками преступления. Поскольку найти кибермошенников достаточно проблематично, то всю ответственность за совершенное преступление понесет дроп. Он по указанию злоумышленника переводит денежные средства, осуществляет операции с помощью банкомата или платежного терминала, либо оформляет на себя банковские карты и передает их мошенникам.

В качестве основных трендов в кибермошенничестве следует выделить:

1) переход в мессенджеры и социальные сети;
2) уход от непродуманных звонков к тщательно подготовленным атакам;
3) использование современных технических средств. В 2025 г. ключевым инструментом стало использование искусственного интеллекта, автоматизированного фишинга и дипфейк-технологий.

4) рассылка и внедрение вредоносного программного обеспечения. Основными каналами являются фишинговые письма, смс и мессенджеры, QR коды, поддельные объявления об обновлении программного обеспечения. Таким образом кибермошенники комбинируют социальную инженерию и технические уловки;

5) целевые атаки на участников специальной военной операции и несовершеннолетних. Атаки стали все чаще носить персонифицированный характер

В 2024 г. Банк России разработал рекомендации по усилению кредитными организациями информационной работы с клиентами в целях противодействия:

1) осуществлению переводов денежных средств бех добровольного согласия клиентов;

2) заключению договоров по получению кредитных (заемных) средств под влиянием обмана и осуществлению операций с использованием указанных денежных средств (кредитный фрод);

3) вовлечению граждан в деятельность по выводу и обналичиванию средств, полученных преступным путем (дропперство).

В целях борьбы с кибермошенничествами вводятся ограничения на 2 суток по переводам, если есть подозрения на мошеннические операции, либо счет, на который переводят денежные средства содержится в базе данных Банка России в разрезе мошеннических операций. По кредитам с 1 сентября 2025 г. начал действовать период охлаждения. Так, по операциям на сумму от 50 до 200 тыс. руб. вводится период охлаждения на 2 часа. Этого времени достаточно, чтобы человек смог прийти в себя, совладать со своими эмоциями и принять взвешенное и осознанное решение о целесообразности взятия кредита. Для кредитов свыше 200 тыс. руб. период охлаждения составит 2 суток. Эти меры направлены на то, чтобы человек успел спокойно всё обдумать и отменить заявку до получения средств, ничем не рискуя. Ранее с 1 марта 2025 г. каждый желающий может установить самозапрет на выдачу кредитов как дистанционно, так и очно. Он распространяется на самые распространенные виды кредитов: потребительские в банках и микрозаймы в микрофинансовых организациях. Заметим, что есть варианты самозапрета: полный и частичный. Так, при первом запрещена выдача кредита любым способом, а при втором – только, к примеру, онлайн.

Также для борьбы с кибермошенничеством используются антифрод-системы, криптографические алгоритмы, технологии типа SmartVista и 3D Secure, двухфакторные аутентификации, отключение доступа к дистанционному обслуживанию. Последнее применяется в отношении тех клиентов, которые занимаются выводом и обналичиванием похищенных денег.

Таким образом, кибермошенничество в современной банковской системе России актуальной проблемой. Ежегодно жертвами мошенников становятся разные категории как физических и юридических лиц.

Список использованных источников

1. Банк России: Официальный сайт [Электронный ресурс] / Банк России, 2000-2025. Электрон. дан. URL: http://www.cbr.ru (дата обращения: 28.10.2025).