УДК 34 **Юридические науки**

Стулина Екатерина Александровна, *студентка 2 курса магистратуры*
Московский университет Министерства внутренних дел Российской Федерации им В. Я. Кикотя

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ФИШИНГОВЫХ МЕТОДОВ

Аннотация: данное исследование затрагивает фишинг — как один из распространенных методов интернет-мошенничества. Актуальность статьи обусловлена дальнейшим развитием цифровых технологий, в частности, в сфере информационных платежей, упрощающих ведение расчетно-хозяйственной деятельности государственных органов, коммерческих организаций и частных лиц.

Ключевые слова: фишинг, мошенничество, софт.

Abstract: This study addresses phishing as one of the most common methods of online fraud. The relevance of the article is due to the further development of digital technologies, in particular, in the field of information payments, which simplify the conduct of settlement and economic activities of government agencies, commercial organizations and individuals.

Key words: phishing, fraud, software.

Сопутствующим эффектом дальнейшего развития цифровых технологий помимо расширения возможностей производства и коммуникации является расширение возможностей для совершения преступлений мошеннического характера, что особенно заметно в коммерческой сфере, а также в сфере оборота личных финансовых средств граждан. Развитие цифровых технологий значительно расширяет арсенал злоумышленников. Одним из распространённых

способов ведения незаконной преступной деятельности выступает мошенничество посредством так называемого фишинга. Негативные тенденции статистики ставят перед нами задачу глубинного исследования преступной деятельности интернет-мошенников, использующих фишинговые методы.

Термин фишинг характеризует один из видов мошенничества, в котором технологии и возможности сети «Интернет» используются для выполнения действий, направленных на незаконное завладение информацией пользователя тех или иных сервисов, предоставленных онлайн, хранящих данные пользователя – такие как логины и пароли, данные банковских карт, а также любую информацию, которая может быть использована преступником в целях незаконного обогащения посредством использования данных пользователя.

Анализ статистики подобных преступлений в России и за рубежом показывает, что тенденция распространенности подобных преступлений нарастает, а наивные схемы мошенников усложняются в противовес к выработке «иммунитета» у населения к подобным схемам обмана в интернете.

На данный момент активные интернет пользователи в развитых странах составляют заметное большинство населения, устройство сервисов и услуг выглядит таким образом, что современному человеку сложно обойтись без таковых не рискуя быть оторванным от полноценной социальной активности. Следовательно, возросло и число мошенников, которые стремятся поживиться ценной информацией «юзеров». Составленная в ходе осуществления практики и посредством трудов ученых теоретиков картина преступника, практикующего фишинг, отсылает нас к технически грамотному и оснащенному передовой технологией злоумышленнику, который достаточно хорошо осведомлен о том, как сохранить собственную анонимность, вернее обеспичить обезличенность собственного присутствия в сети, а помимо прочего подкованного в психологии, а более в разделе «социальная инженирия». Оценка интерпола показывает, что рост числа преступлений с использованием сети «Интернет» растет с наибольшими темпами в сравнении с другими видами преступлений [1].

Так, например, в России подобный рост составлял 91,7% в период с января по июнь 2020 года в сравнении с аналогичным периодом предыдущего года, что свидетельствует о сохранении негативной тенденции в стране [2].

Фишинг является не единственным, но одним из самых распространённых способов мошенничества в глобальной сети. Несмотря на то, что это один из самых «древних» способов интернет-мошенничества, появившийся ещё на заре интернета, он по-прежнему остается распространенным и прибыльным для интернет-мошенников. Основанный на психологических ошибках людей данный метод, позволяет максимально обезличено отнимать деньги у доверчивых граждан сохраняя обезличенный статус злоумышленника. Буквально — рыбалка, но рыбой выступают владельцы банковских карт и иных данных пользователей.

Существуют различные способы реализации фишинговых схем, например, одну из них мы можем наблюдать на рисунке ниже:

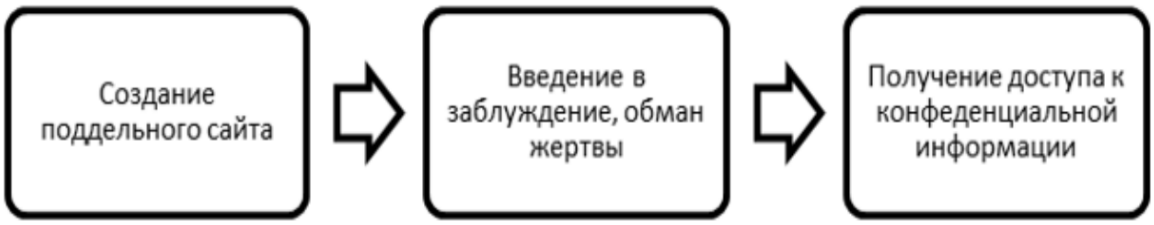

Рис. 1 Схема работы фишинга.

Такая деятельность, направленная на завладение чужими данными может иметь вид электронного письма, направленного от имени знакомых получателю контактов или организаций. В данных целях распространена практика так называемого «спуфинга» - подделка адрес отправителя, который отображается в письме. Содержание письма отличается вредоносным файлом, в который заложено опасное программное обеспечение, вредоносными ссылками, ведущими на небезопасные для посещения сайты. Целью такого письма является заражение устройства пользователя и последующее завладение его данными. Последствиями выступает заражение устройства носителя с последующим завладением информации, представляющей финансовую ценность для

мошенника. Чаще всего такие письма направляются от лица, банков, провайдеров сети и т.п. и содержат информацию о обновлениях безопасности, заблокированных картах либо попытках мошенничества. Злоумышленники стремятся получить конфиденциальную информацию, такую как номера банковских карт, ПИН-коды и CVV/CVC. Перепуганные или не подозревающие жертвы часто раскрывают эту информацию, что приводит к финансовым потерям [3].

Также излюбленной технологией мошенников является копирование сайтов известных интернет-магазинов, где совершение «покупки» чревато тем, что данные банковской карты получает мошенник, который снимает с нее все имеющиеся средства [4].

Количество возможных схем ограничивается лишь фантазией злоумышленников, так как обычно, они не испытывают трудностей с профессиональной подготовкой и техническим оснащением. Нас же интересует дальнейший анализ противодействия фишинговому мошенничеству.

В действующем законодательстве предусмотрена ответственность по ст. 159.6 Уголовного кодекса РФ «Мошенничество в сфере компьютерной информации» [5]. Согласно данной норме уголовного закона фишинговые действия полностью подпадают под определение «Компьютерное преступление». Данный состав имеет место быть в случае совершения незаконных операций с данными пользователей, в том числе их банковских карт и счетом, с использованием сети «Интернет», а также следует подчеркнуть, в добровольном порядке со стороны потерпевшего, заведомо введенного в заблуждение. Так, по данным компании «Антифишинг», а также на базе открытых источников, за 2021 г. 30 % сотрудников открывали фишинговые письма, а 21 % переходили по ссылкам из таких писем, скачивали и открывали вложенные в письма программы [6].

1. Учитывая добровольный характер передачи собственных данных потерпевшими, следует обратить внимание на аспекты не сколько

противодействия таким видам преступлений, но скорее профилактики. Рекомендуется выделить наиболее распространенные темы фишинговых писем:

2. Тема массовых эпидемий — стала актуальна в период пандемии COVID-19;

3. Рассылки от компании работодателя — например о премировании, изменении порядка выдачи заработной платы;

4. Новинки кино и ожидаемые сериалы — распространено среди любителей подобных зрелищ;

5. Различные ставки на результаты спортивных мероприятий;

6. Услуги по обеспечению компенсаций пострадавшим в результате природных и техногенных катастроф, терактов, боевых действий;

7. Фальшивые письма от сервисов доставки и маркетплейсов;

8. Покупка билетов на спортивные или культурные мероприятия;

9. Подписки на сервисы;

10. Инвестиции;

11. Фейковые знакомства — наиболее тяжелый случай, как показывает практика [7].

Таким образом мы наблюдаем распространенный вид мошенничества несущий в совокупности большой материальный ущерб в масштабах государства — не говоря о том, что зачастую ущерб отдельным лицам признается ими значительным. Классификация фишинговых схем, методов их реализации и слабых мест пользователей, легковерно отдающих свои деньги мошенникам, требует тщательной работы и перманентного мониторинга данного направления преступной деятельности.

Библиографический список:

1. Поддубный И. В. К вопросу об использовании злоумышленниками программ удаленного доступа и вредоносного ПО как средств совершения хищений с банковских карт граждан // Криминалистика: вчера, сегодня, завтра. 2000. №3 (15).

2. Министерство внутренних дел / Главная / Новости / О состоянии преступности в Российской Федерации в 1-м полугодии 2000 года. [Электронный ресурс] // URL: https://xn--b1aew.xn--p1ai/news/item/058066 (Дата обращения 30.04.2024).

3. Галыджова А., Данатаров Д. О., Гурбанназаров М. Р. Софт-мошенничество с применением фишинговых методов // Вестник науки. №3 (72) 2024. С. 328-333.

4. Могунова М. М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) // Вестник СГЮА. 2000. No4 (135).

5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 25.12.2023) (с изм. и доп., вступ. в силу 30.12.2023) // URL: https://www.consultant.ru/document/cons_doc_LAW_10699/c193654ae5c3bd5b02d92ade18796cd8864ec353/ (Дата обращения 30.04.2024).

6. Александров А.Г., Петухов А.Ю., Даньялов А.С. Анализ угроз информационной безопасности при использовании фишинговых сайтов // Юрист-Правоведъ. 2022. №4 (103). С. 156-161.

7. Фишинговые сайты [Электронный ресурс]. URL: https://volgograd.megafon.ru/bezopasnoe_obschenie/fraud_on_the_internet_social_networks/fishingovye_sayty/ (Дата обращения 04.05.2024).