УДК 004.8

# СОВРЕМЕННЫЕ ВИДЫ МОШЕННИЧЕСТВА И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

Салдаева А.А., студент гр. Б-ИСиТ-22, II курс
Научный руководитель: Ткаченко А.Л., к.т.н, доцент
Калужский государственный университет им. К.Э. Циолковского
г. Калуга

В 21 веке активно развиваются информационные технологии, появляются новые устройства для взаимодействия как с окружающим миром, так и между людьми. Кроме того, телефон сейчас хранит в себе множество вещей: кошелек, фотографии, номера, переписки и много другой конфиденциальной информации. Чем активнее развиваются различные устройства, тем больше появляется соблазна у мошенников завладеть конфиденциальной информацией. Они постоянно придумывают новые уловки и способы обмануть пользователей мобильных устройств, поэтому попытки защитить личную информацию стали неотъемлемой частью нашей жизни. В случае если вы все-таки потеряли мобильное устройство, можно потерять много личной информации, которая может попасть в руки мошенников. Чтобы знать, как защищаться в таком случае, и какую информацию не стоит передавать третьим лицам, необходимо знать какие именно бывают виды мошенничества и способы защиты [5,6].

Активное развитие телефонное мошенничество получило в начале 2000-х годов, когда мобильные устройства проникли в массы. Именно в это время телефон мог иметь как ребенок, так и пенсионер. Тогда мошенники выявили новую область, где можно незаконно заработать и начали активно развивать свои незаконные методы получения денежных средств на чужом доверии. Тогда стало распространяться преступления против собственности, совершаемые при помощи применения различных форм хищения чужого имущества. Самое страшное в этом то, что преступники, применяя новые технологии могут жить за счет другого человека и никто об этом не узнает. Они осваивали область мобильного мошенничества постепенно, проникали в разные сферы связи и практически везде находили слабые места, чтобы начать применение новых идей мошенничества [3,9].

Изучив множество источников, мною было выделено 4 самых распространенных вида мошенничества, которые сбивают вашу бдительность [1,2,4].

Первый вид мошенничества - это ложное сообщение о заражении мобильного устройства вредоносной программой. Спросите, как это работает?

После очередного посещения сайта, на экране появляется ложное сообщение о попытке взлома и внедрении вируса на ваше устройство. Затем тут же предлагают установить программу, которая якобы защитит от всех вирусов, но на самом деле лишь через эту программу попадает вирус на ваше мобильное устройство. Как себя защитить? Прежде всего не стоит поддаваться на такие сообщения и лучше установить антивирус на мобильное устройство, особенно актуальным способ будет для защиты пожилых родственников [4].

Самым распространенным и зарекомендованным антивирусом на мобильное устройство за последние годы стало приложение Avast Mobile Security. Данное приложение показывает очень хорошие результаты в процессе своей работы, гарантируя 100-процентную защиту мобильного устройства от атак и вирусов самого различного характера. Еще существенным плюсом данного приложения является то, что весь интерфейс (рис.1) представлен на русском языке, что будет способствовать повышению уровня понятности и простоты использования русскоязычной аудитории. Mobile Security помогает оградить вас и ваше устройство от фишинга и вредоносных сайтов, а также обеспечивает защиту от кражи и блокирует подозрительные вызовы.

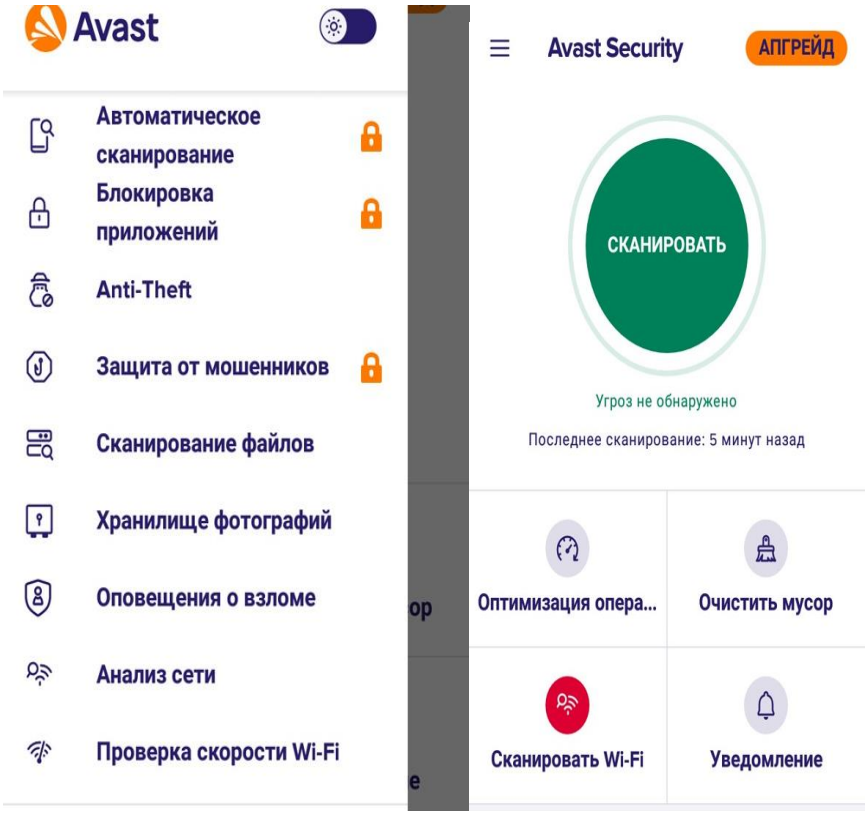


*Рисунок 1. Интерфейс Avast Mobile Security*

Второй способ - это телефонный фишинг, казалось страшное и непонятное слово, но думаю, что практически каждый сталкивался с подставными банковскими работниками. Фишинг - это вид мошенничества, когда вам звонят как будто сотрудники организации и пытаются побудить вас

к какому-либо действию. Чаще всего мошенники притворяются реальными людьми или сотрудниками компании, чтобы быстрее завоевать ваше доверие. Данным способом мошенники стараются вытянуть из вас конфиденциальную информацию: пароль, личные данные или же сразу перевести деньги на “безопасный счет”. Важно отметить, что мошенники требуют от вас действий прямо здесь и сейчас, чтобы вы не успели запаниковать или рассказать родным о данном звонке. Как обезопасить себя в таком случае? Включить блокировку незнакомых входящих номеров и никогда не общаться по телефону с сотрудниками организации, если можно сходить и поговорить лично [7,8].

Третий способ “SMS- фишинг”. В данном способе мошенники побуждают нас к действию через сообщение. Например, перейти по ссылке, перезвонить на платный номер, оформить подписку или выдать личные данные. Хочется отметить, что данный способ является наиболее опасным нежели телефонный фишинг. Спросите почему? Ведь можно просто не обращать внимание на такие смс и все, но дело обстоит куда глубже, приведу аргументы, почему SMS- фишинг опаснее [7,8]:

1. Все уже привыкли, что на почту приходит много лишней информации, рекламы и особо никто не заостряет на этом внимание, поэтому проще попасться на уловки мошенников.
2. Во-вторых, несмотря на то, что доверия к SMS больше, защищены они в среднем хуже, чем та же электронная почта. В любую приличную почтовую службу сегодня обязательно встроен спам-фильтр, зачастую очень даже умный, но спам-фильтрами мобильные операторы на сегодняшний день похвастаться особо не могут.
3. В-третьих, SMS чаще читают на ходу и между делом, что в сочетании с первым пунктом усиливает некритичность взгляда и повышает вероятность успешной атаки.
4. У SMS значительно меньше признаков, по которым можно распознать, что это мошенники, поэтому стоит внимательнее относиться к различным рассылкам SMS.

Ниже приведены примеры SMS-фишинга для более четкого представления о виде мошенничества.

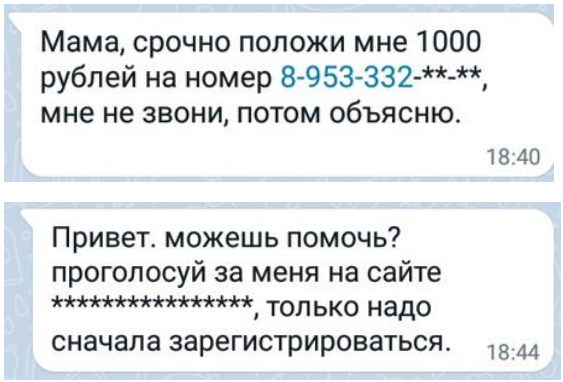


*Рисунок 1. SMS-фишинг*

Как себя обезопасить в таком случае? Самый верный и надежный способ никуда не переходить, никому не отвечать и блокировать подозрительные номера.

И последний способ - это сбрасывающие звонки, вызовы с неизвестного номера, которые сбрасываются через пару секунд. Зачем сбрасывают звонок? Таким способом проверяют «живой» или «неживой номер» [8]. Если номер окажется живым, то есть вы ответите на звонок, то в дальнейшем вам будут поступать различные звонки и будут стараться продать вам что-то, в противном случае скорее всего номер будет помечен как «неживой» и его вычеркнут из списка в случае обзвона потенциальных клиентов. Как защитить себя в такой ситуации? Есть несколько вариантов:

1. Не брать вызовы с незнакомых номеров или установить специальные приложения, которые блокируют номера, на которые поступали жалобы
2. Не перезванивать на незнакомые номера! Если кому-то необходимо с вами связаться это можно сделать по смс или другим доступным способом, если даже закончились денежные средства на телефоне.

Многие сейчас активно пользуются продуктами кампании Google, но почему-то не пользуются всем функционалом бесплатных продуктов данной компании. Скорее всего у вас на телефоне уже установлена программа «Телефон», в которой хранятся все ваши номера, так же в данном приложении есть очень актуальная в 21 веке функция – фильтр спам-звонков, отображение идентификатора абонента и спам. Включив данные функции (рис. 2) вы можете забыть про телефонный фишинг и сбрасывающиеся звонки.

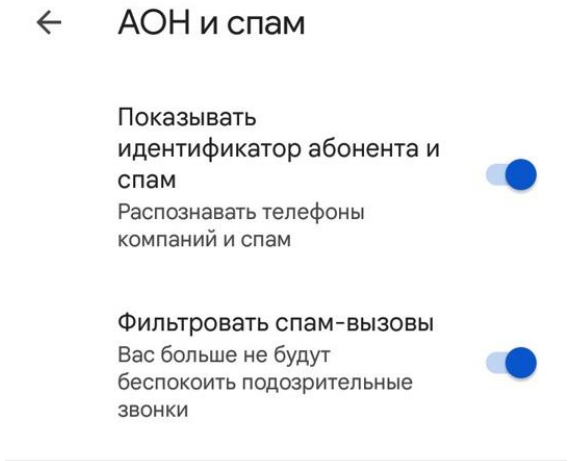


*Рисунок 2. Вспомогательные функции для блокировки звонков*

Важно ответить, что на притяжении всей истории нашей страны, были законодательные акты, которые регламентировали действия и последствия от

мошенничества. Самым первым документом, который стал своего рода источником уголовного права стала «Русская Правда», регулирующая наказание за преступление и его совершение с XI века по XVI век. В настоящее время ответственность за мошенничество регламентирует ст. 159 Уголовного кодекса Российской Федерации, которая разъясняет случаи и виды ответственности, а именно штраф от 10 тысяч рублей и до 5 лет лишения свободы в зависимости от тяжести преступления [3].

Исходя из вышесказанного, можно сделать вывод, что мобильное мошенничество в дальнейшем будет только развиваться и не стоит расслабляться, если не хотите, чтобы ваши персональные данные попали в чужие руки. Человеку в современном обществе стоит знать о всевозможных угрозах, чтобы обезопасить себя и своих близких [10].

**Список литературы:**

1. Баранова, Е. К. Информационная безопасность и защита информации: учеб. пособие /Е. К. Баранова, А. В. Бабаш; 4-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2019. —322 с.
2. Ярочкин, В. И. Информационная безопасность: учебник для студентов вузов /В. И. Ярочкин. — Москва: Академический проект; Гаудеамус, 2004. — 544 с
3. Колескин Д. В. История развития мошенничества, современные виды мошенничества и способы борьбы с ними // Социально-гуманитарные проблемы современности : сборник научных трудов по материалам Международной научно-практической конференции 24 апреля 2020г. : Белгород : ООО Агентство перспективных научных исследований (АПНИ), 2020. С. 37-42.
4. Гусев, В.Н. Вопросы обеспечения телефонной безопасности / В.Н. Гусев // Вестник Казанского юридического института МВД России. – 2015. – № 2. – С. 34-42.
5. Гусев, В.Н. Вопросы обеспечения телефонной безопасности / В.Н. Гусев // Вестник Казанского юридического института МВД России. – 2015. – № 2. – С. 34-42.
6. Шаевич, А. А. Актуальные перспективы борьбы с мошенничествами, совершаемыми с использованием средств мобильной связи / А. А. Шаевич, А. А. Рудых, В. А. Родивилина // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) : Сборник статей Международной научно-практической конференции, Москва, 18 мая 2018 года. – Москва: Академия управления Министерства внутренних дел Российской Федерации, 2018. – С. 305-310.
7. Ситдикова, Г. З. К вопросу о квалификации мошенничества, совершенного с использованием мобильного устройства / Г. З. Ситдикова // Вестник Института права Башкирского государственного

университета. – 2021. – № 4(12). – С. 107-112. – DOI 10.33184/vest-law-bsu-2021.12.11.

8. Романов, А. А. О современных способах мошенничеств, совершаемых с использованием средств мобильной связи / А. А. Романов, В. А. Машлякевич // Евразийский юридический журнал. – 2021. – № 10(161). – С. 254-255.
9. Иванец, М. Э. Анализ угроз информационной безопасности для коммерческой организации / М. Э. Иванец, А. Л. Ткаченко // Цифровая трансформация промышленности: тенденции и перспективы : Сборник научных трудов по материалам 2-й Всероссийской научно-практической конференции, Москва, 11 ноября 2021 года. – Москва: Общество с ограниченной ответственностью "Русайнс", 2022. – С. 364-370.
10. Ткаченко, А. Л. Анализ эффективности защиты персональных данных и проблема cookie файлов / А. Л. Ткаченко, Е. С. Сафронов, В. И. Кузнецова // Дневник науки. – 2021. – № 6(54).