Особенности фишинга в кредитно-финансовой сфере

Павел Владимирович Ревенков
доктор экономических наук,
профессор кафедры информационной безопасности,
Финансовый университет при Правительстве Российской Федерации,
4-й Вешняковский проезд, д. 4, корп. 2, г. Москва, 109456, Россия.
E-mail: PVRevenkov@fa.ru
orcid.org/0000-0002-0354-0665

Марина Дмитриевна Шуликова,
студентка 3-го курса, Финансовый университет при Правительстве Российской Федерации, Российская Федерация, Москва, 4-й Вешняковский проезд, д. 4, корп. 2, г. Москва, 109456
E-mail: 230867@edu.fa.ru
ORCID: 0009-0005-8113-3167

Аннотация. В статье рассматриваются наиболее распространённые виды фишинга, осуществляемые как самостоятельно, так и с использованием методов социальной инженерии. Проанализированы основные причины «успешных» фишинговых атак. Представлены алгоритмы типичных мошеннических схем. Перечислены наиболее характерные признаки фишинговых сайтов и даны рекомендации, каким образом можно проверить достоверность размещаемой на сайте информации.

Ключевые слова: фишинг, кибермошенничество, социальная инженерия

Features of phishing in the credit and financial sector

Pavel V. Revenkov
Doctor of Economics,
Professor, Department of Information Security,
Financial University under the Government of the Russian Federation,
4th Veshnyakovsky Proezd, Building 4, Bldg. 2, Moscow, 109456, Russia.
E-mail: PVRevenkov@fa.ru
https://orcid.org/0000-0002-0354-0665

Marina D. Shulikova,
Third-year student, Financial University under the Government of the Russian Federation, Russian Federation, Moscow, 4th Veshnyakovsky Proezd, Building 4, Bldg. 2, Moscow, 109456
E-mail: 230867@edu.fa.ru
https://orcid.org/0009-0005-8113-3167

Annotation. This article examines the most common types of phishing, both self-inflicted and through social engineering. It analyzes the main reasons for "successful" phishing attacks. The algorithms of typical fraudulent schemes are presented. The most characteristic signs of phishing sites are listed and recommendations are given on how to verify the authenticity of the information posted on the site.

Keywords: phishing, cyber fraud, social engineering

Введение / Introduction

Современный бизнес уже давно стал использовать возможности интернет-технологий, переводя почти все процессы взаимодействия с клиентами в киберпространство. Отсутствие необходимости строить (или снимать) офисы для обслуживания клиентов стало одним из основных преимуществ данного способа ведения бизнеса.

Однако с перемещением бизнеса «из офисов» в кибепространство возникли новые риски, среди которых особо выделяются риски кибермошенничества [1]. Наиболее распространённым видом кибермошенничества сегодня является фишинг (от англ. fishing — «рыбалка»), при котором злоумышленники обманывают пользователя, чтобы получить его конфиденциальные данные. К ним относятся логины, пароли, паспортные данные, реквизиты банковских карт и другие сведения, предоставляющие доступ к денежным средствам клиентов организаций кредитно-финансовой сферы (ОКФС).

По итогам первого квартала 2026 года, по данным системного интегратора «Информзащита», почти все направления атак кибермошенников показали заметный рост. Лидером остается сегмент фишинга и социальной инженерии, который за год вырос на 11 п. п., до 68%, а также вредоносное программное обеспечение (ВПО) с удаленным доступом — рост на 11 п. п., до 41% [2].

Материалы и методы / Materials and Methods

Теоретическую основу исследования составили труды российских и зарубежных ученых в области кибербезопасности, кибермошенничества и поведенческой психологии. Вопросы противодействия фишинговым угрозам в кредитно-финансовой сфере рассматриваются в работах П.В. Ревенкова, А.А. Бердюгина, А.Г. Чебаря, К.Р. Ошманкевич [3-5]. Психологические аспекты уязвимости граждан к финансовому внушению раскрыты в работах О.В. Медяник и Н.А. Низовских [6], а также Ю.В. Щербатых [7]. Среди зарубежных исследований следует выделить работы, посвященные систематизации фишинговых атак, методов противодействия им и анализу психологических профилей жертв социальной инженерии [8; 9].

Эмпирическую базу исследования составили статистические материалы Центрального банка Российской Федерации [10], а также данные российских компаний,

работающих в сфере кибербезопасности: CICADA8 [11] — разработчика решений для управления уязвимостями, системного интегратора «Информзащита» [2].

Методологическую основу исследования составили аналитический, описательный и сравнительный методы, а также классификация.

Обсуждение / Discussion

В CICADA8[1] проанализировали массив фишинговых ресурсов за первый квартал 2026 года и сформировали топ угроз:

1. Поддельные инвестиционные компании, обещающие пользователям высокий доход, доступ к «эксклюзивным» инвестиционным программам или участие в якобы проверенных финансовых проектах.

2. Опросы с денежным вознаграждением от имени известной компании, ОКФС, маркетплейса или сервиса.

3. Поддельные формы входа в личные кабинеты ОКФС и государственных порталов. В первом квартале 2026 года фиксировались схемы с использованием брендов Сбера, ВТБ, Т-Банка, Ozon Банка и Банка России.

4. Сайты с обещанием социальных выплат, материальной помощи или участия в специальных программах поддержки. Один из выявленных сценариев — фейковая акция «Помощь 2026».

5. Фишинговые клоны популярных маркетплейсов и сервисов доставки: Ozon, Wildberries, СДЭК, Avito и Яндекс.Маркет. Используются схемы с прохождением опросов, оплатой заказа, подтверждением доставки или возвратом средств [11].

Чаще всего, полученную с помощью фишинга информацию злоумышленники используют для кражи денег. Но фишинг опасен не только этим. С его помощью мошенники могут:

- получить доступ к электронной почте и социальным сетям, а затем рассылать спам от имени пользователя или шантажировать его;

- похитить копии документов (в том числе содержащие сведения, которые относятся к коммерческой тайне), персональные данные для перепродажи или для использования в других мошеннических схемах;

- установить ВПО для перехвата данных и удалённого управления устройством;

[1] Cicada8 — сервис централизованного управления уязвимостями внешнего периметра, предназначенный для обеспечения кибербезопасности организаций. Разработан компанией «Айтипи Сервисы» (Россия). Официальный сайт - https://cicada8.ru/contact.

- проникнуть в инфраструктуру организации с целью получения доступа к управляющим серверам и хранилищам данных.

Алгоритм фишинговой атаки строится на имитации легитимного источника. Злоумышленники маскируют ресурсы под известные сервисы: онлайн-банки, интернет-магазины, социальные сервисы, государственные порталы или корпоративные системы. В некоторых случаях подделка полностью копирует оригинал и внешне отличить подмену практически невозможно. Или же предлагают воспользоваться услугами «нового» банка (рисунок 1).[2]

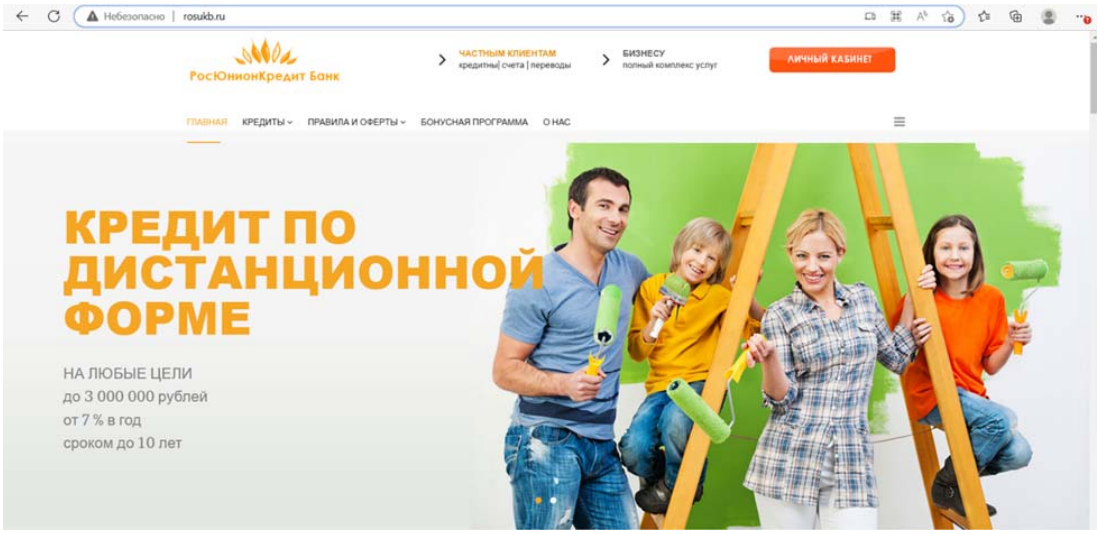

Рис. 1. Сайт несуществующего (фишингового) банка

После перехода по фишинговой ссылке пользователь оказывается на странице сайта несуществующей ОКФС, где ему предлагают ввести свои конфиденциальные данные, которые сразу же может видеть злоумышленник.

Фактически современный фишинг является разновидностью семантической атаки. Семантические атаки представляют собой атаки, которые основаны на взаимодействии человека с компьютерной средой. Иными словами, потенциальную жертву обманывает не другой человек, а интерфейс, сайт, сообщение системы или визуальная среда в целом. Суть семантической атаки заключается в изменении внешнего вида или контекста таким образом, чтобы пользователь сам совершил ошибочное действие. Атака воздействует на то, как человек воспринимает и осмысливает увиденное, эксплуатируя особенности человеческого мышления: привычку доверять знакомым визуальным образам, склонность к автоматическим реакциям и невнимательность к деталям. Таким образом, главным

[2] Рис. 1. Сайт несуществующего (фишингового) банка. Источник: [14]

инструментом обмана в фишинге выступает подделанная визуальная среда, формирующая у жертвы ложное ощущение подлинности.

Одной из самых распространенных категорий фишинговых ресурсов являются сайты фиктивных ОКФС, инвестиционных сервисов и различных маркетплейсов [3]. Высокий спрос на услуги этих организаций среди потребителей активно используется злоумышленниками в корыстных целях. Только за 2025 год Банк России направил регистраторам доменных имен информацию о 1002 подобных ресурсах для последующего снятия их с делегирования [10].

Зачастую для привлечения повышенного внимания со стороны потенциальных жертв злоумышленники размещают на сайте или в социальных сетях заманчивые рекламные предложения, обещают получение выигрыша или выгодную для потребителя акцию. Обманутая жертва, вводит реквизиты своей карты и лишается своих средств (рисунок 2).[3]

Рис. 2. Схема мошенничества «Фишинговый розыгрыш / акция»

При этом для осуществления фишинговой атаки мошенниками не обязательно создаётся самостоятельный фишинговый ресурс. Зачастую злоумышленники регистрируются на легитимных площадках и ведут деятельность там. Воздействовать на жертву им удаётся за счёт того, что они переводят коммуникацию за пределы доверенного ресурса — например, предлагают продолжить общение в мессенджере или обсудить условия сделки вне портала. Именно там генерируются и распространяются фишинговые ссылки. В качестве конкретного примера можно рассмотреть схему, получившую

[3] Рис. 2. Схема мошенничества «Фишинговый розыгрыш / акция». Источник: составлено авторами

распространение на сервисах доставки: выбор товара и первичный контакт происходят на настоящем сервисе, а сама атака разворачивается уже вне его контура (рисунок 3).[4] Это особенно опасно, поскольку пользователь не замечает подмены, и мнимое нахождение в знакомой, надёжной среде ещё больше усыпляет его бдительность [12].

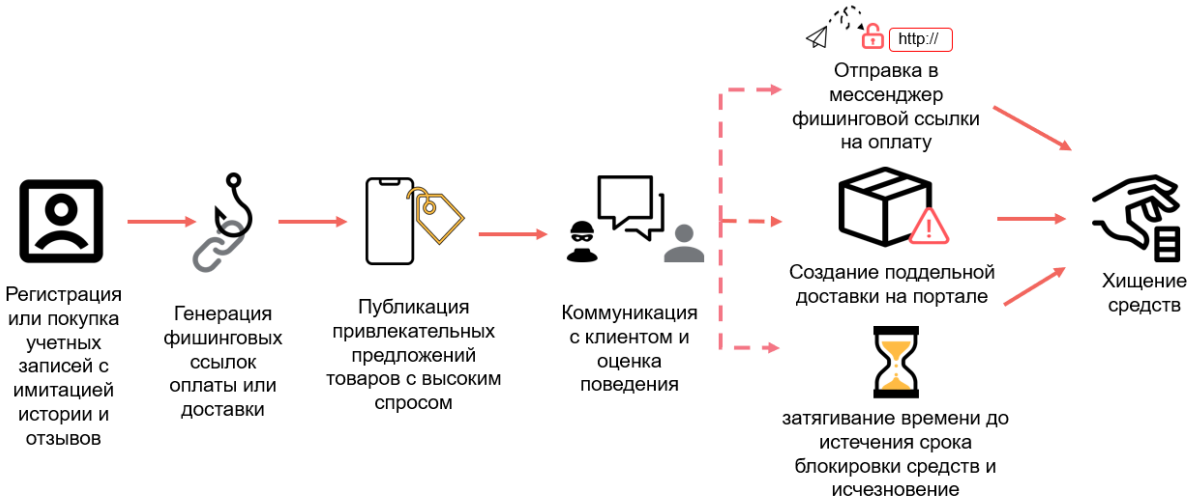

Рис. 3. Схема мошенничества «Мошенник-продавец»

Далее рассмотрим, как изменился фишинг за последние несколько лет и какие новые технологии стали использовать злоумышленники.

В современных фишинговых атаках востребована схема с промежуточным сервером — прокси. Сам по себе прокси — это легитимный инструмент, который применяется, например, для балансировки нагрузки или фильтрации трафика.

В фишинге он становится точкой перехвата между пользователем и сервисом. Основная цель — перехватить уже активный доступ к аккаунту без повторной авторизации (такой подход называют прокси-фишингом). Прокси выступает посредником между пользователем и оригинальным сервисом: через него проходит весь трафик. Поддельная страница в реальном времени передаёт данные на реальный сайт и одновременно отправляет их злоумышленнику. При этом пользователь взаимодействует с настоящим сервисом и не замечает подмены.

Данный сценарий относится к классу атак «человек посередине» (Man-in-the-middle, MitM) – это атака, при которой злоумышленник тайно встаёт между двумя сторонами (например, между пользователем сети Интернет и сайтом, банком или почтовым сервером), чтобы перехватывать, а при необходимости и изменять передаваемые ими данные. При этом обе стороны остаются в неведении: они думают, что общаются

[4] Рис. 3. Схема мошенничества «Мошенник-продавец». Источник: составлено авторами

напрямую, а на самом деле весь трафик проходит через атакующего. Атакующий перехватывает данные при передаче и получает не только логин и пароль, но и коды многофакторной аутентификации и сессионные токены (временные данные, которые сервер выдаёт после входа в аккаунт для подтверждения авторизации).

Фишинг также может использоваться для осуществления многоходовых атак. Например, сначала жертва получает письмо по электронной почте с просьбой перейти по ссылке на какой-нибудь сайт. Затем происходит звонок с целью уточнить код подтверждения (под каким-нибудь предлогом) и в итоге злоумышленник получает доступ к аккаунту. Эта же атака может начинаться и с СМС-сообщения (или же сообщения в мессенджере), в котором злоумышленник под различным предлогом просит перейти на сайт.

Добавим, что сегодня есть предложения по оказанию помощи в части осуществления фишинга. Такой сервис получил название Phishing-as-a-Service (PhaaS) – т.е. фишинг, как услуга. Для злоумышленника использование такой «услуги» дает возможность (без особых технических знаний и умений) получать:

шаблоны писем и сайтов;

домены и хостинг;

инструменты рассылки;

панели управления и статистика.

Также для автоматизации некоторых процессов могут использоваться чат-боты. Они (чат-боты) могут работать по заранее установленным скриптам, ведя диалог с жертвой, отвечать на их вопросы и т.д.

Следует отметить, что искусственный интеллект (ИИ) также стал использоваться для осуществления фишинга. По оценкам экспертов сегодня 3 из 5 фишинговых атак готовятся с использованием ИИ.

ИИ трансформировал фишинг, сделав его массовым, дешёвым и более убедительным. Это привело к нескольким заметным трендам.

Совершенная персонализация. Раньше сбор информации о жертве занимал часы и дни. Сегодня ИИ за секунды способен анализировать открытые источники (сайты, соцсети, профили в сервисах), после чего использует эти данные в атаке. В сгенерированные сообщения включаются имя, должность, недавние события и рабочий контекст. Это делает их персонализированными и снижает бдительность даже у опытных пользователей.

С помощью искусственного интеллекта мошенники могут генерировать тексты, близкие к естественной речи. Они не содержат в себе грамматических ошибок, а кроме того, могут быть адаптированы под конкретную жертву. Сгенерированные сообщения позволяют перенимать стиль общения потенциальной жертвы и ее характерные фразы.

Причем это касается не только частных пользователей, но и государственных структур. Для этого злоумышленники используют ИИ в 65% случаев. По данным Microsoft, фишинговые письма, созданные с помощью ИИ, в 4,5 раза эффективнее написанных вручную: количество переходов составляет 54% против 12% у обычных сообщений [13].

Благодаря развитию дипфейков мошенники могут имитировать не только стиль общения в тексте, но также голос и внешность человека в аудио- и видеосообщениях.

Ещё одно ключевое изменение — *масштаб и скорость*. ИИ позволяет запускать тысячи уникальных атак одновременно, автоматически вести диалог и быстро создавать фишинговые сайты.

Вместе с тем коммуникация с жертвой происходит в режиме реального времени: мошенник не просто рассылает ссылки и ждёт результата, а сопровождает жертву на каждом этапе — от ввода логина и пароля до запроса дополнительных данных. Автоматизированный помощник на базе ИИ постоянно готов отвечать на вопросы, а в случае колебаний начинает убеждать жертву, подталкивая к нужному действию. По сути, злоумышленник всегда остаётся «на связи» и по мере развития диалога собирает всё больше информации — паспортные данные, реквизиты карты, номер телефона (рисунок 4).[5] Именно эта непрерывность контакта и способность гибко реагировать на поведение жертвы кратно повышают эффективность атаки по сравнению с традиционными фишинговыми схемами

[5] Рис. 4 Схема мошенничества «Фишинг с использованием искусственного интеллекта». Источник: составлено авторами

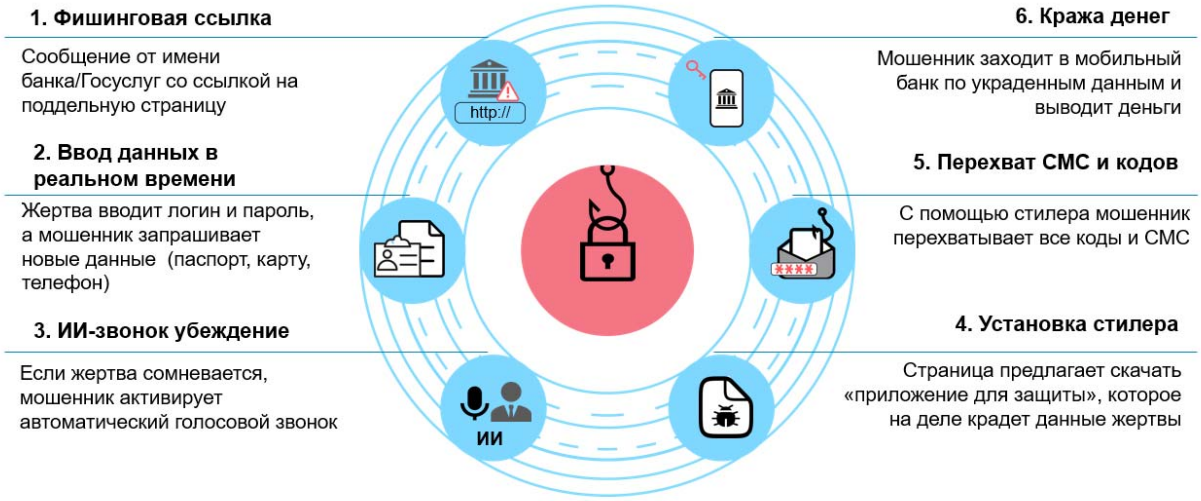

Рис. 4. Схема мошенничества «Фишинг с использованием искусственного интеллекта»

Отметим, если мошенник при самостоятельной работе может совершить до 300 фишинговых звонков в день, то благодаря ИИ это число увеличивается до 40–50 тысяч.

Автоматизация на базе ИИ способна повысить прибыльность фишинга до 50 раз за счёт масштабирования атак. При этом расходы снижаются на 95%[6].

Во многом «успех» от фишинга связан с особенностями поведения людей и их психологического состояния. Интересные исследования ведутся учеными в области поведенческой психологии. Так, в частности в работе Ольги Викторовны Медяник и Нины Аркадьевны Низовских приводятся наиболее характерные черты людей, которые чаще всего подвержены внушаемости [6]. Среди них выделяются, например, высокая восприимчивость к внушению: гипнабельные[7] люди легко воспринимают идеи или поведение, предложенные другими людьми. Кроме того, внушаемостью могут обладать люди, способные глубоко концентрироваться на задаче, игнорируя внешние факторы. Вместе с тем способность к фантазированию и яркое развитое воображение позволяют человеку дорисовывать реальную картину, наделяя её дополнительными чертами. Гипнабельностью обладают также люди, находящиеся в стрессе и тревожные люди: они подвержены внушению из-за желания найти решение своего состояния. Такие, люди, по

[6] См. подробнее «Что такое фишинг и как он изменился в 2026 году» (https://firstvds.ru/blog/chto-takoe-fishing-i-kak-izmenilsya-v-2026-godu?ysclid=mr37a7l72e569571651).

[7] Гипнабельность — это индивидуальная способность человека входить в гипнотическое состояние и воспринимать внушение. Этот показатель отражает, насколько легко человек реагирует на гипноз и принимает терапевтические установки. При этом гипнабельность не относится к мистике: она рассматривается как психологическая и нейрофизиологическая особенность, которая в той или иной степени присутствует у большинства людей.

природе не склонные к скептицизму и открытые новому опыту, тоже могут быть более подвержены манипулятивному воздействию.

Можно выделить несколько групп людей, склонных к финансовому внушению.

Во-первых, чаще других поддаются манипуляциям недостаточно информированные люди: они не обладают достаточной финансовой грамотностью и знаниями о банковских и инвестиционных продуктах, а потому уязвимы в ситуациях финансового внушения.

Во-вторых, люди, ищущие простых решений: зачастую они стремятся получить результат быстрым и лёгким способом и могут быть привлечены яркой рекламой с обещанием выгодных для них условий.

В-третьих, чрезмерно оптимистичные люди склонны недооценивать имеющиеся риски и верить в свою удачу и возможность успеха.

В-четвёртых, люди, подверженные социальному давлению: их мнение формируется под влиянием общественности, знакомых и популярных трендов.

В-пятых, люди с импульсивным характером: они быстро принимают решения и в большинстве случаев не анализируют возможные последствия.

В-шестых, люди, испытывающие финансовые трудности: они могут не видеть выхода из сложившейся ситуации и более открыты к рискованным предложениям.

В-седьмых, эмоционально уязвимые люди, находящиеся в стрессе в результате различных потрясений, связанных с личной жизнью.

Результаты / Results

Как бы злоумышленники не старались добиться полной аналогии с истинным ресурсом – сделать это очень сложно. Если речь идет о фишинговом сайте. то все равно полного совпадения добиться невозможно. В первую очередь надо обращать внимание на доменное имя (оно может отличаться всего одной буквой или символом). Далее можно узнать, когда был создан сайт и на кого зарегистрирован, почитать отзывы на организацию (которой принадлежит сайт). Как правило, мошеннические ресурсы имеют очень маленький срок службы (т.е. созданы были несколько дней назад). Помимо этого, в текстах, размещенных на страницах сайта, могут быть грамматические ошибки или несоответствие фактическим сведениям (например, по указанному на сайте адресу организации находится совершенно другое юридическое лицо, а в ряде случаев на указанной улице вообще нет дома с номером, который указан на сайте).

В случае поступления сообщения на электронную почту необходимо также обращать внимание на отсутствие грамматических ошибок, а также на тот факт, что

сообщение написано слишком универсально и могло быть адресовано любому человеку. Как правило, когда начинается диалог, должно всегда настораживать, если ответы оператора или бота приходят слишком быстро, как будто автоматически, а в тексте замаскировано давление (слова «пожалуйста» и «спасибо» повторяются часто, но при этом создаётся ощущение срочности). Скорее всего такой диалог поддерживает не человек (оператор), а ИИ. И уж тем более надо прекращать диалог, когда запрашивают CVV-код, полный пароль или одноразовый код из SMS.

Еще несколько рекомендаций для клиентов ОКФС:

- перепроверяйте запросы. Не действуйте сразу, если к вам обращаются с просьбой — особенно если речь идёт о деньгах или важных аккаунтах (например, на Госуслугах). Завершите разговор и уточните информацию в банке или сервисе по официальному номеру или через приложение;

- никогда не сообщайте секретные коды (коды из SMS и PUSH-уведомлений нужны только для входа или подтверждения операций. Сотрудники банков и сервисов их не запрашивают — это конфиденциальная информация);

- осторожно относитесь к звонкам с неизвестных номеров (если почувствовали давление или просьбы срочно что-то сделать – положите трубку. Если речь идет о взаимодействии с ОКФС, сотрудниками правоохранительных органах – не отвечайте, а перезвоните сами по известным телефонам горячих линий.

- проверяйте источник звонка или сообщения (даже если звонок или сообщение пришло от знакомого, это может быть дипфейк или взломанный аккаунт. Свяжитесь с человеком через другой канал и уточните, действительно ли он звонил или писал);

- не переходите по ссылкам. Не открывайте ссылки из сообщений в соцсетях и мессенджерах. Лучше вручную ввести адрес сайта в строке браузера или найти его через поиск;

- имейте несколько номеров. Используйте один номер для личных нужд, а другой — для банков и государственных порталов. Это снижает риск утечек (номер, привязанный к важным сервисам, обычно нигде не используется и реже попадает в открытые базы. Если на него поступит подозрительный звонок или сообщение, это сразу вызовет сомнение).

Конечно, это не полный перечень рекомендаций для клиентов ОКФС, и чтобы снизить риск попадания под влияние мошеников необходимо постоянно повышать свой уровень финансовой грамотности. Банк России и поднадзорные ОКФС проводят большую работу по разработке различных памяток, предупреждений (не говоря уже о внедрении новых антифродовых решений), но люди должны сами привыкнуть, что интернет – это, в

первую очередь, не доверенная среда и любое сообщение не должно восприниматься как указание к действию, а подвергаться сомнению. Только ежедневная внимательность и критическое отношение к любой подозрительной информации смогут обезопасить денежные средства клиентов ОКФС.

Заключение / Conclusion

Таким образом, фишинг продолжает оставаться одной из значимых угроз для кредитно-финансовой сферы. При этом современный фишинг превратился в высокотехнологичную индустрию, использующую искусственный интеллект для автоматизации и повышения эффективности атак. Вместе с тем развиваются сервисы, предоставляющие готовые решения для организации подобных атак, что делает их проведение доступным даже для технически неподкованных злоумышленников.

Кроме того, опасность фишинга обусловлена тем, что он эксплуатирует психологические особенности человека: подверженность внушению, склонность к фантазированию, доверчивость. Свою роль играет и нахождение человека в состоянии тревожности или стресса, которое снижает критичность восприятия и делает его более уязвимым.

Необходимо отметить, что противодействие фишингу представляет собой непрерывный процесс, требующий от ОКФС внедрения современных антифрод-решений, а от их клиентов — сохранения бдительности и критического отношения к любой входящей информации из интернета. Без формирования у пользователей привычки к критическому восприятию поступающих сведений технические меры не смогут полностью устранить угрозу. Дальнейшие исследования в этой области должны быть направлены на создание комплексных моделей защиты, сочетающих технологические антифрод-решения и системное повышение цифровой грамотности населения.

Список источников

1. Кибербезопасность в условиях электронного банкинга. Практическое пособие / под ред. П. В. Ревенкова. — М.: Издательство «Прометей», 2020. — 520 с.
2. Хакерские атаки на финсектор в 2026 году: рост сложности и новых угроз [Электронный ресурс] // Коммерсантъ. — 2026. — URL: https://www.kommersant.ru/doc/8606569 (дата обращения: 30.06.2026).

3. Ревенков, П. В. Фишинговые схемы в банковской сфере: рекомендации пользователям интернета по защите и разработка задач регулирования / П. В. Ревенков, К. Р. Ошманкевич, А. А. Бердюгин // Финансы: теория и практика. — 2021. — Т. 25, № 6. — С. 212–226.
4. Ревенков, П. В. Управление киберрисками: участие руководителя кредитной организации в обеспечении ее кибербезопасности / П. В. Ревенков, А. А. Бердюгин, А. Г. Чебарь // Банковское дело. — 2022. — № 8. — С. 52–59.
5. Ревенков П. В., Бердюгин А. А. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания // Национальные интересы: приоритеты и безопасность. — 2017. — Т. 13, № 9. — С. 1747–1760.
6. Медяник О. В., Низовских Н. А. Общение с жертвами финансового внушения: учебно-методические рекомендации и практикум для банковских сотрудников / Москва: Литрес, 2025. — 118 с.
7. Щербатых, Ю. В. Не дайте себя обмануть! / Ю. В. Щербатых. — Санкт-Петербург : Питер, 2024. — 446 с.
8. Aleroud, A.; Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. Computers & Security, 68, 160–196. doi:10.1016/j.cose.2017.04.006
9. Steinmetz K. F. The Identification of a Model Victim for Social Engineering: A Qualitative Analysis // Victims & Offenders. — 2020.
10. Обзор операций, совершённых без добровольного согласия клиентов финансовых организаций [Электронный ресурс] // Центральный банк Российской Федерации. — 2025. — URL: https://cbr.ru/analytics/ib/operations_survey/2025/ (дата обращения: 30.06.2026).
11. CICADA8 предупредила о волне фишинговых атак на популярные российские сервисы [Электронный ресурс] // CICADA8. — 2026. — URL: https://cicada8.ru/news/v-cicada8-nazvali-klyuchevye-kiberugrozy-dlya-rossiyan-v-1-kv-2026 (дата обращения: 30.06.2026).
12. Как мошенники крадут деньги и данные клиентов известного маркетплейса [Электронный ресурс] // Kaspersky Daily. — URL: https://www.kaspersky.ru/blog/marketplace-scam-russia/33931/ (дата обращения: 30.06.2026).
13. ИИ-фишинг и дипфеки: как искусственный интеллект помогает киберпреступникам [Электронный ресурс] // Anti-Malware.ru. —

URL: https://www.anti-malware.ru/analytics/Technology_Analysis/How-AI-Amplifies-Phishing-Attacks (дата обращения: 30.06.2026).

14. Ревенков, П. В. Кибермошенничество в кредитно-финансовой сфере : учебное пособие / П. В. Ревенков, И. В. Ожеред, К. Р. Ошманкевич ; Финансовый университет при Правительстве Российской Федерации. — Москва : Прометей, 2023. — 108 с.

List of sources

1. Cybersecurity in the context of electronic banking. A practical guide / edited by P. V. Revenkov. - Moscow: Prometheus Publishing House, 2020. - 520 p.

2. Hacker attacks on the financial sector in 2026: growing complexity and new threats [Electronic resource] // Kommersant. - 2026. - URL: https://www.kommersant.ru/doc/8606569 (date of access: June 30, 2026).

3. Revenkov, P. V. Phishing schemes in the banking sector: recommendations for internet users on protection and development of regulatory tasks / P. V. Revenkov, K. R. Oshmankevich, A. A. Berdyugin // Finance: Theory and Practice. — 2021. — Vol. 25, No. 6. — P. 212–226.

4. Revenkov, P. V. Cyber Risk Management: Participation of the Head of a Credit Institution in Ensuring Its Cybersecurity / P. V. Revenkov, A. A. Berdyugin, A. G. Chebar // Banking. — 2022. — No. 8. — P. 52–59.

5. Revenkov P. V., Berdyugin A. A. Social Engineering as a Source of Risks in the Context of Remote Banking Services // National Interests: Priorities and Security. — 2017. — Vol. 13, No. 9. — P. 1747–1760.

6. Medyanik, O. V., Nizovskikh, N. A. Communication with Victims of Financial Scams: Training and Methodological Recommendations and a Workshop for Bank Employees / Moscow: Litres, 2025. 118 p.

7. Shcherbatykh, Yu. V. Don't Let Yourself Be Fooled! / Yu. V. Shcherbatykh. St. Petersburg: Piter, 2024. 446 p.

8. Aleroud, A.; Zhou, L. (2017). Phishing Environments, Techniques, and Countermeasures: A Survey. Computers & Security, 68, 160–196. doi:10.1016/j.cose.2017.04.006

9. Steinmetz, K. F. The Identification of a Model Victim for Social Engineering: A Qualitative Analysis // Victims & Offenders. — 2020.

10. Review of transactions carried out without the voluntary consent of clients of financial institutions [Electronic resource] // Central Bank of the Russian Federation. — 2025. — URL: https://cbr.ru/analytics/ib/operations_survey/2025/ (date of access: June 30, 2026).

11. CICADA8 warned of a wave of phishing attacks on popular Russian services [Electronic resource] // CICADA8. — 2026. — URL: https://cicada8.ru/news/v-cicada8-nazvali-klyuchevye-kiberugrozy-dlya-rossiyan-v-1-kv-2026 (date of access: June 30, 2026).

12. How fraudsters steal money and data from clients of a well-known marketplace [Electronic resource] // Kaspersky Daily. — URL: https://www.kaspersky.ru/blog/marketplace-scam-russia/33931/ (date of access: 30.06.2026).

13. AI Phishing and Deepfake: How Artificial Intelligence Helps Cybercriminals [Electronic resource] // Anti-Malware.ru. — URL: https://www.anti-malware.ru/analytics/Technology_Analysis/How-AI-Amplifies-Phishing-Attacks (date of access: 30.06.2026).

14. Revenkov, P. V. Cyberfraud in the Credit and Financial Sphere: a study guide / P. V. Revenkov, I. V. Ozhered, K. R. Oshmankevich; Financial University under the Government of the Russian Federation. — Moscow: Prometey, 2023. — 108 p.