МЕЖДУНАРОДНЫЙ КООРДИНАЦИОННЫЙ СОВЕТ БАНКОВСКИХ АССОЦИАЦИЙ (МЕЖДУНАРОДНЫЙ БАНКОВСКИЙ СОВЕТ)

INTERNATIONAL COORDINATION COUNCIL OF BANKING ASSOCIATIONS (INTERNATIONAL BANKING COUNCIL)

Открытое заседание
Международного Координационного
Совета банковских ассоциаций
(Международный Банковский Совет, МБС)

СБОРНИК АНАЛИТИЧЕСКИХ МАТЕРИАЛОВ

Социальная инженерия.
Способы борьбы с мошенниками.

г. Сочи
25 сентября 2024 г.

ОГЛАВЛЕНИЕ

АССОЦИАЦИЯ БАНКОВ АЗЕРБАЙДЖАНА

Раздел 1

Результаты работы Экспертной группы по борьбе с мошенничеством Ассоциации банков Азербайджана

За последние годы в Азербайджанской Республике на фоне стремительной цифровизации банковского сектора наблюдается рост случаев мошенничества.

Особенно участились случаи мошенничества с использованием механизмов социальной инженерии (social engineering), фишинга (phishing), а также захвата данных учетной записи (account takeover) посредством вышеуказанных методов.

Основной спектр мошеннических транзакций составляют следующие сценарии:

1. Рекламирование фишингового ресурса (URL) с контентом «лотерейная акция/кампания/выигрыш от имени банка», через социальные сети вроде Instagram, Facebook и т.д.;
2. Звонки клиентам от имени банка, Центробанка и т.д.;
3. «Оплата штрафов ПДД со скидкой», «пополнить баланс номера 2x», «покупка билетов в кино» и т.д.;
4. Сообщения через WhatsApp или iMessage с контентом «проблема с доставкой посылки, неверный адрес, для завершения оплаты перейти по URL...».

Также отдельная категория, которую нельзя включить в перечень социальной инженерии или фишинга – это Финансовые Пирамиды или Схемы Понци.

В ответ на эту тенденцию Ассоциацией банков Азербайджана была создана «Экспертная группа по борьбе с мошенничеством в сфере цифровых платежей».

Краткий отчет о работе, проделанной Экспертной группой

1. **Разработка плана проекта на основе 7 Общих Принципов**. Экспертная группа разработала проект, включающий 7 общих принципов, направленных на эффективную борьбу с мошенничеством. Ключевые принципы включают:

- «Рамки деятельности»;

- «Распределение полномочий»;
- «Функциональные возможности Программного Обеспечения»;
- «Управление сценариями мониторинга»;
- «Организация мониторинга и отчетности в формате 24/7»;
- «Организация оценки рисков мошенничества (Fraud Risk Assessment)»;
- «Организация коммуникации».

2. **Организация эффективной коммуникации между членами Ассоциации**. Экспертная группа разработала формат эффективного взаимодействия между членами Ассоциации, а именно банками. В рамках обмена информацией осуществляется выявление и анализ трендовых случаев мошенничества, подготовка рекомендаций и плана действий на краткосрочную и долгосрочную перспективу, а также организация встреч и согласование общей стратегии.

В долгосрочной перспективе планируется расширить сотрудничество между МВД (Министерство внутренних дел Азербайджана), СГБ (Службой государственной Безопасности Азербайджана), СФМ (Службой финансового мониторинга Азербайджана) и другими госучреждениями.

3. **Экспертные заключения по нормативным актам**. Были представлены экспертные заключения по следующим нормативным актам:

- Правила применения усиленной аутентификации клиентов (GMA tətbiqi Qaydaları). Были рассмотрены такие стандарты и практики как, European Council Payment Services Directive 2 (PSD2), Strong Customer Authentification standart (SCA), MFA (Multi-Factor Authentication standart), а также планируется рассмотреть документ «Обеспечение безопасности финансовых сервисов при проведении дистанционной идентификации и аутентификации» (Центробанк Российской Федерации, от 28.02.2024) и т.д.;
- Закон «О платежных услугах и платежных системах» (Ödəniş xidmətləri və Ödəniş sistemləri haqqında Qanun);
- Правила проведения платежных операций и использования платежных инструментов (Ödəniş Aləti Qaydaları).

4. **Разрабатываются политики и процедуры рекомендационного характера**:

- «Политика по борьбе с мошенничеством» (Rəqəmsal Fırıldaqçılığa qarşı mübarizə üzrə Siyasət);

- «Процедура организации 24/7 мониторинга подозрительных операций» (Şübhəli əməliyyatların 24/7 monitorinqi);
- «Процедура управления сценариями мониторинга» (Monitorinq ssenarilərin idarə edilməsi proseduru).

5. **Запуск проекта по созданию Централизованной системы противодействия мошенничеству при Центробанке Азербайджана**. В рамках проекта планируется реализация следующих сервисов:
- Информирование Центрального банка о случаях мошенничества в режиме реального времени (case-by-case Reporting);
- Создание централизованного «черного списка» для физических лиц и предпринимателей;
- Внедрение централизованного реестра скоринга для торговцев (Merchant);
- Оптимизация предоставления квартальной отчетности о мошеннических транзакциях в Центробанк (rüblük ÖS-11 hesabatlığın optimizasiyası).

6. **«Предоставление услуг по Anti-Fraud» членам Ассоциации банков Азербайджана**, включает в себя следующие услуги:
- Программное обеспечение для борьбы с мошенничеством;
- Услуга мониторинга в формате 24/7;
- Услуга управления правилами (Rule Management);
- Оценка рисков мошенничества (Fraud Risk Assessment);
- Услуга ECOM Screening и Merchant Onboarding.

7. **ABA Academy**:
- Видеоуроки на основе подписки;
- Проведение тренингов на местах для членов Ассоциации;
- Организация конкурсов по Anti-Fraud;
- Проведение лекций для университетов;
- «Тренинги по повышению осведомленности» (Awareness trainings).

Эти меры направлены на повышение безопасности и устойчивости банковского сектора Азербайджана в условиях растущих угроз цифрового мошенничества.

Раздел 2

Динамика показателей развития банковского сектора Азербайджанской Республики

№ п/п	Наименование показателя	Ед. изм. (в нац. валюте)	01.05.24	01.07.24
1.	Количество действующих кредитных организаций (КО)	ед.	23	23
2.	Количество КО с иностранным участием	ед.	9	9
2.1	- в т.ч. со 100% долей иностранного капитала	ед.	5	5
3.	Количество филиалов действующих КО	ед.	480	486
4.	Собственные средства (капитал) КО	миллион манат	6323,9	6241,8
5.	Активы КО - всего	миллион манат	49221,6	50328,1
5.1	- ссудная задолженность - всего	миллион манат	24644,5	25429,5
5.1.1	- в т.ч.просроченная	%	1,8%	1,7%
5.2	-кредиты, предоставленные физическим лицам	миллион манат	11168,09	11554,68
5.3	- кредиты нефинансовым организациям	миллион манат	13476,4	13874.8
6.	Пассивы КО - всего	миллион манат	42897,7	44086,3
6.1	депозиты физических лиц	миллион манат	13210,4	13880,3
6.2	Привлеченные кредитными организациями ресурсы на межбанковском рынке	миллион манат	4966,5	5690,1
7.	Финансовый результат банковского сектора	миллион манат	407,5	614
8.	Минимальный размер капитала для действующих кредитных организаций	миллион манат	50	50
9.	Ставка рефинансирования (ключевая ставка) Национального Банка	%	7,5	7,25
	Справочно:			
10.	Валовой внутренний продукт	миллион манат	38181,9	59520,4
11.	Курс национальной валюты к доллару США		1,7	1,7

АССОЦИАЦИЯ БЕЛОРУССКИХ БАНКОВ

Раздел 1

Способы борьбы с кибермошенниками в банковском секторе Республики Беларусь

С учетом быстро развивающейся в Республике Беларусь IT-индустрии банковским сектором достигнуты высокие результаты по расширению цифровизации взаимодействия банков и их клиентов, банков и государственных органов.

Сегодня физические и юридические лица имеют круглосуточный доступ к широкому спектру финансовых услуг, в том числе банковских, посредством удаленных каналов взаимодействия снижена стоимость услуг для населения, расширен круг пользователей финансовых услуг. Банковские и финансовые услуги выведены на качественно иной уровень предоставления.

Вместе с тем масштабное внедрение цифровых финансовых технологий создает возможности для увеличения случаев несанкционированных платежных операций, мошеннических действий и киберугроз. Их подавляющее большинство связано с использованием методов социальной инженерии, когда человек под психологическим воздействием добровольно переводит денежные средства или сообщает злоумышленникам свои конфиденциальные данные (вишинг), либо когда злоумышленники с использованием интернет-мошенничества получают доступ к конфиденциальным данным пользователей (фишинг).

В целях предупреждения, выявления и противодействия несанкционированным платежным операциям Национальным банком и банками реализуется комплекс мер, в том числе информационно-профилактических.

Действенным инструментом по реализации указанных целей является автоматизированная система обработки инцидентов Национального банка Республики Беларусь (далее – АСОИ).

Организация работы АСОИ регулируется постановлением Правления Национального банка Республики Беларусь от 15 декабря 2023 г. № 454 «О предоставлении информации об инцидентах и нарушениях безопасности в сфере защиты информации». Посредством данной системы банки, НКФО, ОАО «Банк развития Республики Беларусь» в качестве поставщиков платежных услуг, а также правоохранительные органы представляют информацию о совершенных операциях либо попытках совершения несанкционированных переводов денежных средств (электронных денег),

фактах или попытках мошенничества в банковском секторе (далее – инциденты), а также о нарушениях безопасности и защиты информации, в том числе компьютерных атаках, направленных на объекты информационной инфраструктуры, которые могут привести к случаям и (или) попыткам осуществления несанкционированных переводов денежных средств (электронных денег).

При представлении в АСОИ указанной информации поставщики платежных услуг руководствуются информационной технологией о порядке предоставления информации об инцидентах и нарушениях безопасности в сфере защиты информации, разработанной Национальным банком, в которой регламентируются состав, форма и форматы информационного взаимодействия и определяются типы инцидентов и перечень информации о них. Кроме того, регулятором выработаны и направлены в банки и НКФО рекомендации по применению выявления признаков совершения перевода денежных средств (электронных денег) без согласия пользователя платежной услуги.

Механизм взаимодействия выстроен таким образом, что позволяет не только получать информацию от поставщиков платежных услуг о совершенных инцидентах, но и оперативно предотвращать дальнейший вывод денежных средств (электронных денег) в случае несанкционированного их списания.

Так, Указом Президента Республики Беларусь от 29 августа 2023 г. № 269 «О мерах по противодействию несанкционированным платежным операциям» предусматривается:

- осуществление информационного обмена об инцидентах между поставщиками платежных услуг (ППУ) и правоохранительными органами посредством АСОИ;
- обязанность финансовых организаций обеспечить проверку совершения платежей на соответствие признакам несанкционированного перевода денежных средств (электронных денег);
- предоставление Генеральной прокуратуре, Комитету государственной безопасности, Следственному комитету и Министерству внутренних дел права на принятие решения о приостановлении на срок до 10 суток расходных операций по банковскому счету, счету по учету вкладов (депозитов), электронному кошельку пользователя платежных услуг, являющегося участником инцидента, в отношении которого у названных правоохранительных органов имеется информация (подозрения), свидетельствующая о его участии в совершении противоправных деяний.

Работа банковского сообщества по приостановлению несанкционированных платежных операций регулируется постановлением Правления Национального банка Республики Беларусь от 15 декабря 2023 г. № 453 «О несанкционированных переводах денежных средств (электронных денег)».

В настоящее время к АСОИ подключены 32 ППУ (включая все банки и НКФО), а также Министерство внутренних дел и Следственный комитет.

Механизм взаимодействия выстроен таким образом, что позволяет не только получать информацию от ППУ о совершенных инцидентах, но и оперативно предотвращать дальнейший вывод денежных средств (электронных денег) в случае несанкционированного их списания.

Так, за март - июль 2024 г. получено и проанализировано 8 899 сообщений о несанкционированных платежных операциях, попытках их совершения и выявленных поддельных сайтах поставщиков платежных услуг и других организаций, в том числе фишинговой направленности (далее - инциденты), а также о нарушениях безопасности в сфере защиты информации. Из общего количества поступивших сообщений 99,0% составляют инциденты и 1,0% - нарушения безопасности в сфере защиты информации.

Всего за текущий период зарегистрировано 8 808 инцидентов, сумма ущерба клиентам банков составила 26,6 млн. руб. Банками приостановлено 3 287 переводов на сумму 3,8 млн. руб. (14,3% от всей суммы ущерба за вышеуказанный период).

Также в целях обеспечения безопасности совершения платежей в каналах ДБО и сети Интернет и минимизации рисков клиентов банки применяют:

- фрод-мониторинг карточных операций, в том числе мониторинг IP-адресов, с использованием которых осуществляется доступ к СДБО;
- установление ограничений на суммы операций и предоставление клиентам возможности самостоятельного управления лимитами по карточкам;
- в дополнение к сеансовому ключу направление на номер мобильного телефона клиента кода подтверждения операции при осуществлении определенных операций либо платежей в СДБО с целью подтверждения операции в сумме, превышающей определенный банком лимит;
- голосовую авторизацию расходных операций в СДБО на сумму, превышающую установленный лимит белорусских рублей;
- предоставление пользователям СДБО возможности самостоятельного управления типами аутентификации;
- оформление договоров добровольного страхования карточек.

Кроме того, Национальным банком совместно с банками на постоянной основе осуществляется комплекс мероприятий по установлению и блокировке фишинговых сайтов, который включает в себя регулярный мониторинг информации в сети интернет на предмет выявления ресурсов, web-дизайн которых идентичен дизайну официального сайта системы «Интернет-банкинг» банка, выявление неправомерного использования бренда (использование зарегистрированного товарного знака и его элементов), поддельных аккаунтов (групп) в социальных сетях и мессенджерах, поддельных мобильных приложений;

Одним из распространённых видов мошенничества продолжает оставаться схема с кредитами, которые клиенты самостоятельно оформляют, а затем переводят кредитные денежные средства в адрес мошенников.

С учетом наличия данного вида мошенничества Национальным банком и банками принимается широкий спектр мер, направленных на их предупреждение (профилактику), в частности банки:

- до заключения кредитного договора информируют под подпись заявителей – физических лиц, обратившихся в банк за получением кредита, в том числе посредством систем дистанционного банковского обслуживания, о формах и методах мошенничества со стороны третьих лиц;
- осуществляют заключение кредитного договора не ранее рабочего дня, следующего за днем обращения (заявления) заявителя – физического лица за получением кредита, или предоставление кредита не ранее рабочего дня, следующего за днем заключения кредитного договора, кроме случаев перечисления денежных средств юридическим лицам и индивидуальным предпринимателям на отплату товаров (работ, услуг), для приобретения которых предоставляется кредит;
- при анализе сведений, содержащихся в кредитном отчете заявителя-физического лица, учитывают информацию о количестве запросов пользователей кредитной истории на получение кредитного отчета в отношении данного физического лица, поступивших в течение семи календарных дней, предшествующих дню его обращения за получением кредита.

Данные рекомендации позволяют заявителю, кредитополучателю еще раз оценить необходимость получения кредита и принять взвешенное решение.

Кроме того, в целях принятия дополнительных мер, направленных на ограждение физических лиц от оформления на их имя кредитов мошенническим путем, Национальный банк рекомендовал банкам при заключении кредитных договоров с использованием программно-аппаратных

средств и технологий применять факторы свойства объекта – биометрические данные клиентов (фото- и видеоизображение, голос) в качестве одного из аутентификационных факторов. В настоящее время кредитные учреждения находятся в процессе внедрения в свою практику метода биометрической идентификации.

Среди законодательных мер, направленных на предотвращение случаев мошеннических действий со стороны третьих лиц при предоставлении кредитов, необходимо выделить следующие:

1. В Инструкцию о формировании кредитных историй и предоставлении кредитных отчетов, утвержденную постановлением Правления Национального банка Республики Беларусь от 22 августа 2018 г. № 291, внесены изменения, в соответствии с которыми:

- с 1 сентября 2023 г. источники формирования кредитной истории предоставляют информацию о заключенной кредитной сделке в Кредитный регистр на следующий рабочий день после ее оформления;
- с 4 июля 2023 г. дополнительно к сведениям о количестве запросов пользователей за последние 7, 30 дней и за весь период включены сведения о количестве пользователей, от которых поступил запрос на получение кредитного отчета субъекта кредитной истории, за последние 3, 30 и 180 дней.

2. Постановлением Правления Национального банка Республики Беларусь от 26 декабря 2023 г. № 488 утверждена в новой редакции Инструкция о порядке предоставления денежных средств в форме кредита и их возврата (погашения).

В ней закреплена возможность приостановления начисления процентов банком в случае, если в отношении кредитополучателя третьими лицами совершены мошеннические действия при предоставлении кредита. Так, в соответствии с пунктом 27 Инструкции начисление процентов за пользование кредитом может быть приостановлено или прекращено банком в том числе при наличии постановления (определения) органа, ведущего уголовный процесс, о признании кредитополучателя потерпевшим в результате хищения, в том числе путем модификации компьютерной информации, мошенничества и др.

3. Принят Закон Республики Беларусь от 1 апреля 2024 г. № 362-З «Об изменении Закона Республики Беларусь «О кредитных историях». Закон предусматривает возможность установления физическим лицом запрета на предоставление пользователям кредитной истории его кредитного отчета. Данные положения направлены на повышение уровня защищенности граждан от мошеннических действий, а также на предотвращение недобросовестного использования кредитных отчетов пользователями кредитных историй.

4. В настоящее время Национальным банком подготовлен проект Закона Республики Беларусь «О потребительском кредите (микрозайме)», который содержит ряд положений, направленных на дальнейшее повышение уровня информированности и защиты прав потребителей финансовых услуг, а также обеспечение более качественного оказания услуг при осуществлении кредитования (микрофинансирования).

В свою очередь, кроме мер, предусмотренных на законодательном уровне для снижения рисков мошенничества при кредитовании населения, банки активно используют такие инструменты обеспечения безопасности предоставляемых услуг, как:

- запрос цифрового изображения заявителя, который держит в руках документ, удостоверяющий личность, открытый на последней странице;
- запрет на удаленное изменение номера мобильного телефона клиента (предоставление возможности выполнения данного действия только при обращении клиента в подразделение банка);
- видеоидентификация клиента путем сканирования страниц паспорта и записи видео, в котором клиент сообщает информацию о ФИО и желании заключить кредитный договор;
- установление запрета оформления заявки на кредит и (или) заключения кредитного договора в банке по заявлению клиента;
- аутентификация клиента с помощью Межбанковской системы идентификации, которая включает в себя сличение фото заявителя с биометрическим шаблоном;
- установление лимитов на вывод кредитных денежных средств путем совершения 2р2-переводов и осуществления операций через ЕРИП;
- телефонные звонки потенциальным кредитополучателям с целью подтверждения факта самостоятельного оформления ими заявки на кредит в каналах ДБО и (или) телефонной верификации, а также направления SMS-сообщения, содержащего проверочный код.

Таким образом, Национальный банк и банки принимают все доступные превентивные меры, направленные на минимизацию рисков мошенничества, а также на регулярной основе проводят информационно-просветительскую работу по повышению уровня цифровой грамотности населения.

2 раздел

Динамика показателей развития банковского сектора Республики Беларусь

№ п/п	Наименование показателя	Ед. изм. (в нац. валюте)	01.01.24	01.07.24
1.	Количество действующих кредитных организаций (КО)	ед.	21	21
2.	Количество КО с иностранным участием	ед.	14	14
2.1	- в т.ч. со 100% долей иностранного капитала	ед.	2	2
3.	Количество филиалов действующих КО	ед.		2487 структурных подразделений
4.	Собственные средства (капитал) КО	млн рублей	19 766,5	20 875,0
5.	Активы КО - всего	млн рублей	112 542,3	
5.1	- ссудная задолженность - всего	млн рублей	65 607,1	69 633,1
5.1.1	- в т.ч.просроченная	млн рублей	223,8	359,0
5.2	-кредиты, предоставленные физическим лицам	млн рублей	18 169,5	19 288,5
5.3	- кредиты нефинансовым организациям	млн рублей	47 437,6	50 344,6
6.	Пассивы КО - всего	млн рублей	112 569,2	120 802,0
6.1	депозиты физических лиц	млн рублей	26 634,5	27 650,0
6.2	Привлеченные кредитными организациями ресурсы на межбанковском рынке	млн рублей	2 121,4	
7.	Финансовый результат банковского сектора	млн рублей	1,1	
8.	Минимальный размер капитала для действующих кредитных организаций	млн рублей	60	60
9.	Ставка рефинансирования (ключевая ставка) Национального Банка		9,5%	9,5%
	Справочно:			
10.	Валовой внутренний продукт	млн рублей	97,6	157,2
11.	Курс национальной валюты к доллару США		3,28	3,18

АССОЦИАЦИЯ БАНКОВ РЕСПУБЛИКИ КАЗАХСТАН

Раздел 1

Социальная инженерия. Способы борьбы с мошенниками

В связи с активным развитием цифровых сервисов и повсеместным переходом на безналичные способы осуществления расчетов наблюдается рост мошеннических операций и несанкционированный доступ к чувствительной информации. Все чаще для подобных деяний используются методы социальной инженерии (сообщения от «знакомых» об одолжении денег, звонки от «службы безопасности банка» и др.), когда человек, не подозревая, предоставляет злоумышленникам банковские, личные и конфиденциальные данные. При слове «кибербезопасность» большинство думает о том, как защититься от хакеров, использующих технические уязвимости сетей. Но есть и другой способ проникнуть в организации и сети – используя человеческий фактор. Это и есть социальная инженерия: способ обманом заставить кого-то раскрыть информацию или предоставить доступ к сетям данных. Например, мошенник, притворяясь сотрудником службы поддержки, может попросить пользователей сообщить их пароли. Удивительно, как часто люди добровольно выдают эти данные, особенно если им кажется, что запрос поступает от уполномоченного лица. Иначе говоря, в случае социальной инженерии мошенники манипулируют людьми, чтобы получить от них информацию или доступ к ней.

Социальная инженерия включает в себя широкий спектр кибератак, направленных на использование доверчивости людей или их ошибок для получения доступа к некоторой информации или сервисам. Пользователей могут убедить предоставить доступ к системам или открыть определенные документы, файлы, электронные письма или веб-сайты. Злоумышленники, полагаясь на человеческий фактор применяют разные формы манипуляций, технологий и пр.

В 2023 году 44 тысячи казахстанцев потеряли от действий мошенников в общей сложности 140 миллиардов тенге по данным из Генпрокуратуры РК. При этом все чаще преступники используют интернет-технологии и цифровизацию (фишинг, брашинг, дипфейки, социальная инженерия, телефонное мошенничество и т.п.). Министерством внутренних дел Республики Казахстан принят ряд организационных и практических мер, направленных на предупреждение и раскрытие мошеннических схем социальной инженерии. В связи с ростом мошенничеств с использованием IP-телефонии, совместно с Министерством цифрового развития и операторами

связи выработаны технические меры по блокированию фрод-звонков. Это позволило в значительной мере сократить количество телефонных мошенничеств от имени якобы сотрудников банков, когда граждане под их убеждением переводили мошенникам свои сбережения, оформляли кредиты. Проведены встречи с представителями финансового сектора. Совместно с банками второго уровня будут реализованы дополнительные меры по обеспечению сохранности счетов граждан и пресечению оформления нелегитимных кредитов, в т.ч. по оперативному взаимодействию с полицией. Проводится обширная работа по информированию населения о мерах предосторожности. С операторами связи заключены меморандумы о противодействии фрод-звонкам. В целях противодействия интернет-мошенничествам стране внедрен проект «Киберпол», пилот реализован в рамках исполнения поручения Главы Государства и масштабирован по всем регионам. Основной акцент сделан на усиление взаимодействия с другими госорганами, финансовыми учреждениями и частным сектором. Реализуется комплекс мер, направленных на выявление и раскрытие таких преступлений, а также задержание организаторов и соучастников. Во всех регионах созданы и действуют специализированные группы «Киберпол» по расследованию интернет-мошенничеств. Большинство интернет-мошенничеств, связанных с оформлением на граждан кредитов и займов, а также хищением их банковских накоплений, совершаются «зарубежными преступниками». Они входят в состав транснациональных ОПГ, работающих по принципу «Call-центров», с постоянной дислокацией в странах ближнего и дальнего зарубежья.

В рамках проекта успешно внедрена система блокировки «зарубежных» звонков с подменных номеров, используемых мошенниками. Это позволило пресечь свыше 43 млн. попыток таких соединений, вследствие чего, количество пострадавших сократилось более чем в 2,5 раза. Сотрудники напрямую взаимодействуют с банками и операторами сотовой связи. Это позволяет снизить риски потери гражданами своих денег. Таким образом на стадии вывода за пределы страны заблокировано порядка 220 млн. тенге, а также обеспечено возмещение ущерба на сумму 850 миллионов. Эффект работы «Киберпола» весьма ощутим: уже раскрыто более 3 тыс. таких преступлений. Для борьбы с подобными махинациями МВД Казахстана, предлагает принять следующие меры:

- исключить авторизацию на сайте по номеру иностранного оператора или информировать интернет-посетителей о размещении объявлений из-за рубежа;

- начать применение биометрической идентификации зарегистрированных в маркет-плейсах предпринимателей при совершении онлайн-операций (получение, перевод, снятие денег), что позволит гарантировать получение денежных средств за товары и услуги исключительно самими предпринимателями;
- обязать владельцев сайтов установить антифрод-системы для выявления IP-адресов, с которых размещены одинаковые подозрительные объявления;
- установить ответственность за содействие в выводе похищенных денег, а также за передачу посторонним лицам банковских карт и абонентских номеров;
- ввести ответственность предпринимателей за передачу третьим лицам своих личных кабинетов в банковских приложениях;
- ввести лицензирование интернет-телефонии.

В целях выявления и пресечения проведения мошеннических операций, эффективной борьбы с интернет-мошенничеством, телефонным мошенничеством, противостояния международным мошенническим преступным группам и предотвращения социальной инженерии регулятором финансового рынка совместно с правоохранительными органами и участниками финансового рынка предпринимаются различные превентивные меры. В частности, реализован Проект по созданию Антифрод-центра по обмену данными о мошеннических транзакциях. Создание Антифрод-центра на базе АО «Национальная платежная корпорация Национального Банка Республики Казахстан» предусматривает сбор и обработку данных по платежам и переводам денег с признаками мошенничества; консолидацию «черных» списков в формате единого API для последующей передачи субъектам финансового рынка; сбор, хранение и обмен информацией об инцидентах мошенничества на финансовом рынке и передачу информации о платежных транзакциях с признаками мошенничества в органы внутренних дел. К платформе Антифрод-центра подключены финансовые организации, операторы сотовой связи и правоохранительные органы. Антифрод-центр создан для противодействия мошенническим операциям, а также позволяет финансовым организациям выявлять и блокировать мошеннические транзакции, оперативно реагировать на операции с признаками мошенничества, обмениваться информацией в режиме реального времени между его участниками. Работа Антифрод-центра предусматривает также ведение единой базы данных по мошенническим операциям. С момента запуска платформы финансовыми организациями и правоохранительными органами установлено около 400 инцидентов по мошенническим операциям и

заблокированы средства на сумму порядка 30 миллионов тенге, связанные с мошенническими действиями. Дальнейшее развитие Антифрод-центра включает в себя расширение технологической функциональности с помощью открытых программных интерфейсов (API) и автоматизации бизнес-процессов. Планируется применение технологий искусственного интеллекта для повышения эффективности выявления подозрительных транзакций. Национальный Банк также в целях предупреждения потенциальных мошеннических действий информирует, что сотрудники и представители Антифрод-центра никогда не совершают звонки физическим лицам с целью сбора информации или проведения каких-либо операций. В рамках своей деятельности Антифрод-центр не взаимодействует с физическими лицами, а работает только с финансовыми, платежными организациями, правоохранительными органами и сотовыми операторами.

Наиболее используемые злоумышленниками виды социальной инженерии

Взлом

Схема действий мошенников: Злоумышленники взламывают страницы в социальных сетях и рассылают от имени владельца аккаунта фишинговые сообщения с просьбой от имени владельца странички занять или перевести некоторую сумму либо с целью выманивания реквизитов банковских платежных карточек, а также паролей для проведения в дальнейшем мошеннических операций.

Способы защиты: При обращении родственников/друзей/знакомых через социальные сети с просьбами о помощи в переводе денежных средств на карточку/оплаты мобильной связи, билетов и т.д. необходимо убедиться, что лицо, обратившееся через страницу социальной сети, является именно тем, за кого себя выдает. Наряду с номером и сроком действия карточки, логином и паролем от интернет-банкинга, паролем 3-D Secure и SMS-паролем (ключом), также не следует сообщать CVV2/CVC2-код (трехзначное число на обороте карточке), данный код используется исключительно для расходных операций и не нужен для перевода денежных средств на банковскую карту. В случае, если аккаунт пользователя в социальных сетях был взломан, ему необходимо по возможности оповестить об этом подписчиков страницы и сменить пароль.

Вишинг

Схема действий мошенников: Злоумышленники используют телефонные звонки с целью выманивания у держателей банковских

платежных карт личной информации, номера банковской платежной карты, логина и пароля от систем дистанционного банковского обслуживания, SMS-кодов и др. Мошенники могут представляться работниками банка или сотрудниками Службы сервиса клиентов ОАО «Банковский процессинговый центр», использовать скрытые телефонные номера или программы-анонимайзеры, подменяющие номера телефонов на реальные номера, размещенные на официальных ресурсах организаций.

Способы защиты: Важно помнить, что работники банков или сотрудников Службы сервиса клиентов никогда не запрашивают информацию о номере банковской платежной карты, сроке ее действия, CVC/CVV код, пароль 3D Secure, одноразовый подтверждающий код. Во время телефонного разговора важно не сообщать собеседнику информацию о реквизитах банковской карты, логины и пароли, SMS-коды, информацию о сеансовых ключах к Интернет-банкингу и мобильным приложениям. В случае поступления подобных телефонных звонков необходимо срочно обратиться в банк по номерам телефонов, указанным на официальном сайте.

Мошенничество при осуществлении сделок на интернет-площадках

Схема действий мошенников: Продавец размещает информацию о продаже товара на общедоступной площадке. Чаще всего внимание мошенников привлекают объявления о продаже дорогостоящего имущества (бытовая техника, мебель, автомобили). Мошенники под видом покупателей связываются с продавцом и просят предоставить им реквизиты банковской платежной карты для осуществления предоплаты либо сами предоставляют мошенническую ссылку для перевода денежных средств. Используя полученную информацию (зачастую держатели карточек разглашают не только номер карты, но и CVV2/CVC2- код, а также пароли 3D Secure) злоумышленники переводят деньги с карточки жертвы на свои карточки (телефонные счета, электронные кошельки и пр.).

Существует также другая схема, в рамках которой покупатель обращается к продавцу, который на самом деле является мошенником, по вопросу приобретения того или иного товара, после чего мошенник просят произвести предоплату путем перевода средств с карточки на карточку или электронный кошелек. Получив деньги, мошенник перестает выходить на связь.

Способы защиты: При покупке товаров и услуг у незнакомых людей или на интернет-площадках необходимо обращать внимание на форму оплаты. Если покупка товара возможна только по предоплате, есть основания предполагать, что это преступная схема. В этом случае не следует переводить

оплату за предоставляемые товар или услугу на банковскую пластиковую карту продавца или его электронный кошелек.

Сообщения о выигрыше ценных призов

Схема действий мошенников: Злоумышленники рассылают сообщения о выигрыше ценных призов и провоцируют потенциальную жертву перевести на счет некую сумму денег для получения «приза» или участия в розыгрыше и объясняют это тем, что ему нужно оплатить комиссию, таможенную пошлину, налоги либо транспортные расходы для доставки «выигрыша».

Способы защиты: Для того, чтобы не стать жертвой мошенников, необходимо получить от организаторов розыгрыша максимально возможную информацию об акции, условиях участия в ней и правилах ее проведения. Также гражданину необходимо вспомнить, принимал ли он участие в розыгрыше призов и знакома ли ему организация, направившая уведомление о выигрыше? Кроме того, необходимо учитывать, порядок уплаты налогов за выигрыш в лотерею регламентирован действующим законодательством, в этой связи уплата налогов не осуществляется посредством перевода денежных средств на электронные счета граждан и организаций или электронные кошельки.

Способы защиты от социальной инженерии

Одним из наиболее эффективных способ защиты от действий мошенников является повышение уровня осведомленности граждан, что позволяет им правильно вести себя во время диалога с мошенниками и вовремя закончить разговор, не раскрыв свои персональные данные.

Важно также учитывать, что действия мошенников зачастую направлены на дестабилизацию эмоционального состояния жертвы, поэтому при возникновении негативных эмоций (страх, тревога, раздражение) во время телефонного звонка необходимо прекратить разговор, чтобы успокоиться, и затем перезвонить собеседнику самостоятельно – в банк по номеру телефона, указанном на официальном сайте или на банковской карте, звонившему родственнику и пр.

2 раздел

Динамика показателей развития банковского сектора Республики Казахстан

№ п/п	Наименование показателя	Ед. изм. (в нац. валюте)	01.01.24	01.04.24	01.07.24
1	Количество действующих кредитных организаций (КО)	единиц	21	21	21
2	Количество КО с иностранным участием	единиц	12	11	11
2.1	в т.ч. со 100% долей иностранного капитала	единиц	8	8	8
3	Количество филиалов действующих КО	единиц	262	261	261
4	Собственные средства (капитал) КО	млрд. тенге	6 860,5	7 511,5	7 490,5
5	Активы КО - всего	млрд. тенге	51 440,0	52 923,4	55 323,0
5.1	Ссудная задолженность - **всего**	млрд. тенге	29 853,7	30 282,9	31 967,1
5.1.1	в том числе: *просроченная (свыше 90 дн.)*	млрд. тенге	*863,8*	*928,7*	*987,7*
5.2	Кредиты физическим лицам	млрд. тенге	16 698,2	17 554,3	18 348,5
5.3	Кредиты юридическим лицам	млрд. тенге	12 472,1	12 400,0	13 158,5
5.3.1	в том числе: *кредиты малому бизнесу*	млрд. тенге	*7651,0*	*7 553,5*	*8214,4*
5.4	Кредиты банкам и организациям, осуществляющим отдельные виды банковских операций	млрд. тенге	137,3	133,1	165,5
5.5	Операции «Обратное РЕПО»	млрд. тенге	546,1	195,7	294,6
6	Пассивы КО - всего	млрд. тенге	44 579,5	45 411,9	47 832,5
6.1	Вклады клиентов, всего	млрд. тенге	35 090,7	35 772,1	37 458,5
6.1.1	в том числе: - *депозиты физических лиц* - *депозиты юридических лиц* - *текущие счета физических лиц* -*текущие счета юридических лиц*	млрд. тенге млрд. тенге млрд. тенге млрд. тенге	17 166,0 8 904,0 3 239,3 5 781,4	17 426,5 10 412,3 2 857,8 5 075,5	18 429,5 10 162,5 3 258,7 5 607,8
6.2	Межбанковские вклады	млрд. тенге	467,6	634,1	783,4

6.3	Займы, полученные от других банков и организаций, осуществляющих отдельные виды банковских операций	млрд. тенге	548,0	437,9	489,8
6.4	Займы, полученные от Правительства Республики Казахстан	млрд. тенге	728,8	728,5	750,8
6.5	Займы, полученные от международных финансовых организаций	млрд. тенге	85,2	84,5	90,6
6.6	Выпущенные в обращение ценные бумаги	млрд. тенге	2 822,8	2 792,1	2 726,1
6.7	Операции «РЕПО» с ценными бумагами	млрд. тенге	1 850,1	2 050,3	2 500,9
6.8	Прочие обязательства	млрд. тенге	2 946,3	2 912,2	3 032,4
7	Финансовый результат банковского сектора	млрд. тенге	2 183,1	569,5	1 156,6
8	Минимальный размер капитала для действующих кредитных организаций	млрд. тенге	10,0	10,0	10,0
	Справочно:				
9	Базовая (ключевая) ставка НБРК	% годовых	15,25	14,75	14,25
10	Валовой внутренний продукт за год	млрд. тенге	113 825,0 (оценка)	113 825,0 (прогноз)	124 414,0 (прогноз)
11	Курс национальной валюты к доллару США	тенге	454,56	446,78	471,46

СОЮЗ БАНКОВ КЫРГЫЗСТАНА

Раздел 1

Социальная инженерия. Способы борьбы с мошенниками

Социальная инженерия — это форма психологического манипулирования людьми с целью получения конфиденциальной информации, доступа к системам или выполнения определенных действий, которые выгодны злоумышленнику. Это одна из самых эффективных и распространенных тактик в арсенале киберпреступников, поскольку она направлена на слабое звено в системе безопасности — человеческий фактор.

Борьба с социальной инженерией требует комплексного подхода, который включает в себя обучение, технические меры, разработку политик и процедур, а также создание культуры безопасности. Важно понимать, что успешная защита зависит от осведомленности и активного участия всех пользователей и сотрудников организации.

В Кыргызстане в части регулирования IT и информационной безопасности Национальным банком Кыргызской Республики разработаны нормативные акты - Положение НБКР «О минимальных требованиях по управлению операционным риском в коммерческих банках Кыргызской Республики» и Положение НБКР «О требованиях по обеспечению информационной безопасности в коммерческих банках Кыргызской Республики». Данные нормативные акты включают в себя требования, предъявляемые к коммерческим банкам и другим финансово-кредитным организациям, как для осуществления безопасной деятельности самих организаций, так и безопасного сохранения персональных данных клиентов организаций. Министерством цифрового развития Кыргызской Республики в настоящее время разрабатывается Цифровой кодекс Кыргызской Республики, который также будет охватывать данный вопрос.

В последнее время в стране участились случаи следующих видов социальной инженерии:

- фишинг (метод, при котором злоумышленники отправляют ложные электронные письма или сообщения, чтобы обманным путем заставить получателя раскрыть конфиденциальную информацию, такую как пароли или данные банковских карт). Так, посредством мессенджера WhatsApp к гражданам поступали сообщения от якобы Служб безопасности коммерческих банков о предоставлении номеров и CVV кодов платежных карт для проверки. На электронную почту граждане получали сообщения с некой

ссылкой (например, www.[название бренда].id4007.kg), которая ведет на форму для заполнения личных данных. Предлоги были разные: нужно получить денежный перевод из-за границы или получение крупного выигрыша;

- вишинг (телефонные звонки от мошенников, представляющихся сотрудниками компаний или служб поддержки с целью получения конфиденциальной информации). Представляясь банковскими сотрудниками, мошенники запрашивали конфиденциальные данные по счетам и/или платежным картам клиентов банка. Мошенники стали активно использовать видеосвязь через мессенджеры WhatsApp и Telegram для звонков, представляясь сотрудниками банка. Мошенники, действуя через видеосвязь, предлагали клиентам оформить кредитную заявку, сменить доверенный номер телефона, перевести деньги на «безопасный счет» или просили предоставить СМС-коды под различными предлогами для получения доступа в личный кабинет клиента банка. Мошенники посредством видеозвонков через мессенджеры просили подключить демонстрацию экрана своего смартфона. В случае предоставления такого доступа мошенники видели все данные телефона, в том числе персональные коды, которые приходят от банка в SMS для подтверждения финансовых операций или входа в личный кабинет, чем и воспользовались, похитив все денежные средства на счетах клиента. В Кыргызстане наблюдается усиление активности мошенников, которые представляются или предъявляют поддельные документы сотрудников Национального банка с целью получения доступа к средствам граждан. В мае-июне месяцах текущего года прокатилась волна новой схемы мошенничества – мошенники, имитируя голос близких родственников, сообщали, что попали в ДТП и необходимо срочно передать через курьера/водителя Яндекс-такси определенную сумму денег. Жертвами таких мошенников подавляющее большинство составили граждане пенсионного возраста;
- смишинг (фишинг через текстовые сообщения (SMS), которые содержат вредоносные ссылки или просьбы предоставить личные данные). Через мессенджер Telegram ко многим гражданам от их знакомых поступали сообщения с просьбой проголосовать за племянника/сына/дочь в каком-либо конкурсе пройдя по такой-то ссылке. Впоследствии, мошенники, получая доступ к данным граждан, похищали денежные средства. Также были случаи, когда граждане получали сообщения от друга или родственника с просьбой одолжить деньги под любым предлогом с указанием номера карты. Граждане, не перепроверив, делали перевод на карты мошенников.

В связи с указанными выше фактами, в настоящее время правоохранительные государственные органы, Национальный банк

Кыргызской Республики, коммерческие банки, операторы мобильной связи на регулярной основе посредством интернет СМИ и социальных сетей проводят населению разъяснительные и предупреждающие компании. Основные рекомендации для населения следующие:

- ни при каких условиях не передавать третьим лицам свои персональные данные, номера банковских карт, коды и СМС;
- не переходить по непроверенным интернет-ссылкам, особенно если они требуют ввода личных данных;
- воздерживаться от ответов на видеозвонки с незнакомых номеров в мессенджерах. Никогда не включать трансляцию экрана, так как это может привести к утечке конфиденциальной информации.
- избегать активных телефонных разговоров с незнакомцами;
- чтобы голос гражданина не был использован для подтверждения финансовых операций, стараться слушать незнакомцев молча, не вступать в дискуссию и не произносить слова «да» и «подтверждаю»;
- проявлять бдительность и перепроверять информацию.

Союз банков Кыргызстана, в свою очередь, регулярно организовывает тематические мероприятия для обсуждения дальнейших перспектив развития банковского и финансового сектора. Так, в октябре 2023 года проводилась Финансовая конференция «FinConference2023: Будущее финансов: Инновации и Трансформация», на которой рассматривались ситуация по дальнейшему развитию децентрализованных финансов и блокчейн технологий, вопросы кибербезопасности и платежных инструментов, а также повышения потенциала финансового сектора посредством образовательных программ и другие вопросы дальнейшего развития финансового рынка. В текущем году в мае было проведено ежегодное крупное финансовое мероприятие «Бишкекский Международный Финансовый Форум 2024» (BIFF2024) с темой «Финтех и Устойчивое развитие: Будущее финансов». Пленарная и сессионные дискуссии форума предусматривали обзор мировых и региональных трендов, обсуждение вопросов дальнейшего развития финансовых, платежных и государственных технологий, безналичных платежей, цифровых активов, искусственного интеллекта, кибербезопасности, устойчивого финансирования зеленых проектов, а также вопросы, связанные с развитием Исламских принципов финансирования. Кроме того, на базе Учебного центра Союза банков Кыргызстана регулярно проводятся треннинги и семинары на темы информационной и кибербезопасности.

Раздел 2

Динамика показателей развития банковского сектора Кыргызской Республики

№ п/п	Наименование показателя	Ед. изм. (в нац. валюте)	01.05.24	01.07.24
1.	Количество действующих кредитных организаций (КО)	Ед.	23	21
2.	Количество КО с иностранным участием	Ед.	13	12
2.1	- в т.ч. со 100% долей иностранного капитала	Ед.	6	5
3.	Количество филиалов действующих КО	Ед.	316	305
4.	Собственные средства (капитал) КО	млрд сом	104,3	110,0
5.	Активы КО - всего	млрд сом	678,2	727,3
5.1	- ссудная задолженность - всего	млрд сом	268,9	281,1
5.1.1	- в т.ч.просроченная	млрд сом	7,0	7,2
5.2	-кредиты, предоставленные физическим лицам	млрд сом	92,7	100,1
5.3	- кредиты нефинансовым организациям	млрд сом	176,2	181,0
6.	Пассивы КО - всего	млрд сом	573,9	618,3
6.1	депозиты физических лиц	млрд сом	176,0	184,3
6.2	Привлеченные кредитными организациями ресурсы на межбанковском рынке	млрд сом	2,2	3,2
7.	Финансовый результат банковского сектора	млн сом	8 355,1	14 158,8
8.	Минимальный размер капитала для действующих кредитных организаций	млн сом	600	800
9.	Ставка рефинансирования (ключевая ставка) Национального Банка	%	11	9
	Справочно:			
10.	Валовой внутренний продукт	млрд сом	341,7	559,7
11.	Курс национальной валюты к доллару США	сом (за 1 доллар США)	88,6821	86,4454

АССОЦИАЦИЯ БАНКОВ РОССИИ

Раздел 1

Социальная инженерия. Способы борьбы с мошенниками

Вопросы кибербезопасности прочно вошли в число наиболее обсуждаемых тематик в банковском секторе. Особая значимость информационной безопасности и защиты данных подчеркивается на уровне высшего руководства страны. Такое пристальное внимание вызвано значительными показателями ущерба от киберпреступлений. По оценкам МВД России, в 2023 году он достиг 156 млрд рублей.

По результатам опроса Банка России, в 2023 году 40% респондентов[1] сталкивались с разными видами финансового мошенничества, при этом 10% лишились денег. Количество людей, которым звонили или писали злоумышленники, увеличилось. Чаще всего на уловки мошенников попадались:

- городские жители (75,4%)
- женщины (55,5%);
- люди в возрасте от 25 до 44 лет (37,8%);
- люди со средним уровнем образования (41,3%) и средним достатком (44,8%).

По данным Банка России, в 2023 году было совершено почти 1,2 млн операций без согласия клиента (+33,0% по сравнению с 2022 годом) на сумму 15,8 млрд рублей (+11,5% по сравнению с 2022 годом). За этот же период доля возмещенных средств возросла с 4,4% до 8,7%.

По результатам опроса Банка России, 64% респондентов теряет сумму до 20 тыс. рублей. Треть таких пострадавших даже не заявляют о мошенничестве. До 100 тыс. рублей теряет 18% респондентов, а со значительными хищениями на суммы свыше 1 млн рублей столкнулись лишь 4,3% опрошенных.

[1] Было опрошено 395 381 физическое лицо.

В 2024 году продолжился рост мошенничества. По итогам I полугодия 2024 года количество (551 тыс.) и объем (9,0 млрд руб.) операций без согласия превысили среднеквартальные значения за последние 4 квартала.

В объеме операций без согласия физических лиц наибольшую долю (47%) стабильно занимают операции по банковским картам. В этом году доля хищений через СБП (30%) впервые превысила долю мошенничества по счетам (через дистанционное банковское обслуживание и переводы) – 22%.

Основным каналом мошенничества, по информации Банка России, остаются телефонные звонки или СМС-сообщения (54%[2]). По экспертным оценкам, в России совершается порядка 20 млн мошеннических звонков ежедневно. На фоне принимаемых операторами сотовой связи мер, направленных на противодействие мошенническому трафику, ряд атак ушел в мессенджеры (22,5%). Иные способы взаимодействия: социальные сети (9,8%), электронная почта (7,2%), поддельные сайты (4,8%) и приложения (1,7%) остаются не столь популярными.

При этом 87,6% респондентов при взаимодействии со злоумышленниками не поддавались на их уловки и не совершали никаких действий. Среди 12,4% опрошенных, которые верили мошенникам, наиболее популярными действиями были перевод сбережений злоумышленникам (15,3%), передача кода из СМС (15,3%) и данных банковской карты (14,8%). В этой связи особую важность приобретает не только защита клиентских данных, но и препятствование успешной коммуникации мошенника с потенциальной жертвой усилиями мобильных операторов и других провайдеров связи.

Помимо телефонного мошенничества растет и фишинг[3]. За 2023 год, по информации компании Bi.Zone, в России число мошеннических сайтов

[2] С учетом ответов всех контактировавших с мошенниками респондентов.

[3] Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. 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 поддельной странице свои логин

выросло на 86% и достигло 207,1 тыс. штук. А в январе-июне 2024 года доля писем с вредоносными ссылками в корпоративном почтовом трафике выросла более чем вдвое по сравнению со средним уровнем 2023 года. Из каждых 100 писем как минимум одно оказывалось фишинговым.

С прошлого года кредитные организации направляют в Банк России информацию об объеме предотвращенных хищений денежных средств. За прошедший год он составил 5,8 трлн рублей. Благодаря эффективной работе банковского антифрода злоумышленникам не удалось совершить 34,8 млн мошеннических операций. В этом году банками предотвращено 30,2 млн таких операций на сумму более 4,3 трлн рублей.

Растет и финансовая грамотность населения: 86,2% опрошенных Банком России физических лиц помнят о правилах безопасности при контакте с мошенниками. Совсем не знают о таких правилах только 4% респондентов.

В целях противодействия мошеннической активности законодателями и Банком России разрабатываются регуляторные меры. С 25 июля 2024 года вступил в силу закон[4], направленный на повышение эффективности существующих антифрод-процедур:

– Банки обязаны приостанавливать на два дня переводы, если информация о получателе денег содержится в базе данных[5] Банка России. Такой «период охлаждения» поможет клиенту обдумать свои действия и понять, что он находился под влиянием мошенников. В противном случае кредитной организации придется вернуть клиенту деньги в течение 30 календарных дней.

– Перевод будет приостанавливаться даже в том случае, когда клиент настаивает на нем или пытается совершить его повторно во время

и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

[4] Федеральный закон от 24.07.2023 № 369-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе».

[5] База данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, в которой содержатся в том числе сведения о совершенных мошеннических операциях, о плательщиках и получателях таких денежных средств. Сведения этой базы доводятся до банка-отправителя и банка-получателя платежа, и они, в свою очередь, будут обязаны использовать эту информацию в своих антифрод-системах.

двухдневного периода охлаждения. Но если спустя два дня клиент все-таки решит сделать перевод на этот же подозрительный счет, то банк обязан незамедлительно исполнить такое поручение и финансовую ответственность за это нести не будет.

– Банки обязаны отключать доступ к дистанционному обслуживанию клиентам, которые занимаются выводом и обналичиванием похищенных денег. Их платежные инструменты будут блокироваться, если от правоохранительных органов поступили сведения об участии человека в мошеннической схеме.

Результаты применения новых норм законодательства можно будет оценить в начале 2025 года, когда будет сформирована достаточная статистическая база по предотвращенным операциям без согласия.

Принимая во внимание развитие кредитного мошенничества (по информации ПАО Сбербанк, 30% всех мошеннических звонков связанно именно с таким видом хищений), необходимо проработать эффективные механизмы противодействия мошенничеству при выдаче гражданам необеспеченных кредитов наличными. Такая мера позволит клиентам выйти из-под психологического влияния мошенника и предотвратить хищение заемных средств.

Получать похищенные деньги мошенникам помогают специальные люди – дропперы – они обналичивают в банкоматах банковские карты и передают полученные деньги мошенникам за вознаграждение. По данным исследования ПАО Сбербанк, как правило, это молодые мужчины, их средний возраст – 26 лет. Дропперов довольно легко выявить по камерам, их нередко ловят.

В настоящее время Уголовным кодексом Российской Федерации установлена ответственность до 7 лет лишения свободы, однако с учетом масштабов преступлений явно назрела необходимость усиления уголовной ответственности за такое правонарушение, установленной статьей 187 «Неправомерный оборот средств платежей» Уголовного кодекса Российской

Федерации. Такая мера снизит привлекательность продажи банковской карты мошенникам для использования ее в качестве дропперской.

Кроме того, целесообразно предоставить возможность обращаться в суды с требованиями имущественного характера к дропперам. Для этого предлагается разрешить банкам передавать потерпевшим данные потенциального мошенника, необходимые для обращения в суд (ФИО, место жительства, дата и место рождения). В настоящее время такие сведения составляют банковскую тайну и не могут быть переданы лицу, пострадавшему от мошеннических действий. Имущественная ответственность способна быть превентивным фактором, который позволит снизить участие граждан в дроперской деятельности.

Одним из наиболее важных направлений повышения эффективности противодействия мошенничеству является развитие информационного обмена между всеми заинтересованными участниками: кредитными организациями, операторами связи, регуляторами (Банк России, Минцифры России, МВД России, Роскомнадзор), а также иными организациями, обладающими полезными сведениями для борьбы с преступниками (например, Единый регулятор азартных игр и Единый портал государственных услуг Российской Федерации). Повышение скорости передачи информации о мошеннических реквизитах, схемах обмана и выявленных преступлениях позволит оперативно принимать необходимые меры и не допускать хищений.

Еще одним направлением в противодействии финансовому кибермошенничеству должна стать борьба с фишингом. Сейчас основными препятствиями в России являются:

– отсутствие формальных нормативных правовых оснований для блокировки некоторых фишинговых сайтов;

– длительные процедуры блокировки, превышающие реальный срок активности фишингового ресурса;

– отсутствие централизованной площадки для противодействия фишингу с участием государственных органов и коммерческих игроков рынка.

Централизованной площадкой для борьбы с фишингом могла бы стать информационная система мониторинга фишинговых сайтов (ИС Антифишинг) Минцифры России, которая предназначена для автоматизации и повышения эффективности процессов сбора, систематизации, обработки, анализа и хранения сведений о фишинговых ресурсах и фишинговой активности на территории Российской Федерации. При этом важно максимально расширить нормативное определение фишинга, чтобы позволить регуляторам блокировать максимальное количество ресурсов.

Для активизации борьбы с фишингом необходимо продолжить работу над законопроектом Минцифры России, направленным на закрепление механизма оперативного межведомственного взаимодействия при ограничении доступа к выявленным фишинговым ресурсам.

Наконец, необходимо активизировать процессы повышения финансовой грамотности, чтобы люди не попадались на удочку мошенников и социальных инженеров. В последнее время помимо телефонного мошенничества активное развитие получают направления, связанные с инвестициями. По данным Банка России, около половины всех выявленных схем приходится на компании с признаками финансовых пирамид, порядка 30% — на нелегальных кредиторов, остальные — на нелегальных форекс-дилеров. В этой связи важно подойти к вопросу повышения финансовых знаний граждан максимально комплексно.

Этому будет способствовать систематическая актуализация содержания федеральных программ, направленных на повышение финансовой грамотности и осведомленности населения о мошеннических действиях, с учетом постоянного развития платежных инструментов, финансовых технологий и сценариев мошенничества и привлечение к просветительской

деятельности крупнейших СМИ, образовательных учреждений и популярных лидеров мнений.

О защите прав потребителей финансовых услуг при совершении противоправных действий сотрудником кредитной организации.

Совершение работником проступка в отношении клиентов банка и / или в отношении самого банка несет для банка риски финансовых потерь и потери деловой репутации. При этом умышленные действия работников финансовых организаций, направленные, например, на присвоение ценностей, подделку подписей клиентов на документах о поручении совершить те или иные операции, в настоящее время не рассматриваются в качестве однократного грубого нарушения, являющегося основанием для расторжения работодателем трудового договора. Так, в случае, когда работник действует во вред организации или ее клиентам, его можно уволить только по сокращению штата либо по собственному желанию, в отдельных случаях в связи с утратой доверия. Таким образом, в настоящее время у кредитной организации фактически отсутствуют инструменты, позволяющие защитить интересы клиентов и свои собственные непосредственно при совершении сотрудником нарушения, так и от повторения им таких действий в будущем, в том числе посредством отстранения сотрудника на период проведения служебного расследования.

Представляется необходимым устранить выявленный правовой пробел, путем внесения изменений в Федеральный закон от 02.12.1990 № 395-I «О банках и банковской деятельности», предусматривающие возможность увольнения в случае совершениями ими действий (бездействий), повлекших причинение ущерба кредитной организации и / или её клиентам, либо создавших реальную угрозу его причинения.

Раздел 2

Динамика показателей развития банковского сектора Российской Федерации

№ п/п	Наименование показателя	Ед. изм. (в нац. валюте)	01.05.24	01.08.24
1.	Количество действующих кредитных организаций (КО)	ед.	356	355
2.	Количество КО с иностранным участием	ед.	96 (01.01.2024)	96 (01.01.2024)
2.1	- в т.ч. со 100% долей иностранного капитала	ед.	44 (01.01.2024)	44 (01.01.2024)
3.	Количество филиалов действующих КО	ед.	407	395
4.	Собственные средства (капитал) КО[6]	трлн руб.	15,0	14,6
5.	Активы КО - всего	трлн руб.	175,1	180,6
5.1	- ссудная задолженность - всего	трлн руб.	115,6	121,0
5.1.1	- в т.ч.просроченная	%	3,6	3,5
5.2	-кредиты, предоставленные физическим лицам	трлн руб.	35,4	37,3
5.3	- кредиты нефинансовым организациям	трлн руб.	65,2	68,0
6.	Пассивы КО - всего	трлн руб.	175,1	180,6
6.1	депозиты физических лиц	трлн руб.	32,0	33,4
6.2	Привлеченные кредитными организациями ресурсы на межбанковском рынке	трлн руб.	19,9	18,6
7.	Финансовый результат банковского сектора	трлн руб.	1,2	2,2
8.	Минимальный размер капитала для действующих кредитных организаций	млрд руб.	1 млрд руб. – для банков с универсальной лицензией; 300 млн руб. – для банков с базовой лицензией	
9.	Ставка рефинансирования (ключевая ставка) Национального Банка	%	16,00	18,00
	Справочно:			
10.	Валовой внутренний продукт[7]	трлн руб.	32,2 (1 кв. 2024 г.)	66,9[8] (1-2 кв. 2024 г.)
11.	Курс национальной валюты к доллару США	руб./долл.	91,7791	86,1091

[6] Балансовый капитал
[7] В постоянных ценах 2021 г.
[8] Расчет на основе данных по индексу физического объема ВВП.

АССОЦИАЦИЯ БАНКОВ УЗБЕКИСТАНА

Раздел 1

Социальная инженерия. Способы борьбы с мошенниками

В последние годы расширяется цифровой сектор экономики страны, стремительно развиваются ключевые драйверы его роста — платформы электронной коммерции и цифровые сервисы, а также финансовые технологии, связанные с качественной и безопасной обработкой осуществляемых платежей на маркетплейсах и цифровых сервисах.

Вместе с тем увеличение за последнее время случаев кражи или мошенничества с использованием банковских карт свидетельствует о недостаточности цифровой финансовой грамотности населения и квалификации сотрудников правоохранительных органов, об отсутствии современных систем предупреждения правонарушений в коммерческих банках и платежных организациях, у операторов платежных систем.

В Постановлении Президента Республики Узбекистан №381 «О мерах по усилению защиты прав потребителей цифровой продукции (услуг) и борьбы с правонарушениями, совершаемыми посредством цифровых технологий» уделено особое внимание задаче по внедрению транзакционной антифрод системы у операторов платежных систем, сессионных антифрод систем в банках и платежных организациях и централизованной антифрод системы в самом Центральном банке Республики Узбекистан.

В целях своевременного пресечения краж, мошенничества и других правонарушений Центральный банк уполномочен направлять обязательные указания коммерческим банкам, операторам платежных систем и платежным организациям о временном ограничении использования на срок до трех дней банковских карт, банковских счетов и счетов на мобильных приложениях в случае осуществления сомнительных (фрод) операций, связанных с банковскими картами.

Центральный банк страны получил право на блокировку банковских карт и счетов при подозрительных операциях, разработал комплекс мер по совершенствованию методов технической защиты при оказании гражданам онлайн-услуг коммерческими банками, операторами платежных систем и платежными организациями и внедрение систем, программных комплексов для предотвращения мошеннических транзакций.

Согласно статистике МВД, количество преступлений, совершенных с помощью информационных технологий в Узбекистане за последние 3 года выросло в 10,3 раза, составив 8,5% от общего числа преступлений.

В свою очередь, Ассоциация банков Узбекистана ежегодно проводит ряд диалогов во всех районах и во многих регионах страны, направленный на повышение цифровой финансовой грамотности населения по предупреждению современных угроз, в частности незаконных операций с банковскими картами (их реквизитами), в том числе посредством электронных платежных систем.

В мае текущего года Ассоциация банков Узбекистана совместно с Советом Ассоциаций Тюркских стран провела конференция на тему «Финансовые тенденции – Финтех и банки, антифрод (борьба с мошенничеством), популяризация Исламского банкинга».

В сессии «Антифрод» спикерами выступали, Руководитель Центра Кибербезопастности, Центральный банк Республики Узбекистан, Менеджер по развитию бизнеса, LexisNexis Risk Solutions, Руководитель отдела расследований мошенничества, OTB Bank Венгрия.

Данная сессия раскрыла эффективность вышеуказанных мер, современное состояние и перспективы защиты финансовых систем от цифровых угроз, характер индустрии платежных карт и стандарты безопасности данных.

Раздел 2

Динамика показателей развития банковского сектора Республики Узбекистан

№ п/п	Наименование показателя	Ед. изм. (в нац. валюте)	01.04.24	01.07.24
1.	Количество действующих кредитных организаций (КО)	ед.	35	35
2.	Количество КО с иностранным участием	ед.	9	9
2.1	- в т.ч. со 100% долей иностранного капитала	ед.	7	7
3.	Количество филиалов действующих КО	ед.	653	614
4.	Собственные средства (капитал) КО	млрд сум	100 713,3	104 157,5
5.	Активы КО - всего	млрд сум	665 656,9	690 424,1
5.1	- ссудная задолженность - всего	млрд сум	478 200,6	493 952,1
5.1.1	- в т.ч.просроченная	млрд сум	21 600,7	20 000
5.2	-кредиты, предоставленные физическим лицам	млрд сум	153 330,0	161 070,9
5.3	- кредиты нефинансовым организациям	млрд сум	324 870,6	332 881,3
6.	Пассивы КО - всего	млрд сум	665 656,9	690 424,1
6.1	депозиты физических лиц	млрд сум	88 531,3	97 248,5
6.2	Привлеченные кредитными организациями ресурсы на межбанковском рынке	млрд сум	59 697,9	61 034
7.	Финансовый результат банковского сектора	млрд сум	2 381,1	5 517,1
8.	Минимальный размер капитала для действующих кредитных организаций	млрд сум	350,0	350,0
9.	Ставка рефинансирования (ключевая ставка) Национального Банка	%	14	14
	Справочно:			
10.	Валовой внутренний продукт	млрд.сум	242 701,6	567 346,3
11.	Курс национальной валюты к доллару США	сум	12 655,0	12 558,32

АССОЦИАЦИЯ БАНКОВ СЕРБИИ

Part 1

Social Engineering and Anti-Fraud Measures in Serbia
Social Engineering Tactics in Serbia

The digital transformation and increasing internet penetration in Serbia have led to a rise in cybercrime, including social engineering attacks. The COVID-19 pandemic further exacerbated this issue, as more people relied on online services for work, education, and social interactions. Cybercriminals have exploited these changes, adapting their tactics to target remote workers and online platforms.

Several high-profile incidents in Serbia have highlighted the severity of social engineering threats. For example, there have been cases of phishing attacks targeting major banks, where fraudsters successfully obtained customer information and siphoned funds from their accounts. Additionally, businesses have reported instances of CEO fraud, where attackers impersonate senior executives to authorize fraudulent transactions.

Anti-Fraud Measures in Serbia

To combat social engineering and other forms of cybercrime, the Republic of Serbia has implemented various anti-fraud measures, involving both the government and the private sector. These measures include legislative frameworks, public awareness campaigns, technological solutions, and international cooperation.

Legislative Frameworks: Serbia has established comprehensive laws and regulations to address cybercrime. The Law on Information Security and the Criminal Code of Serbia provide the legal basis for prosecuting cybercriminals and protecting digital assets. These laws define offenses related to unauthorized access, data breaches, and other cybercrimes, imposing strict penalties on offenders.

Public Awareness Campaigns: The Serbian government, along with non-governmental organizations and private companies, conducts regular public awareness campaigns to educate citizens about the risks of social engineering. These

campaigns aim to teach individuals how to recognize and respond to potential scams, emphasizing the importance of skepticism and verification before sharing personal information.

Technological Solutions: Financial institutions and businesses in Serbia have adopted advanced technological solutions to enhance security. Multi-factor authentication, encryption, and intrusion detection systems are commonly used to protect sensitive data and prevent unauthorized access. Additionally, many organizations conduct regular security training for their employees to ensure they are aware of the latest threats and best practices.

International Cooperation: Serbia collaborates with international organizations and neighboring countries to combat cybercrime. The country is a member of the Council of Europe's Convention on Cybercrime (Budapest Convention), which facilitates international cooperation in investigating and prosecuting cybercrimes. This cooperation is crucial for addressing cross-border cyber threats and sharing best practices.

Social engineering remains a significant threat in the Republic of Serbia, exploiting human psychology to gain access to sensitive information and systems. However, the country has made considerable efforts to combat this threat through legislative measures, public awareness campaigns, technological advancements, and international cooperation. While these efforts have had a positive impact, the evolving nature of cyber threats necessitates continuous vigilance and adaptation. By fostering a culture of cybersecurity awareness and leveraging technological innovations, Serbia can better protect its citizens and businesses from the dangers of social engineering.

Common Social Engineering Tactics detected in Serbia

1. **Phishing**:

Involves sending fraudulent emails that appear to be from reputable sources to trick recipients into revealing personal information, such as passwords and credit card numbers.

2. **Whaling**:

A type of phishing attack that targets high-profile individuals such as executives or key employees within an organization to steal sensitive information or gain access to high-level corporate resources.

3. **Baiting**:

Involves offering something enticing to lure victims into a trap, often using physical media such as infected USB drives to install malware.

4. **Diversion Theft**:

A physical form of social engineering where the attacker tricks a delivery service into diverting a shipment to a different location.

5. **Business Email Compromise (BEC)**:

Involves compromising a business email account through phishing or hacking and then using that account to authorize fraudulent transactions or request sensitive information.

6. **Smishing**:

Involves sending fraudulent text messages that appear to come from reputable sources to trick recipients into revealing personal information or clicking on malicious links.

Association of Serbian banks

Security commetee established in 2014 organized information sharing between their members through closed member only web portal and initate banking customer security awareness section on public web site on which they collect most important information.

Commetee and FIN-CSIRT lately have been acitve supporter of International fraud awareness week since 2017. Tribines, conference and other digital events have been organized

Security commetee evolved in Financial CERT (FIN-CSIRT) registered in accordance with National Law on information security in 2021. Trough FIN-CSIRT different activities have been done:

The Association of Serbian Banks (ASB) plays a critical role in promoting anti-fraud measures and enhancing the security of the financial sector in Serbia. Here are some of the key initiatives and activities undertaken by the ASB:

1. Education and Training

Workshops and Seminars: The ASB organizes regular workshops and seminars focused on fraud prevention and detection. These sessions are designed for bank employees and cover various topics such as identifying fraud schemes, using anti-fraud technologies, and compliance with legal requirements.

International Fraud Awareness Week: The ASB actively participates in International Fraud Awareness Week, organizing events and campaigns to raise awareness among banks and the public about the importance of fraud prevention.

2. Collaboration and Information Sharing

Coordination with Financial CSIRT: The ASB collaborates with the Financial Computer Security Incident Response Team (CSIRT) to share threat intelligence and best practices. This partnership helps in the timely identification and mitigation of fraud risks.

Partnerships with Law Enforcement: The ASB works closely with law enforcement agencies, including the Ministry of Interior, to facilitate the investigation and prosecution of fraud cases.

3. Public Awareness Campaigns

Educational Materials: The ASB produces and distributes educational materials such as brochures, infographics, and videos that explain common fraud schemes and provide tips on how to avoid becoming a victim.

Media Engagement: Engaging with the media to spread awareness about fraud prevention, highlighting the importance of vigilance among consumers and businesses.

4. Regulatory Advocacy

Policy Development: The ASB actively participates in the development of national policies and regulations related to financial fraud. They provide input and

recommendations to ensure that the regulatory framework is robust and effective in combating fraud.

Compliance Support: Assisting member banks in understanding and complying with anti-fraud regulations, including those related to anti-money laundering (AML) and counter-terrorism financing (CTF).

5. Technology and Innovation

Promoting Anti-Fraud Technologies: Encouraging the adoption of advanced technologies such as artificial intelligence and machine learning for fraud detection. These technologies help banks analyze transaction patterns and detect anomalies that may indicate fraudulent activity.

Cybersecurity Initiatives: Implementing cybersecurity measures to protect against cyber-attacks and data breaches that could lead to financial fraud.

6. Networking and Best Practices

Conferences and Forums: Hosting conferences and forums where banking professionals can discuss emerging fraud trends, share experiences, and learn about the latest tools and techniques for fraud prevention.

Best Practice Guidelines: Developing and disseminating guidelines on best practices for fraud prevention and response. These guidelines help banks standardize their approaches to handling fraud incidents.

7. Research and Reporting

Fraud Research: Conducting research on fraud trends and publishing reports that provide insights into the types of fraud affecting the banking sector and the effectiveness of various prevention measures.

Reporting Systems: Establishing systems for banks to report fraud incidents, which helps in tracking and analyzing fraud patterns across the sector.

By implementing these comprehensive measures, the Association of Serbian Banks aims to enhance the security and integrity of the financial system in Serbia, protect consumers, and foster a culture of vigilance and proactive fraud prevention within the banking community.

Government and Institutional Initiatives

1. National CERT of Serbia:

- **Awareness Campaigns**: Regular public awareness campaigns such as "Think Before You Click" to educate citizens on phishing and other social engineering tactics.
- **Training and Simulations**: Conducting training sessions and simulation exercises to improve the incident response capabilities of organizations.

2. **Ministry of Information and Telecommunications**:

- **Cyber Hygiene Initiative**: Promoting safe online behavior and digital hygiene practices through educational programs integrated into school curricula and national media broadcasts.
- **Public Service Announcements**: Disseminating information about the dangers of social engineering through public service announcements and community engagement.

3. Ministry of Interior:

- **Cybercrime Investigations**: Intensifying efforts to investigate and prosecute cybercrime, including social engineering attacks. Collaborative efforts with international law enforcement agencies to tackle cross-border cyber threats.

4. Prosecutor for High-Tech Crime in Serbia

- The Prosecutor for High-Tech Crime in Serbia plays a crucial role in combating cybercrime, including social engineering, fraud, and other forms of digital offenses. This office is responsible for investigating and prosecuting crimes that involve sophisticated technology and cyber tactics.

5. National bank of Serbia

Consumer Protection Initiatives

Financial Consumer Protection Center: The NBS operates a dedicated center for protecting financial consumers. This center handles complaints and disputes between consumers and financial institutions, providing mediation and resolution services.

Public Awareness Campaigns: The NBS runs campaigns to educate the public about their rights and how to protect themselves from financial fraud. These campaigns include informational materials, workshops, and collaborations with other organizations

6. Non-Governmental Organizations (NGOs) in Serbia Covering Cybersecurity and Anti-Fraud Topics

Several non-governmental organizations (NGOs) in Serbia are actively involved in addressing cybersecurity, anti-fraud measures, and the broader scope of digital safety and rights.

Public Security Awareness Campaigns in Serbia

1. Cybersecurity Awareness Month

Organized by: National CERT of Serbia in collaboration with various governmental and non-governmental organizations.

Description: This annual campaign, observed in October, focuses on raising awareness about the importance of cybersecurity. It includes activities such as webinars, workshops, public service announcements, and social media campaigns aimed at educating the public and businesses about online security best practices.

Activities:

- Webinars on safe internet practices
- Workshops for different demographics (students, employees, senior citizens)
- Social media campaigns to spread awareness about phishing, malware, and other cyber threats

Objective: To enhance the overall cybersecurity posture of individuals and organizations by educating them on how to protect their digital lives.

2. Think Before You Click

Organized by: National CERT of Serbia

Description: This campaign aims to educate the public about the dangers of phishing and other social engineering tactics. It focuses on teaching individuals how to recognize fraudulent emails and messages.

Activities:

- Distribution of informative brochures and posters
- Online seminars and workshops
- Social media posts with tips on recognizing phishing attempts

Objective: To reduce the number of successful phishing attacks by increasing public awareness and knowledge.

3. Cyber Hygiene Initiative

Organized by: Ministry of Information and Telecommunications

Description: This initiative promotes safe online behavior and digital hygiene practices. It includes educational programs integrated into school curricula and media broadcasts.

Activities:

- Educational programs in schools and universities
- National television and radio broadcasts
- Development of an online portal with resources for safe internet use

Objective: To instill good cybersecurity habits in the general population, particularly among the youth.

4. Secure Your Digital Identity

Organized by: Financial CSIRT and the Association of Serbian Banks (ASB)

Description: Focuses on protecting individuals' and businesses' digital identities from theft and misuse. This campaign addresses the growing threat of identity theft.

Activities:

- Seminars for financial sector employees
- Informative videos and infographics shared online
- Collaboration with banks to include security tips in customer communications

Objective: To protect digital identities by educating the public and financial sector employees about the risks and prevention methods.

5. Stop. Think. Connect.

Organized by: Ministry of Interior

Description: A global initiative adapted to the Serbian context to promote cybersecurity awareness. It encourages the public to think before they connect to the internet or share personal information.

Activities:

- Public service announcements
- Community sessions in public libraries and community centers
- Creation of a dedicated website with safety tips and tools
- Objective: To promote a culture of cybersecurity awareness and responsible online behavior.
-

Public Anti-Fraud Awareness Campaigns in Serbia

1. International Fraud Awareness Week

Organized by: Association of Certified Fraud Examiners (ACFE) in collaboration with Serbian institutions.

Description: International Fraud Awareness Week is a global campaign that takes place annually in November. It aims to increase awareness about fraud and promote anti-fraud education and training.

Activities:

- Webinars and online seminars for businesses and individuals.
- Distribution of educational materials, including infographics and guides on recognizing and preventing fraud.
- Social media campaigns with shareable images and videos to raise public awareness about various types of fraud.

Objective: To educate the public and organizations on how to detect and prevent fraud, thereby reducing the incidence of fraudulent activities globally and locally in Serbia.

More Info: International Fraud Awareness Week

2. Fraud Awareness Training and Benchmarking Reports

Organized by: ACFE and local financial institutions.

Description: These reports and training programs are designed to provide insights into how organizations conduct fraud awareness training and to benchmark anti-fraud technologies and practices.

Activities:

- Providing detailed guides on setting up effective fraud prevention programs.
- Offering self-study courses and seminars to improve understanding of fraud risks and prevention strategies.
- Publishing case studies and benchmarking reports to help organizations adopt best practices.

Objective: To help organizations understand their fraud risks better and implement effective anti-fraud measures.

3. Stop! Think Fraud Campaign

Organized by: Various Serbian government bodies in partnership with international anti-fraud organizations.

Description: This campaign focuses on providing consistent, clear, and robust anti-fraud advice to the public.

Activities:

- Public service announcements and media campaigns to educate citizens on common fraud schemes.
- Workshops and community meetings to discuss fraud prevention strategies.
- Collaboration with local media to disseminate anti-fraud messages.
- Objective: To reduce the incidence of fraud by educating the public on how to recognize and report fraudulent activities.

4. Regional Anti-Corruption Initiative (RAI)

Organized by: Regional Anti-Corruption Initiative (RAI) in cooperation with Serbian Anti-Corruption Agency.

Description: Aimed at strengthening measures to combat corruption and fraud within the region.

Activities:

- Developing and implementing national anti-corruption strategies and action plans.
- Training sessions for public officials on integrity and anti-corruption measures.
- Public awareness campaigns to highlight the dangers and impacts of corruption and fraud.

Objective: To foster a culture of integrity and transparency within public administration and to increase public trust in governmental institutions.

5. Fraud Conferences and Seminars

Organized by: Various academic and professional bodies in Serbia.

Description: Regular conferences and seminars focusing on different aspects of fraud, including detection, prevention, and technological advancements.

Activities:

- Hosting international and local experts to discuss current trends and challenges in fraud prevention.
- Providing networking opportunities for professionals to share best practices.
- Offering specialized sessions on emerging fraud risks and innovative solutions.

Objective: To keep professionals updated on the latest developments in fraud prevention and to foster a collaborative approach to tackling fraud.

These campaigns and initiatives collectively aim to increase public and organizational awareness about fraud, promote best practices in fraud prevention, and enhance the overall resilience of Serbian society against fraudulent activities.

Part 2

Dynamics of indicators of the banking sector development in Serbia

No.	Indicator name	Measurement unit (in national currency)	01.01.24	01.03.24
1.	Number of operating credit institutions (CIs)		20	20
2.	Number of CIs with foreign participation		15	15
2.1	- incl. with 100% foreign capital		15	15
3.	Number of branches of operating CIs		1.341	1.340
4.	Internal funds (equity) of CIs	In million RSD	817.951	845.295
5.	Total assets of CIs	In million RSD	5.941.240	6.002.783
5.1	- Total outstanding loans	In million RSD	3.921.504	4.032.859
5.1.1	- including overdue	In million RSD	48.146	49.596
5.2	- loans to individuals	In million RSD	1.473.847	1.494.471
5.3	- loans to non-financial organizations	In million RSD	1.688.658	1.655.292
6.	Total liabilities of CIs	In million RSD	5.941.240	6.002.783
6.1	- retail deposits	In million RSD	2.255.752	2.303.163
6.2	Resources attracted by credit institutions in the inter-bank market	In million RSD	576.025	549.828
7.	Financial result (P&L impact) of the banking sector	In million RSD	122.242	43.314
8.	Minimum capital requirement for operating credit institutions	In EUR	10 million	10 million
9.	Key interest rate of the National Bank		6,50%	6%
	For reference:			
10.	Gross domestic product (GDP)	In million EUR	69.521	16.835
11.	Exchange rate of national currency to US dollar	Period average	108,41	107,89

Несмотря на то, что мошенники всегда выбирали банковские счета, как самый быстрый способ получить доступ к денежным средствам, после пандемии COVID–19 количество мошеннических атак резко возросло.

Стоит отметить, что в то время, как подавляющее большинство преступлений в сфере банковского мошенничества за этот период было совершено онлайн (93%, согласно отчету о финансовых преступлениях за 2 квартал 2021 года), доля телефонного мошенничества в общем объеме мошенничества резко возросла с 1% до 7%, что также классифицируется как случаи мошенничества с банковскими счетами, если речь идет о прямом или электронном переводе.

Самые популярные виды мошенничества с банковскими счетами

Ниже будут рассмотрены наиболее распространенные виды мошенничества с банковскими счетами в порядке уменьшения частоты, а также рекомендации по их предотвращению.

Получение доступа к банковскому счету

Согласно вышеупомянутому отчету о финансовых преступлениях, доля мошенничества с захватом доступа к банковским счетам, или так называемый ATO (Account takeover), составляет 42% от общего числа всех банковских мошенничеств. В данном случае мошенники получают доступ к банковскому аккаунту и информации на нем, что позволяет им переводить денежные средства с него на свой собственный счет или постепенно выводить средства с данного банковского аккаунта. Поскольку банковские переводы, в отличие от платежей по картам, необратимы, вернуть средства, похищенные мошенниками в данном случае, крайне сложно.

Подобно всем атакам ATO, блокировка банковского счета происходит вследствие:

- Фишинга. Мошенники проводят массовую рассылку по электронной почте или SMS, которая содержит ссылку, перенаправляющую пользователей на поддельную страницу входа в банк. На данной странице пользователи вводят свои регистрационные данные, в результате чего информация оказывается доступна мошенникам. Мошенники также могут убеждать пользователей отправлять им данные учетной записи напрямую;

- Социальной инженерии. Данный метод получения информации непосредственно от пользователей или из банка становится все более популярным. В данном случае мошенники используют желание банков повысить уровень удовлетворенности клиентов и получают все необходимые данные от службы поддержки;
- Покупка учетных данных. Мошенникам редко удается найти действительные реквизиты банковского счета в даркнете, однако риск получения доступа мошенников к реальным данным из данного источника остается;
- Уязвимости в сфере кибербезопасности. Мошенничество и киберпреступность часто взаимосвязаны. Опытные преступники будут искать существующие уязвимости в системе безопасности, такие как плохо настроенный межсайтовый скриптинг (XSS) или подделка запросов на стороне сервера (SSRF);
- Заполнения учетных данных. Мошенники используют специальное программное обеспечение (ботов) для автоматической проверки паролей и комбинаций логинов для того, чтобы войти в учетную запись. Часто это осуществляется с использованием списков паролей, найденных в даркнете, а также с помощью так называемого брутфорса.

Мошенники могут комбинировать все вышеперечисленные способы, чтобы повысить шансы на успех взлома. Поскольку многие банки теперь используют двухфакторную проверку подлинности (2FA), мошенники также могут использовать SIM-джекинг, чтобы получить контроль над номером телефона и получать пароли по SMS.

Способы предотвращения получения доступа к банковским счетам

Помимо повышения уровня безопасности веб-сайта банка, а также работы с клиентами по обеспечению конфиденциальности их персональных данных, необходимо также разработать системы обнаружения. Например, используя комбинацию скоростных правил, отпечатков устройств и инструментов поиска IP-адресов, возможно получать предупреждения о случаях мошенничества всякий раз, когда:

- пользователь несколько раз подряд вводит неправильный пароль,
- местоположение является подозрительно далеким от домашнего адреса пользователя,
- пользователь входит в систему с совершенно нового устройства,
- подключение осуществляется через VPN, прокси или Tor,

- конфигурация устройства эмулируется программным обеспечением,
- часовой пояс или языковые настройки пользователя не совпадают с изначальными настройками.

Мошенничество, связанное с открытием новых банковских счетов

Наблюдается тенденция роста случаев мошенничества, связанного с открытием новых банковских счетов, на долю которых приходится 23% всех случаев мошенничества с банковскими счетами. Мошенники делают это с помощью комбинации синтетической идентификации, выдачи себя за пользователя и подмены конфигурации.

Мошенничество с открытием счетов особенно распространено среди цифровых банков и банков-претендентов. Эти компании часто жертвуют безопасностью ради удобства открытия счета. Мошенники используют данную уязвимость в своих целях:

- для комбинирования реальных данных с украденными;
- для использования технологий для обхода проверок KYC и IDV;
- для подделывания своей конфигурации в Интернете, чтобы создать впечатление, что они подключаются из правильного места.
-

Способы предотвращения мошенничества с новыми счетами

Как и в случае с получением доступа к аккаунту, большая часть ответственности за предотвращение мошенничества с новыми счетами лежит на самих банках. Если их системы KYC или AML (anti-money laundering – противодействие отмыванию денег) недостаточно эффективны для выявления мошенников, необходимо использовать другие подходы:

- Учитывать иную информацию. Необходимо обращать внимание не только на документы, удостоверяющие личность, но и на цифровой след пользователя, такой как активность в социальных сетях, конфигурация устройства и тип подключения;
- Осуществлять мониторинг транзакций в режиме реального времени. Это ключевая функция борьбы с отмыванием денег, которая также может помочь выявить мошенников, как только они начнут вносить или снимать деньги со своих свежесозданных счетов;
- Отслеживать поведение. В сфере предотвращения мошенничества это делается с помощью скоростных правил. Эти правила рассматривают данные за определенный период времени, что позволяет ответить на следующие вопросы: Как быстро этот пользователь прошел проверку KYC?

Не увеличивает ли данный пользователь свои кредиты с намерением объявить банкротство? Отправляет ли пользователь многочисленные регулярные платежи, которые могут указывать на отмывание денег?

- Использовать системы машинного обучения. Преимущество систем машинного обучения заключается в том, что они способны анализировать огромные объемы данных и предлагать правила оценки рисков на основе выявленных закономерностей. Использование подобных систем может помочь менеджеру по управлению рисками цифровых банков, которые пытаются установить поведенческие связи между мошенниками.
-

Денежные мулы

Денежные мулы – понятие, используемое для обозначения лиц, являющихся сообщниками мошенников. Денежные мулы открывают банковские счета на свое имя с использованием настоящих документов, удостоверяющих личность. Благодаря этому их невозможно вычислить как мошенников, поскольку они успешно проходят все проверки KYC и AML.

Денежные мулы сотрудничают с мошенниками, получая и переводя на их счета деньги, как правило, полученные незаконным путем.

Таким образом, мошенники используют денежных мулов для отмывания денег, получения средств и поддержки других видов незаконной деятельности.

Способы предотвращения случаев мошенничества с денежными мулами

Поскольку денежные мулы попадают под категорию мошенничества с открытием новых счетов, стратегии предотвращения подобных случаев мошенничества аналогичны. Тем не менее, банкам следует уделять особое внимание использованию следующих инструментов:

- использованию машинного обучения, которое позволяет выявить закономерности случаев мошенничества, которые могут быть упущены менеджерами по управлению рисками;
- анализу поведения пользователя с помощью скоростных правил и проверок, что позволит выяснить, как денежные мулы работают на платформе банка;
- анализу социальных сетей и визуализации графиков, поскольку эти методы могут помочь обнаружить связи между счетами, которые могут свидетельствовать о работе организованных групп мулов.

Мошенничество с банковскими или электронными переводами

Количество случаев мошенничества с банковскими переводами настолько возросло, что некоторые страны расценивают его как угрозу национальной безопасности.

Мошенники используют различные способы, чтобы побудить пользователей перевести денежные средства на чужой счет.

Мошенники отправляют сообщения с целью запугивания, которые заставляют пользователя действовать быстро. Мошенники также могут просить заплатить за срочную услугу или выдавать себя за друга или родственника.

Главная проблема заключается в том, что, как только деньги покидают счета пользователей, вернуть их практически невозможно. Более того, в последние годы появилось множество сторонних сервисов, которые утверждают, что могут помочь клиентам вернуть потерянные средства. Некоторые из этих сервисов сами могут оказаться мошенническими.

Способы предотвращения случаев мошенничества с банковскими переводами

Возможности банков по контролю за ситуацией в случае с данным видом мошенничества ограничены. Однако большинство из них теперь показывают уведомления при добавлении нового получателя или инициировании крупного перевода. Кроме того, возможен также мониторинг транзакций в банковской системе с целью отслеживания необычно крупные платежи.

Мошенничество с выдачей себя за банк

В случае с данным видом мошенничества преступники выдают себя за банк. Целью мошеннических действий является получение доступа к личной информации, особенно банковским реквизитам, поэтому данный вид мошенничества относится к мошенничеству с банковскими счетами.

Данный вид мошенничества является не только серьезным риском с точки зрения безопасности, но также может повредить деловой репутации банка и снизить доверие потребителей. В число негативных последствий можно также включить потерю денежных средств, интеллектуальной собственности и нарушение операционной деятельности.

К тому же преступникам становится все проще имитировать корпоративную структуру. Они могут найти в Интернете готовые фишинговые наборы или нанять мошенника для выполнений конкретных действий.

Способы предотвращения случаев мошенничества с выдачей себя за банк

Для предотвращения случаев данного вида мошенничества банкам целесообразно:

- регулярно информировать клиентов о том, какую информацию банк будет/не будет у них запрашивать,
- установить более обширную, многофакторную аутентификацию,
- установить антифишинговые коды.

Последний способ становится все более популярным среди онлайн-компаний. Проще говоря, он позволяет клиентам создать свой собственный код, который будет отображаться в обычных каналах, таких как SMS или электронные письма. Его отсутствие является для пользователя поводом для беспокойства.

Распространенные виды банковского мошенничества

Внедрение технологий в банковское дело обеспечило комфорт и удобство пользователей, с одной стороны, и открыло новые возможности для мошенников, с другой стороны. Виды банковского мошенничества эволюционировали, став более трудными для обнаружения. К числу распространенных видов банковских афер, с помощью которых мошенники ставят под угрозу финансовую безопасность пользователей, относятся:

Фишинговые аферы

Фишинговые аферы – один из самых распространенных методов, с помощью которого мошенники получают доступ к личной и финансовой информации пользователей. Мошенники рассылают электронные письма или тексты от имени банка, клиентом которого является пользователь. Сообщения содержат просьбу подтвердить личную информацию или перейти по ссылке, которая, как правило, ведет на поддельный сайт, который имитирует официальный сайт банка. На поддельном сайте пользователю предлагается ввести конфиденциальные данные, такие как учетные данные для входа в систему, или информацию о кредитной карте. После ввода этих данных информация попадает в базу мошенников.

Аферы с использованием вишинга

Вишинг, или голосовой фишинг, осуществляется по той же схеме, что и фишинговые аферы, но в ходе разговора по телефону. Мошенники, часто выдавая себя за банковского работника, обманом заставляют людей раскрыть конфиденциальную информацию нередко с целью получения финансовой

выгоды. Они используют манипуляции страхом, чтобы склонить пользователя к разглашению конфиденциальной информации, например, аргументируя тем, что счет был взломан и для его защиты необходимо принять срочные меры, а также, чтобы узнать номера счетов, пароли или другие личные данные, которые будут в дальнейшем использованы для доступа к счету пользователя.

Мошенничество с применением спуфинга

Спуфинг – это тактика, используемая в кибермошенничестве, при которой мошенники подделывают электронные сообщения, чтобы создать впечатление, что они исходят от надежных источников. Спуфинг предполагает также подделку заголовков электронной почты и идентификационных данных абонентов с целью того, чтобы обманом заставить получателей раскрыть конфиденциальную информацию или перейти по вредоносным ссылкам. Чтобы не стать жертвой мошенничества с подделками, необходимо проявлять бдительность и проверять подлинность сообщений.

Мошенничество с банковскими переводами

В случаях мошенничества с банковскими переводами мошенники могут инициировать разговор, выдавая себя, например, за адвоката или руководителя. Часто мошенники изменяют банковские реквизиты, прося вас перевести деньги на неправильный счет или размещают в Интернете объявления, предлагая услуги, например, по аренде жилья. Как только пользователь переводит деньги мошенникам, вернуть средства становится практически невозможно.

Скимминг (снятие данных) карт

Скимминг карт – это получение несанкционированного доступа к информации о кредитной или дебетовой карте. Мошенники устанавливают специальные устройства на банкоматы, считыватели карт для бензоколонок или системы продаж, которые считывают и сохраняют данные магнитной полосы карты, когда пользователь использует данную карту для оплаты. С помощью данной информации мошенники могут дублировать карту или совершать с ее помощью несанкционированные покупки в Интернете.

Кража личных данных

При краже личных данных мошенники собирают достаточно информации о пользователе, чтобы выдавать себя за него при совершении финансовых операций. Они могут открывать новые счета для банковских карт,

оформлять кредиты или даже подавать документы на получение государственных пособий на имя пользователя. Кража личных данных может произойти вследствие кражи электронной почты, утечки данных или сбора информации из профилей в социальных сетях.

Мошенничество с подменой SIM-карт

Мошенники активируют новую SIM-карту, привязанную к номеру телефона жертвы, переводят звонки, сообщения и одноразовые коды на свое устройство. Это позволяет им обойти меры безопасности для получения банковских и других услуг.

Способы получения мошенниками доступа к банковскому счету

Мошенники разработали множество стратегий для взлома банковских счетов:

- социальная инженерия, которая часто применяется совместно с методами фишинга, вишинга или создания сфальсифицированного сценария для кражи ваших данных. Это один из самых распространенных подходов мошенничества, используемый в отношении пожилых людей, поскольку они более уязвимы для манипуляций;
- вредоносные программы и программы-вымогатели. На устройство пользователя без его ведома устанавливается вредоносное программное обеспечение, которое позволяет мошенникам отслеживать нажатие клавиш или получать прямой доступ к банковской информации;
- использование общедоступной информации. Мошенники используют информацию, доступную в Интернете (например, через социальные сети), чтобы подобрать пароли или ответить на вопросы проверки безопасности, получая несанкционированный доступ к счетам;
- утечки данных. В результате масштабных взломов и утечек информации мошенники могут получить доступ к личным и финансовым данным миллионов пользователей, которые в дальнейшем могут быть использованы для получения денежных средств.

Рекомендации о том, как избежать банковского мошенничества

Предотвращение случаев банковского мошенничества требует бдительности и упреждающих мер со стороны пользователей:

1. Пользователям необходимо повышать уровень своей кибергигиены, в том числе регулярно обновлять защитное программное обеспечение компьютера и мобильных устройств, использовать антивирусные программы и поддерживать операционную систему в оптимальном состоянии, что

позволит защитить ее от уязвимостей. Кроме того, рекомендуется избегать доступа в онлайн- или мобильный банкинг в открытых сетях Wi-Fi, поскольку мошенники могут перехватить учетные данные или конфиденциальную информацию;

2. Рекомендовано использовать надежные, уникальные пароли для каждой учетной записи. В паролях целесообразно сочетать использование букв, символов и цифр. При создании пароля также важно избегать использования информации, которую можно угадать, например, дат рождения. Кроме того, необходимо использовать менеджер паролей, чтобы следить за паролями;

3. Пользователям целесообразно включить двухфакторную или многофакторную аутентификацию (2FA или MFA): двухфакторная аутентификация усиливает защиту, требуя от пользователей двух форм проверки: известного элемента (например, пароля) и имеющегося предмета (например, мобильного телефона). Многофакторная аутентификация требует трех и более форм проверки. Эти подходы обеспечивают безопасный доступ к услугам, включая онлайн-банкинг и операции с банкоматами. Дополнительные функции, такие как распознавание лиц и вход по отпечаткам пальцев, способствуют повышению уровня безопасности;

4. Пользователям целесообразно быть в курсе новых и развивающихся видов мошенничества. Данную информацию можно найти в публикациях банков и фирм, занимающихся кибербезопасностью;

5. Важно скептически относиться к неожиданным сообщениям (электронным письмам, смс) и звонкам и проверять подлинность электронного адреса или номера телефона по официальным каналам, прежде чем предоставлять какую-либо информацию;

6. Рекомендуется регулярно следить за состоянием счетов: отслеживать активность на своих счетах и запрашивать выписки с банковских счетов. Раннее обнаружение попыток проведения несанкционированных операций позволяет минимизировать ущерб и оперативно предотвратить случаи мошенничества. Дополнительно возможно подключить оповещения о транзакциях по счету;

7. Важно следить за защитой своей личной информации: уничтожать конфиденциальные документы, следить за защитой своего почтового ящика и проявлять осторожность при публикации в Интернете личной информации;

8. Пользователю необходимо немедленно сообщать о произошедших действиях в банк, например, о том, что он стал жертвой обмана в Интернете;

9. Необходимо помнить о том, какие данные банк никогда не запрашивает у пользователей (например, пин-код, информацию для входа в

интернет-банк, кроме того, банк не попросит опустить карту в почтовый ящик, чтобы ее забрали);

10. Важно следить за кредитной историей, осуществляя мониторинг новых запросов, а также счетов, открытых на имя пользователя, или других изменений, которые могут свидетельствовать о мошеннических действиях;

11. Дополнительно можно осуществлять мониторинг даркнета на предмет обнаружения собственных данных;

12. Рекомендовано также использовать возможность отказа от получения телемаркетинговых звонков, предодобренных предложений по кредитным картам и коммерческих предложений, что позволит свести к минимуму вероятность кражи личных данных и случаев мошенничества.

ФИНАНСОВО-БАНКОВСКИЙ СОВЕТ СНГ (ФБС СНГ)

Правовые основы сотрудничества по кибермошенничеству в СНГ

Правовые основы сотрудничества государств-участников СНГ в сфере обеспечения информационной безопасности и борьбы с киберпреступностью (в т.ч. с мошенничеством в финансовой сфере):

Раздел 4.9 Стратегии сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2025 года[9]. Стратегия и План действий по ее реализации утверждены 28 октября 2016 года.

Взаимодействие государств – участников СНГ в области информационной безопасности осуществляется по следующим основным направлениям:

- развитие механизмов мониторинга и противодействия киберпреступности;
- обеспечение взаимодействия национальных центров реагирования на компьютерные инциденты;
- выявление и оперативное реагирование на случаи нарушения информационной безопасности, обмен информацией и техническими средствами борьбы с нарушениями;
- формирование систем мониторинга ресурсов национальных сегментов Интернета в целях своевременного выявления угроз, а также поиска оптимальных средств их нейтрализации.

Решение Совета глав правительств СНГ «О Стратегии обеспечения информационной безопасности государств - участников Содружества Независимых Государств». Принято в г. Москве 25.10.2019.

Координация работы по реализации настоящей Стратегии осуществляется Координационным советом государств - участников СНГ по информатизации при Региональном содружестве в области связи во взаимодействии с компетентными органами государств - участников СНГ и заинтересованными органами отраслевого сотрудничества СНГ в соответствии с действующими международными правовыми актами и законодательством государств - участников СНГ.

План мероприятий по реализации Стратегии на период до 2030 года утвержден на заседании Совета глав правительств СНГ 20 мая 2022 г.

[9] утверждена Решением Совета глав правительств СНГ о Стратегии сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2025 года и Плане действий по ее реализации от 28 октября 2016 года

Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий. Заключено в г. Душанбе 28.09.2018. Российская Федерация ратифицировала соглашение с оговорками 1.07.2021[10].

Соглашение определяет формы сотрудничества, регулирует вопросы выдачи, оказания взаимной правовой помощи.

Межгосударственная программа совместных мер борьбы с преступностью на 2024 - 2028 годы. (очередная) Принята на заседании Совета глав государств СНГ 13.10.2023 года в Бишкеке

Включает организационно-правовые, организационно-практические мероприятия, информационное и научное обеспечение в сфере противодействия преступлениям, совершаемым с использованием информационных технологий.

Модельный закон «О противодействии киберпреступности»[11]. Принят на 55-м пленарном заседании Межпарламентской Ассамблеи государств СНГ 14.04.2023.

Развитие модельного законодательства, которое после имплементации его в национальные правовые системы государств СНГ позволит его унифицировать в части определения перечня киберпреступлений, осуществления мер по профилактике, международного сотрудничества.

СНГ: обобщенная ситуация с мошенничеством в финансовой сфере

Наиболее актуальной аналитической информацией по рассматриваемой теме является Аналитический отчёт Лаборатории Касперского - «Ландшафт киберугроз для России и СНГ 2024».

Количество компьютерных атак в странах СНГ (с 1 кв. 2023 по 1 кв.2024)

Таджикистан	60,69%
Беларусь	59,79%
Туркменистан	59,55%
Узбекистан	58,74%
Кыргызстан	57,21%
Казахстан	54,62%
Россия	51,86%
Азербайджан	49,37%
Армения	44,21%

[10] Федеральный закон "О ратификации Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий" от 01.07.2021 №237-ФЗ (последняя редакция)

[11] Приложение к постановлению Межпарламентской Ассамблеи государств — участников Содружества Независимых Государств от 14.04.2023 № 55-20

(% = количество пользователей, столкнувшихся с угрозами, к общему числу пользователей решений «ЛК» в исследуемом регионе).

Атаки на финансовый сектор лидируют среди всех отраслей, они составляют 28% от всего количества зарегистрированных средствами «ЛК» атак. В контексте мошенничества в финансовом секторе ситуация в исследуемом регионе аналогична мировым трендам и несет риски как для частных лиц, так и для организаций от малого до крупного бизнеса.

Мошенничество реализуется посредством:

- утечки данных

Сфера электронной торговли традиционно больше всего страдает от утечек данных, 23 инцидента связанных с утечками данных было выявлено в Q1`2024. 2024 не отличается разнообразием по атакованным сферам, в отличие от предыдущих лет. Помимо торговли, под удар попали организации финансовой отрасли и компании, относящиеся к здравоохранению. Атаки на финансовые организации (банки, микрофинансовые организации, страховые компании) позволили злоумышленникам опубликовать более 83 млн пользовательских данных, что составляет 81% всех данных, опубликованных за Q1`2024.

- кражи персональных данных, финансовой информации и коммерческих секретов
- фишинговых атак (методы социальной инженерии)

Рассылка писем или SMS-сообщений, имитирующих сообщения от известных организаций, чтобы побудить пользователей перейти по вредоносным ссылкам или добровольно предоставить конфиденциальную информацию. Например, пользователям предлагают воспользоваться быстрым кредитом, прибыльно инвестировать в крупную компанию, пройти опрос, оказать финансовую помощь.

В Азербайджане, как и во многих других странах исследуемого региона, фишинг чаще всего направлен на получение доступа к банковским данным или другой конфиденциальной информации, связанной с финансовыми учреждениями.

В Казахстане для атак с использованием социальной инженерии примечательным является то, что большое количество фишинговых сайтов пытаются маскироваться под один из самых популярных в стране банков «Kaspi».

В целом, злоумышленники, в основном, маскируют свои фишинговые сайты под финансовые организации, будь то банки или различные микрофинансовые организации. Встречаются примеры маскировки под популярные социальные сети, магазины или сервисы. Также можно отметить, что популярным способом компрометации является создание поддельных форм аутентификации в мессенджере Telegram под предлогом «подтверждения личности».

- **эксплуатация уязвимостей в программном обеспечении,** особенно в API (программном интерфейсе приложений мобильных устройств). Удаленное выполнение кода занимает все десять позиций TOP-10 в эксплуатации уязвимостей, некоторые из них позволяют раскрытие чувствительной информации, повышение привилегий, подмену пользовательского интерфейса.

Важно отметить, что больше половины эксплуатируемых уязвимостей датируются концом прошлого десятилетия, что говорит о том, что для минимизации рисков эксплуатации необходим грамотно выстроенный процесс обновлений ПО, а также использование современных решений.

Анализ экспертов МВД России

По данным статьи на Научном портале МВД России. 2023[12]

[12] Зенченко Е. П., Ивлиева Н. В. Мошенничества, совершаемые с использованием информационных технологий на территориях государств – участников СНГ // Научный портал МВД России. 2023. № 3 (63). С. 118–124

Современное состояние оперативной обстановки в сфере осуществления платежей, выполняемых посредством применения IT-технологий на территориях государств – участников СНГ, характеризуется весьма высокими показателями зарегистрированных преступных посягательств на территориях этих государств.

В 2022 г. рост компьютерных мошенничеств на территориях стран – участниц СНГ продолжался и составил, как минимум 30 % за счет развития схем социальной инженерии и использования новых технологий (прим. Среди последних можно отметить электронные кошельки и криптовалюты). Самым распространенным способом мошенничества являются телефонные звонки потенциальной жертве, а самым популярным способом хищения средств – вирусы и фишинговые атаки.

Способы интернет-мошенничеств постоянно совершенствуются и развиваются одновременно с сектором IT-технологий и методами социальной инженерии. Также отметим, что способы совершения интернет-мошенничеств универсальны и могут применяться на территории любого государства – участника СНГ, поскольку распространяются в одном информационном поле. В то же время способы дифференцированы в зависимости от личности потенциальной жертвы и текущей информационной повестки (например, в Казахстане уже 28.08.2024 года выявлена почтовая спам-рассылка на английском языке, в которой сообщается о сборе средств на юридическую защиту основателя Telegram Павла Дурова и глобальную информационную кампанию).

Некоторые фактографические материалы по теме

Армения

25.01.2024 Интернет-мошенники обокрали доверчивых граждан Армении, заполучив у них обманом полмиллиона долларов. Они используют нейронные сети для создания рекламных видеороликов, в которых известные люди призывают вложить деньги в различные коммерческие проекты и покупать акции. В том числе, был использован дипфейк с премьер-министром Николом Пашиняном.

28.08.2024 Центробанк Армении предупреждает о новых мошеннических схемах, в которых представляясь сотрудниками банков или кредитных организаций, злоумышленники получают доступ к банковским данным граждан и снимают деньги с их карт.

Азербайджан

2023 год. По данным Лаборатории Касперского в 2023 году защитные решения компании сумели заблокировать более 945 тысяч попыток пользователей из Азербайджана перейти на фишинговые страницы. В числе

самых популярных способов распространения такого контента были мессенджеры и соцсети. Также злоумышленники использовали в своих схемах тему криптовалютных бирж и эксплуатировали повышенный интерес к чат-ботам, в том числе создавали поддельные ресурсы с функционалом, повторяющим официальные государственные сайты, а на самом деле не подключенные ни к одной языковой модели. Настоящие чат-боты злоумышленники тоже используют, например, для написания текстов при подготовке целевых фишинговых атак.

Также мошенники прибегали и к проверенным методам, в частности, адаптировали фишинговые схемы под актуальную новостную повестку, например громкие кинопремьеры, ожидаемые релизы, крупные спортивные и культурные события. Фишеры могут предлагать подешевле или пораньше получить доступ к новинкам.

Злоумышленники постоянно совершенствуют свои методы, делают свои атаки более персонализированными, в том числе с помощью технологий машинного обучения. Кроме того, масштабирование атак с помощью ботов и автоматизированных систем позволяет достигать больше потенциальных целей и повышает вероятность успеха таких атак. Для фишинга используются IP-адреса разных стран.

1.04.2024 МВД Азербайджана злоумышленники разработали довольно простой, но в то же время хитроумный план для получения данных банковских карт граждан. Они используют социальные сети и маркетплейсы для размещения объявлений о продаже товаров или сдаче объектов в аренду. Обычно они предлагают товары и услуги по привлекательным ценам или условиям, чтобы привлечь потенциальных покупателей. Наивные пользователи, не подозревая об уловках, реагируют на такие объявления и вносят предоплату за товар или услугу. После того, как деньги переведены, мошенники связываются с жертвой по телефону или мессенджеру, утверждая, что сделка не может быть осуществлена по тем или иным причинам, и предлагают вернуть предоплату на карту покупателя, для чего просят назвать ее CVV-код.

15.03.2024 Центральный банк Азербайджана (ЦБА) назвал наиболее часто используемые методы мошенничества, совершаемые для получения данных банковских карт. Мошенники чаще всего используют такие методы, как ложные объявления об участии в кампаниях, лотереях, вложение средств в инвестиционные операции, основанные на пирамидальной схеме, которая обещает высокую прибыль в короткие сроки. Деятельность по предупреждению киберпреступности и мошенничества осуществляется в тесной координации с ЦБА, банками и соответствующими государственными органами.

29.08.2024 Сотрудники Главного управления по борьбе с киберпреступностью МВД Азербайджана в результате проведенного расследования и изучения интернет-ресурсов, проведенных оперативно-технических мероприятий задержали 4 членов группировки, которые незаконно действовали в соцсетях, получая путем фишинга данные банковских карт граждан и похищая особо крупные суммы денег. Они создавали фальшивые сайты банков и торговых платформ, и размещали ложные объявления о проводимых банками лотереях с денежным выигрышем и продаже дорогих моделей телефонов по цене ниже их стоимости. Члены банды также организовали платную рекламу этих ссылок в социальных сетях для привлечения большего числа граждан. Установлено, что преступники похитили денежные средства с карт около 400 граждан, причинив им материальный ущерб на общую сумму около 500 тыс. манатов (почти 26,9 млн руб).

Беларусь

29 августа 2023 года Президент Беларуси А.Лукашенко подписал Указ №269 «О мерах по противодействию несанкционированным платежным операциям». Согласно документу, Национальный банк организует информационное взаимодействие между правоохранительными органами и поставщиками платежных услуг по обмену информацией о несанкционированных платежных операциях и попытках их совершения.

Белоруссия активно использует российский опыт. В частности, будут внедряться антифрод-системы с учетом конкретных требований белорусских банков, включая интеграцию с уже действующими системами внутри банков. Будут использоваться технологии выявления телефонных мошенников на основе искусственного интеллекта или сотрудничества с мобильными операторами Республики Беларусь. Вовлечение национальных ИТ-компаний в разработку системы, чтобы обеспечить импортозамещение программного обеспечения.

2023 год. Отчет[13] ОАО «Банковский процессинговый центр» описывает основные тенденции в мошенничестве с банковскими платежными карточками. Основная доля мошенничества в Беларуссии в 2023 году, как и в 2022, году, приходидилась на мошенничество с банковскими платежными карточками в среде без физического присутствия держателя при проведении операции.

Характерной тенденцией 2023 года стало мошенничество с использованием реквизитов карточек наряду с единичными случаями

[13] Мошенничество в сфере платежных инструментов и сервисов в 2023 году: общая статистика и тенденции Отчет на основе данных Банковского процессингового центра https://npc.by/upload/iblock/f1c/638xid022o9wx6u3sx1y9s35ndfo47i8/Приложение%20Отчет%20«Мошенничество%20в%20сфере%20платежных%20инструментов%20и%20сервисов%20в%202023%20году%20общая%20статисти.pdf

мошенничества по поддельным и утерянным/украденным карточкам. В среде мошенничества с использованием реквизитов карточек основная доля мошенничества приходится на социальную инженерию – около 60%. Значительная доля мошенничества с применением социальной инженерии свидетельствует о том, что данный вид мошенничества быстро адаптируется к любым изменениям, а использование методов социальной инженерии приносит быстрый доход злоумышленникам при минимальных финансовых затратах.

Мошенники стремятся получить личные данные держателей карточек, доступы к их счетам, системам дистанционного банковского обслуживания, МСИ и мобильным устройствам. В целях хищения денежных средств и персональных данных в 2023 году злоумышленники в рамках социальной инженерии связывались с потенциальными жертвами посредством торговых площадок, осуществляли звонки от имени работников банков, правоохранительных органов и других различных организаций, направляли сообщения в социальных сетях и осуществляли рассылки в мобильных мессенджерах.

Активно эксплуатировалась схема мошенничества, связанная с установкой приложений удаленного доступа (AnyDesk, TeamViewer, RustDesk) на мобильные устройства держателей, в результате реализации которой злоумышленники получали полный контроль над счетами и денежными средствами. Участились случаи, когда держатели переходили по фишинговым ссылкам, считая, что это официальные ресурсы банков, почтовых служб и служб доставки, где вводили логин и пароль от интернет- банкинга или реквизиты свое й карточки для оплаты услуг, в результате чего конфиденциальные данные становились доступны злоумышленникам и/или держатели лишались своих денежных средств.

По-прежнему использовалась схема мошенничества, связанная с сайтами знакомств, когда злоумышленники для якобы организации встречи присылали держателям фишинговые ссылки на покупку билетов в театр, кино или в другие места для развлечений. В случае, если клиент переходит по данной ссылке и соглашается с проведением оплаты, с его счета списывается денежная сумма.

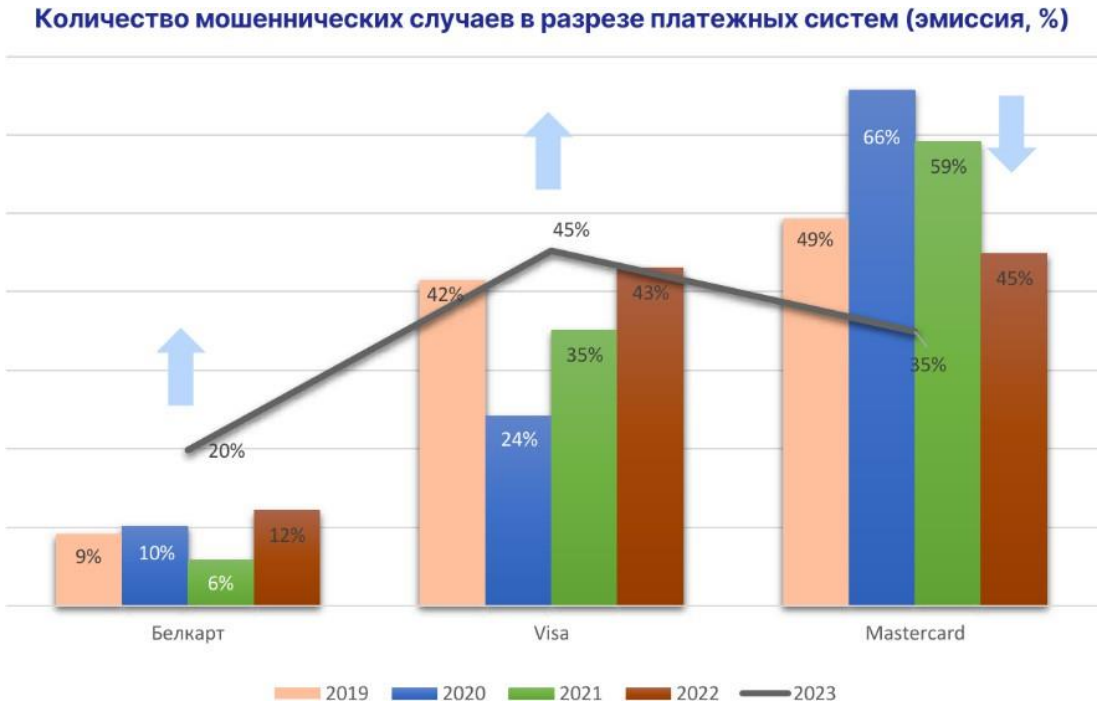
В 2023 году появилась новая схема мошенничества с кредитами, которые держатели самостоятельно оформляют, а затем переводят кредитные денежные средства в адрес мошенников посредством инфокиосков. В данном случае злоумышленникам удается внушить держателям, что они участвуют в проведении служебного расследования по поимке недобросовестного сотрудника банка. Также имели место случаи, когда держатели даже продавали своё имущество (квартиры, автомобили, технику) и осуществляли переводы денежных средств на счета злоумышленников.

В конце 4 квартала 2023 года стала активно использоваться схема мошенничества, связанная с токенизацией скомпрометированных карточек.

После получения необходимых данных карточки с использованием методов социальной инженерии или фишинговых рассылок, мошенники привязывают карточку на свое мобильное устройство и пытаются совершить оплаты в сети интернет либо в организациях торговли и сервиса, которые находятся в различных странах.

Участилось мошенничество, связанное с генерацией номеров карточек и атаками на БИНы банков - процесс инициирования 1-2 тестовых транзакций для проверки карточки с целью ее дальнейшего использования в мошеннических целях. При этом используются программные средства для генерации номеров карточек, а атаки осуществляются в торговых точках электронной коммерции, которые имеют слабые механизмы контроля и защиты от мошенничества.

По итогам 2023 года количество успешных мошеннических операций по карточкам банков, которые обслуживаются в ОАО «Банковский процессинговый центр», по типу мошенничества распределилось следующим образом: 70% мошеннических операций приходится на мошенничество с использованием реквизитов карточек, 30% незаконных операций с банковскими платежными карточками приходится на account takeover (перехват счета).



В 2023 году количество выявленных мошеннических случаев (карточек) увеличилось на 8% относительно 2022 года, при этом на 57% сократилось общее количество успешных мошеннических операций, заявленных в международные платежные системы, общая сумма успешных мошеннических операций уменьшилась на 64%, а средняя сумма 1 мошеннической операции составила 35 долларов США (42 доллара США в 2022 году), что на 15% меньше алогичного показателя прошлого года.

Уменьшение общей суммы успешных мошеннических операций, заявленных в международные платежные системы, обусловлено

переориентацией злоумышленников на использование платежных сервисов, зарегистрированных на территории Республики Беларусь, использование систем дистанционного банковского обслуживания для вывода денежных средств, а также с увеличением количества мошеннических попыток по сгенерированным карточкам.

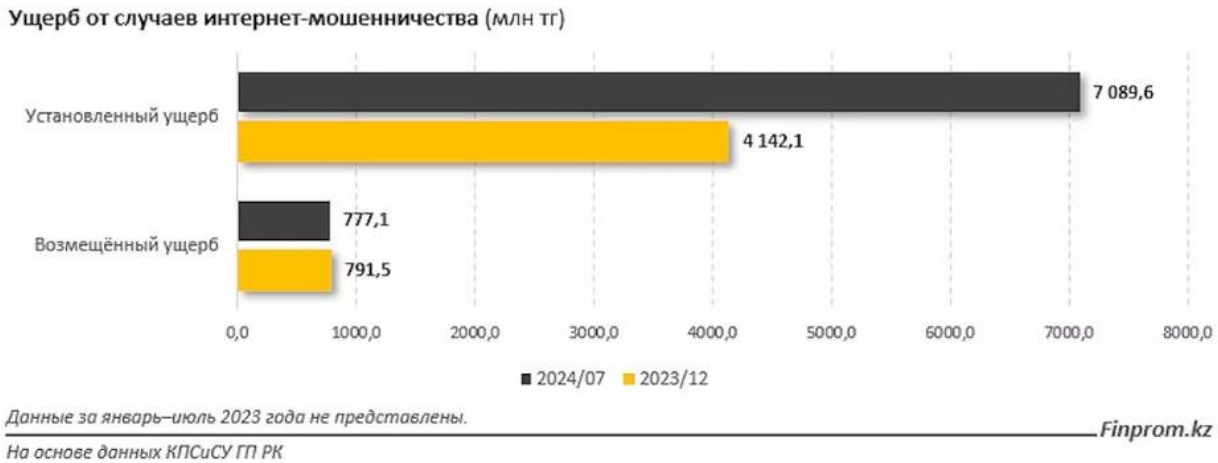
2024 год. В статье заместителя председателя правления Нацбанка Дмитрия Калечица сообщается, что в 2024 году в банковской системе зафиксировано около 8808 инцидентов. Ущерб от них клиентам банков превысил 26 млн рублей. При этом банками приостановлено около 3,3 тыс. переводов на сумму 3,8 млн рублей (около 14% от общей суммы ущерба).

По данным Нацбанка, форма онлайн-взаимодействия клиентов с банками становится все более популярной среди граждан. С учетом роста популярности онлайн-продуктов в финансовой сфере увеличивается и количество мошеннических операций. Но Нацбанк и коммерческие банки принимают меры для их предотвращения. Регулятор, в частности, направил коммерческим банкам соответствующие рекомендаций.

Банкам предложено применять «период охлаждения» (по кредитам, выдаваемым наличными либо перечислением денег на счет, договор заключается на следующий день после подачи заявки на кредит). Второй вариант применения «периода охлаждения», когда деньги предоставляются на следующий день после заключения кредитного договора. Кроме того, банкам рекомендовано учитывать информацию о количестве запросов на получение кредитного отчета в отношении человека, поступивших в течение семи календарных дней, предшествующих дню его обращения за получением кредита.

Казахстан

26 августа 2024. За 7 месяцев 2024 года онлайн-мошенники в Казахстане нанесли ущерб на 7,1 млрд тенге, что больше, чем было за весь прошлый год. Вернуть удалось лишь 11% от этой суммы. Для сравнения: за весь 2023 год сумма была в полтора раза меньше – 4,1 млрд тенге.



Примечательно, что сильнее всего пострадали рядовые граждане. Их совокупный ущерб от онлайн-мошенников составил 6,8 млрд тенге, а вот юридические лица в текущем году потеряли порядка 304,1 млн тенге. Стоит отметить, что большую часть средств вернуть так и не удалось.

Чаще всего интернет-аферисты крадут деньги у казахстанцев во время онлайн-покупок – 3 258 жалоб поступило от купивших что-либо в интернете, но не получивших товар. Второе место заняли заявления граждан о получении мошенниками доступа к их конфиденциальным данным через фишинговые сайты, электронную почту или приложения для смартфонов (3 218 случаев). Преступники также используют фальшивые объявления в Интернете о предоставлении несуществующих услуг (2 917), онлайн-кредитование (1 992 случая) и ложные SMS-сообщения и звонки из "банков" (1 727 случаев). На финансовые пирамиды пришлось 462 случая мошенничества в 2024 году.

Всего же в Казахстане с начала года было зарегистрировано 26,9 тыс. правонарушений по статье "Мошенничество", из которых 44,4%, или около 12 тыс., были совершены в Интернете.

Напомним, ранее стало известно, что микрофинансовые организации в Казахстане теперь должны проводить биометрическую проверку своих клиентов при оформлении займов электронным способом. Поэтому в будущем количество преступлений в сфере онлайн-кредитования может сильно сократиться[14].

26.08.2024 Согласно данным Генеральной прокуратуры Казахстана, случаи интернет-мошенничества увеличились более чем в 40 раз за последние несколько лет. Если в 2018 году было зафиксировано чуть больше 500 таких случаев, то в 2023 году их число достигло 21,8 тысяч.

Мошенники используют новые методы и расширяют свои действия, что приводит к увеличению ущерба. В ответ на эту проблему правоохранительные органы усиливают борьбу с киберпреступностью: в МВД запустили проект CyberPol, а Национальный банк открыл Антифрод-центр для блокировки подозрительных транзакций.

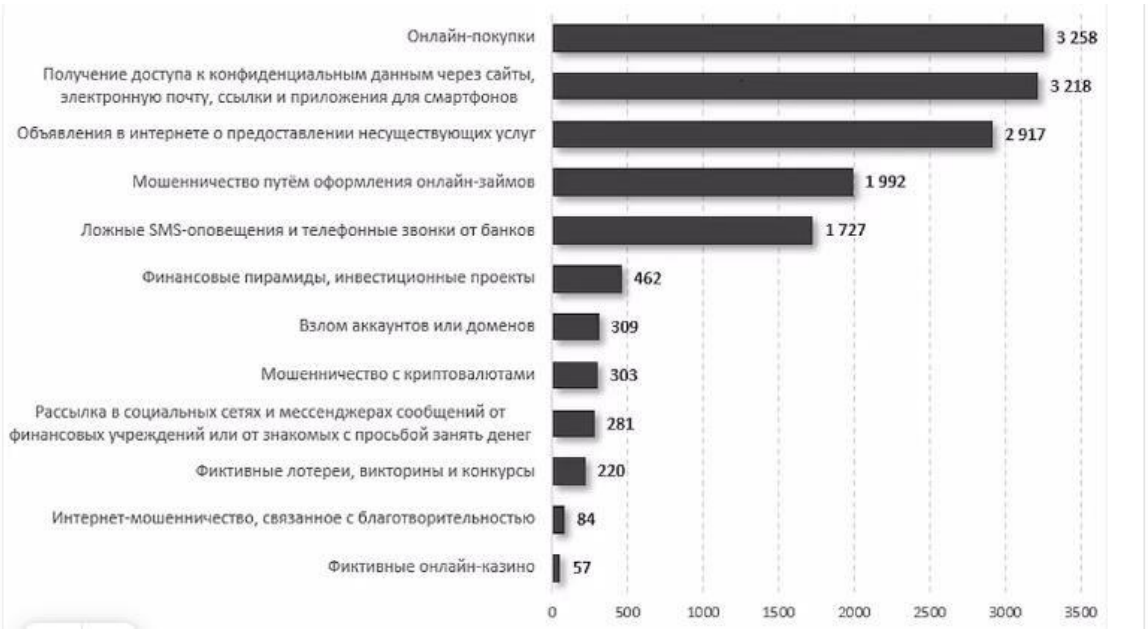
Большинство уголовных дел по интернет-мошенничеству закрываются из-за того, что виновных не удаётся установить. В прошлом году 79,2% дел были прекращены по этой причине, а в этом году уже 56,3%.

С этого года специалисты Комитет по правовой статистике и специальным учетам Генеральной прокуратуры Казахстана начали публиковать данные о структурах интернет-мошенничества, которые помогает понять, на какие уловки попадают казахстанцы.

[14] Сколько украденных онлайн-мошенниками денег удалось вернуть в Казахстане. Опубликовано: 26 августа 2024,https://www.nur.kz/nurfin/personal/2153289-skolko-ukradennyh-onlayn-moshennikami-deneg-udalos-vernut- v-kazahstane/

За январь–июль 2024 года 24,5% случаев мошенничества связано с жалобами на неполученные товары, что составляет около 3,2 тыс. обращений. На втором месте – 24,2% – заявления о кражах конфиденциальных данных через сайты и электронную почту. Мошенники в таких могут использовать эти данные для противоправных действий или оформления кредитов.

Также в 15% случаев фиксируются онлайн-займы. Кроме того, киберпреступники устраивают фиктивные лотереи, взламывают аккаунты в соцсетях и просят знакомых одолжить деньги, звоня от имени банков с просьбой перевести средства на "резервный" счёт.



Кыргызстан

2024 год. Национальный банк Кыргызской Республики предупреждает: участились случаи телефонного мошенничества. Используя разные способы обмана граждан посредством телефонных звонков, мошенники преследуют цель украсть ваши деньги со счетов или оформить на вас онлайн-кредит для последующего перевода.

Пользователей призывают следить за официальным интернет-сайтом Национального банка Кыргызской Республики www. nbkr.kg и официальными страницами Национального банка в социальных сетях, где размещается важная информация для потребителей: Instagram-nbkr_kg; Facebook и Telegram-каналами Национального банка, а также за новостями и уведомлениями финансово-кредитных организаций на веб-сайтах и мобильных приложениях.

14.03.2024 По данным ГУУР МВД по киберпреступности количество преступлений, совершаемых с использованием информационных технологий,

за последние годы увеличилось в несколько раз и продолжает расти. Среди самых распространенных схем: мошенничество с использованием электронной почты, кража цифровой личности, данных платежных карт и другой финансовой информации, хищение и перепродажа корпоративных данных, кибершантаж.

Набирает обороты телефонное мошенничество, когда гражданам звонят неизвестные и, представляясь родственниками или сотрудниками органов внутренних дел, здравоохранения, спасательных служб, сообщают о несчастном случае в результате ДТП и просят отправить деньги через курьеров или на карту. Только по Бишкеку с 16 февраля 2024 года в милицию поступило 1030 обращений. 77 человек пострадали от рук мошенников. Общий ущерб превысил 43 миллиона сомов (46,2 млн руб).

Молдова

По данным СМИ Молдавия занижает статистику по кибермошенничеству. Центр по борьбе с киберпреступностью Национального инспектората расследований при ГИП заявил, что в 2022-2023 годах случи онлайн-мошенничества, когда жертвы получали сообщения на телефон или электронную почту, увеличилось. При этом было возбуждено только 380 уголовных дел, связанных с кибермошенничеством. При их расследовании пользуются помощью от полиции Румынии.

В 2023 году появился новый вид онлайн-мошенничества с использованием образов первых лиц государства, в том числе президента страны Майи Санду, фейковых профилей и поддельных видео с государственными чиновниками, а также с представителями банковских учреждений. Мошенники призывают регистрироваться по подозрительным ссылкам и инвестировать в мошеннические схемы якобы для получения дивидендов.

В 2024 году широкую огласку получил арест мошенников, создавших фальшивую криптобиржу и укравших у своих жертв 4 миллиона леев:

При этом с 2022 года не утихает скандал с мошенничеством в крупных размерах в финансовом, банковском и страховом секторах Молдовы[15]. В отчете независимого консультативного комитета по борьбе с коррупцией изложен анализ факторов, способствовавших систематическому мошенничеству и отмыванию денег в банковском, страховом и финансовом секторе захвату рынка коррумпированными олигархами и лицами.

[15] «Офшорная республика». Обзор факторов, приводящих к систематическому мошенничеству и отмыванию денег в финансовом, банковском и страховом секторах Молдовы, https://ccia.md/wp-content/uploads/2022/07/Ofshornaja-Respublika-Obzor-faktorov-privodjashhih-k-sistematicheskomu-moshennichestvu-otmyvaniju-deneg-v-finansovom-bankovskom-strahovom-sektorah-Moldovy.pdf

Россия

26 июля 2022 г. Возникшая после ввода санкций Запада против ряда российских банков мошенническая схема, основанная на предложении оформить карту кредитных организаций из стран СНГ, стала набирать обороты. Мошенники оперативно перестраивают свои преступные схемы под актуальную повестку, в том числе разыгрывая карту с обменом валют, выводом денег за рубеж, оформлением счетов в банках СНГ. Специалисты Digital Risk Protection Group-IB отмечают появление услуги в виде помощи с оформлением карт банков стран СНГ. Для оформления платежного средства в иностранном банке клиент передает конфиденциальную информацию, в том числе данные карты, сканы документов, доверенность и предоплату за услугу. Предоставление этих данных третьим лицам несет серьезные риски для клиента, и нет гарантий, что банковская карта будет оформлена, а конфиденциальная информация не попадет к мошенникам.

28 сентября 2023 г. По данным исследования Аналитического центра НАФИ и компании «Ингосстрах» в 2023 году на 9 п.п. выросла доля тех, кто сталкивался с попытками мошенничества (82% – 2022 год, 91% – 2023 год). Самой распространенной схемой сегодня является телефонное мошенничество – звонки от псевдосотрудников банков или правоохранительных органов. Подобные звонки за последние 12 месяцев получали 73% россиян. Чаще о подобных ситуациях говорят работающие пенсионеры (86%), опрошенные с высшим образованием (84%) и женщины (73%). Именно эти категории граждан наиболее уязвимы и находятся в группе риска.

С ростом доли тех, кто сталкивается с попытками мошенничества, растет и вариативность способов, которыми злоумышленники пытаются обмануть людей. Так, если в 2022 году в среднем россияне сталкивались с тремя разными схемами мошенничества, то сегодня уже с четырьмя.

Самой распространенной схемой обмана являются звонки от представителей «банков» или «правоохранительных органов» с целью выведать данные банковских карт и счетов. Доля тех, кто сталкивался со звонками псевдобанкиров, псевдополицейских или мнимых сотрудников следственных органов, составляет 73% россиян – на 19 п.п. больше, чем годом ранее (54%).

На втором месте по степени распространения – предложения заработать в интернете на так называемых «инвестициях», например, через вложение денег в криптовалюту. Такие сообщения от мошенников в нынешнем году получали 63% россиян, а в 2022-м на 8 п.п. меньше (55%).

Третье место занимают сообщения или электронные письма с подозрительными ссылками, переход по которым связан с финансовыми угрозами. За последний год такие сообщения получали 46% россиян, а годом ранее – 39% (рост на 7 п.п).

На четвертом месте – предложения получить выплату или компенсацию от государства, для оформления которой нужно сообщить данные карты или другую личную информацию. В этом году подозрительные рекомендации поступали 45% опрошенных, в прошлом – 39% (рост на 6 п.п.).

Завершает ТОП-5 распространенных попыток мошенничества сообщения или звонки с просьбами помочь родственникам или знакомым, которые якобы попали в трудную жизненную ситуацию, а также вымогательства денег под предлогом получения выигрыша в лотерею. О подобных ситуациях рассказали 43% россиян, на 7 п.п. больше, чем в 2022 году (36%). Кроме того, россиян пытались обмануть через фишинговые сайты (28%) и при продаже или покупке товаров в интернете (27%).

11 июля 2023 года Государственной думой РФ принят Федеральный закон № 369-ФЗ «О внесении изменений в федеральный закон «О национальной платежной системе» (далее – ФЗ № 369), в первую очередь направленный на усиление мер противодействия хищению денежных средств. Изменения направлены на модернизацию не только существующего механизма противодействия хищению денежных средств («антифрода»)*, но и действующего механизма возврата уже списанных со счетов клиентов денежных средств.

В целях обеспечения защиты информации при осуществлении переводов денежных средств Банк России будет осуществлять формирование и ведение базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, а также предоставлять информацию обо всех случаях и (или) попытках осуществления переводов денежных средств без добровольного согласия клиента операторам по переводу денежных средств (далее – оператор), операторам платежных систем, операторам услуг платежной инфраструктуры, операторам электронных платформ. В базу данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента будет включается в том числе информация о переводах денежных средств без добровольного согласия клиента, а также переводах денежных средств, связанных с переводами денежных средств без добровольного согласия клиента, в отношении которых от федерального органа исполнительной власти в сфере внутренних дел получены сведения о совершенных противоправных действиях.

Оператор будет обязан осуществить проверку наличия признаков осуществления перевода денежных средств без добровольного согласия клиента, а именно без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием, до момента списания денежных средств клиента (в случае совершения операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием сервиса быстрых платежей платежной системы Банка России) либо при приеме к исполнению распоряжения клиента (при осуществлении перевода денежных средств в иных случаях).

Признаки осуществления перевода денежных средств без добровольного согласия клиента будут регламентированы Банком России (далее – ЦБ РФ). При выявлении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия клиента, оператор приостанавливает прием к исполнению распоряжения клиента на 2 дня. Если операция по переводу выполняется с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием сервиса быстрых платежей платежной системы ЦБ РФ, то оператор отказывает в совершении соответствующей операции (перевода).

Положения закона вступили в силу 25 июля 2024 года, но в течение года банки активно готовились к изменениям в законодательстве. Так, например, Сбер, начал блокировать операции — как онлайн, так и в банкоматах — которые, по определению антифрод-мониторинга, совершаются под влиянием мошенников. Т-Банк официально запустил систему дроп-мониторинга. Если система полагает, что карта продана мошеннику, она сигнализирует об этом

— банк проводит дополнительное расследование или сразу ограничивает дистанционное обслуживание. Также банки усилили меры, направленные на противодействие кредитному мошенничеству. Финансовые организации учатся выявлять заявки на кредиты, которые оформлены под воздействием аферистов. В частности, ВТБ разрабатывает комплексную программу, которая, как утверждают в банке, позволит с вероятностью 99% выявить, что клиент общался со злоумышленниками и предупредить его о рисках оформления кредита или снятия денег.

20 августа 2024 года Банк России опубликовал статистику по операциям без согласия клиентов за II квартал текущего года[16], на которую реализация мер № 369-ФЗ уже оказала влияние. Позитивной новостью

[16] Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // Банк России 1 квартал 2024 - https://www.cbr.ru/statistics/ib/review_1q_2024/2 квартал 2024 - http://www.cbr.ru/statistics/ib/review_2q_2024/

является, что было предотвращено совершение почти 16,3 млн мошеннических операций, что на 70% больше, чем в предыдущих периодах. При этом ситуация выглядит достаточно противоречиво. С одной стороны, во II квартале 2024 года количество мошеннических операций сократилось почти на 15% по сравнению со средним значением за предшествовавшие 4 квартала, но объем операций без согласия клиентов и, соответственно, потери средств увеличились на 19% и достигли более 4,77 млрд руб. Доля возмещенных (возвращенных) физическим лицам средств, имеет следующую структуру: карты - 7,6 %, счета (дистанционное банковское обслуживание, переводы) - 10,3%, СБП - 2,1%, по электронным кошелькам и операциям без открытия счета возврата средств осуществить не удалось. Юридическим лицам доля возмещенных средств по операциям со счетов составила только 0,6%.

Основные типы компьютерных атак: выявлено (ед.), динамика (%)

Тип атаки	Среднее значение за предшествующие четыре квартала	II квартал 2024
Использование методов социальной инженерии	28 136	20 638 -26,65% ▼
Фишинговые атаки	1 131	1 361 20,34% ▲
Атаки с использованием ВПО	80	40 -50,00% ▼
Атаки типа «отказ в обслуживании» (DDoS)	109	87 -20,18% ▼
Иные атаки	70	66 -5,71% ▼

Эффективность противодействия мошенникам, по мнению экспертов, выросла благодаря объединению усилий правоохранительных органов, ведомств, банков и операторов. В течение прошлого года финансовые организации модернизировали свои антифрод-системы, государство активизировало законотворческую деятельность, направленную против мошенников, а телеком-операторы начали развивать взаимодействие с банками и присоединяться к системе Роскомнадзора «Антифрод», которая не позволяет злоумышленникам звонить с подменных номеров.

Также эксперты полагают, что финансовое мошенничество в стране намного более распространено, чем представлено в отчетах регулятора. Дело в том, что многие россияне просто не верят в возможность вернуть деньги, похищенные мошенниками, и не сообщают о том, что стали жертвами преступников. Также рассказать о случившемся мешают стыд, правовой нигилизм и другие причины.

Таджикистан

19 июня 2023 года Россия и Таджикистан подписали Договор о сотрудничестве в области международной информационной безопасности.

2024 г. Согласно аналитическому отчету «Ландшафт киберугроз для России и стран СНГ — 2024», подготовленному Лабораторией Касперского, Таджикистан оказался наиболее уязвим компьютерным атакам среди стран СНГ. Статистика показывает, что 60,69% пользователей в Таджикистане столкнулись с киберугрозами, что значительно превышает показатели других стран Содружества.

Банковские эксперты говорят о том, что количество держателей банковских карт увеличилось после закрытия в Таджикистане наиболее востребованных систем денежных переводов, в том числе, и «Золотой короны». На смену пришли мобильные кошельки и пластиковые карты, куда можно было оформить перевод из России, но только культуры их использования нет. Идентификация мобильных кошельков можно пройти онлайн. И это тоже дает возможность для кражи банковских данных и соответственно денег.

Кроме того, активизировался фишинг. У национальной платежной системы «Корти милли», на долю которой приходится 60% всех банковских карт в стране, до сих пор нет полноценной защиты — 3D (3 Domain Secure)-аутентификации, что является дополнительным уровнем безопасности для банковских карт.

Самые распространенные мошеннические схемы:

Схема №1 – она самая распространенная: покупатель хочет перевести пользователю деньги за товар и для этого требует у него не только номер карты, но и другие данные карты, к примеру, смс с кодом, который был отправлен на номер мобильного телефона. Как только он получает этот код, с карты пользователя исчезают имеющиеся на счету деньги. Эту схему может также использовать якобы потенциальный арендатор.

Схема №2 – Пользователь выиграл деньги. В социальных сетях, к примеру, вКонтакте, разыгрываются призы или деньги. Организаторы призывают участников отмечаться в комментариях и участвовать в розыгрыше. Потом пишут сообщение участнику о том, что он выиграл деньги и просят дать номер карты, чтобы перевести ему деньги. Вслед за этим просят написать срок действия карты и CVV-код, который указан на обороте карты, и номер телефона. Потом просят продиктовать код, который пришел в СМС.

Схема №3 – Данная схема несколько сложнее, но тоже уже используется. У пользователя есть только карта «Корти милли» и нет мобильного кошелька. Но пользователь ранее предоставлял в какое-либо

учреждение копию своего паспорта. Далее открывается на номер третьего лица мобильный кошелек, к которому привязывается карта пользователя, номер, пришедший на телефон, мошенник получает, представившись сотрудником сотового оператора. Деньги с карты уходят посредством мобильного кошелька.

Узбекистан

Постановление Президента Республики Узбекистан, от 30.11.2023 г. № ПП-381 о мерах по усилению защиты прав потребителей цифровой продукции и борьбы с цифровыми правонарушениями.

Согласно документу, в последнее время увеличились случаи кражи или мошенничества с использованием банковских карт, что свидетельствует «о недостаточности цифровой финансовой грамотности населения и квалификации сотрудников правоохранительных органов, об отсутствии современных систем предупреждения правонарушений в банках и платёжных организациях, у операторов платёжных систем».

Для пресечения краж и мошенничества Центральный банк Узбекистана сможет требовать блокировки банковских карт и счетов при сомнительных операциях. Банкам и платёжным организациям поручено внедрять антифрод-системы и контролировать крупные переводы.

По данным регулятора, эти мер направлены на выявление незаконных операций между физическими лицами, которые переводят деньги с карты на карту (p2p-платежи). К таким операциям относятся незаконные операции по азартным играм (тотализаторы, букмекерские конторы для ставок), случаи мошенничества и другие.

Центральный банк Узбекистана прокомментировал расширение перечня подозрительных операций, куда включён в том числе перевод денег с карты через мобильное приложение на другую карту или электронный кошелёк на сумму 500 БРВ (150 млн сумов или 1,08 млн руб.) и более в течение 30 дней.

22.02.2023 В августе 2022 года в структуре ГУВД Ташкента был создан Отдел по борьбе с преступностью в сфере информационных технологий. Его сотрудники занимаются профилактикой правонарушений, оперативно-розыскной и следственной деятельностью. В качестве основного направления определены предупреждение и пресечение преступлений в сфере ИТ.

В 2022 году количество преступлений в сфере информационных технологий увеличилось в 2 раза и составило 4332 случая по сравнению с 2021 годом. Из них 2747 преступлений относятся к киберкражам, 625 – к

кибермошенничеству, 874 – к преступлениям, связанным с наркотиками, совершенным с помощью ИТ.

По данным столичного ГУВД в связи с развитием современных технологий увеличилось количество фактов мошенничества и краж с банковских пластиковых карт. Так, согласно статистической информации, количество преступлений в сфере информационных технологий, совершенных в 2020 году, составило 106, в 2021 году – 2281.

Мошенники чаще всего используют следующие способы для кражи средств с карт:

34% – отправляют своим жертвам поддельные ссылки с предложениями финансовой помощи, получения онлайн-кредита или выигрышей, тем самым, получая секретный код или номер банковской карты;

22% – получают авансовые платежи, а после не выполняют оговоренные соглашения;

17% – представляются сотрудниками платежных компаний (Click, Payme и др.) или службы безопасности банка во время телефонных разговоров. Таким образом, они получают номера банковских карт или секретные коды;

14% – раскрывают секретный код или номер банковской карты через торговые онлайн-площадки;

9% – преступления совершаются через финансовые онлайн-биржи (Binance и др.).

21 декабря 2023 г. Президент Узбекистана Шавкат Мирзиёев на совещании по вопросам развития IT-отрасли поручил выработать единые требования кибербезопасности для платёжных сервисов. За последние одиннадцать месяцев в стране зафиксировано около 5500 преступлений в киберпространстве, из них 70% пришлось на мошенничество и кражи средств с банковских карт. В стране работают почти 50 платёжных сервисов, не все из которых соответствуют требованиям безопасности. Президент поручил сформулировать единые требования к финтех-сервисам и следить за их исполнением.

22 декабря 2023 г. Центральный банк Республики Узбекистан предупредил, что в последнее время отмечаются случаи звонков гражданам с неизвестных номеров от лиц, представляющихся сотрудниками Центробанка.Таким образом злоумышленники пытаются войти в доверие к собеседнику. Кроме того, в мессенджере Telegram был открыт фейковый канал Markaziy_Banki_uz. Через него мошенники предлагают гражданам онлайн- кредиты якобы от Центробанка, чтобы получить доступ к данным банковских карт и присвоить хранящиеся на них средства.