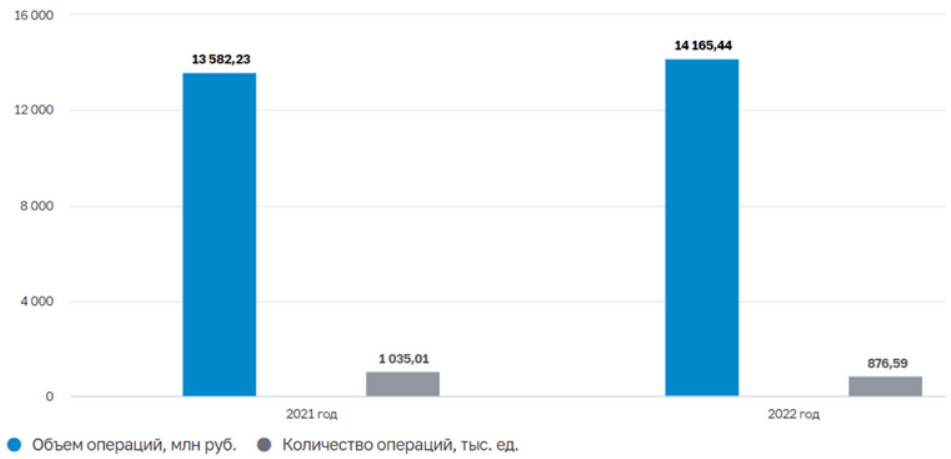
Общий объем и количество операций без согласия клиентов



Самым распространенным методом мошенников является социальная инженерия, ее доля в объеме операций, проведенных без согласия клиентов, в 2022 **году составила** 50,4%.

Если клиент банка самостоятельно перевел деньги мошенникам или предоставил им банковские данные, то банк не обязан возвращать похищенную сумму.

На рассмотрении законопроект «О внесении изменений в Федеральный закон О национальной платежной системе», позволяющий расширить возможности банков по возврату денежных средств.

Согласно данному законопроекту, оператор по переводу денежных средств обязан провести проверку операции на наличие признаков ее совершения без согласия клиента.

При наличии данных признаков оператор приостанавливает прием распоряжений клиента о переводе денежных средств на два дня.

По истечении двух дней оператор может совершить операцию по распоряжению клиента только при подаче повторного поручения и при условии отсутствия признаков совершения операции без согласия клиента.

ifg@fa.ru

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФМЦ ИФГ

Минфин России

ТИПОВЫЕ СЦЕНАРИИ СОЦИАЛЬНОГО ИНЖИНИРИНГА

Подготовлено
Федеральным методическим центром по финансовой грамотности населения Института финансовой грамотности на базе Финуниверситета в рамках проекта Минфина России

Мошенничество - хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. При этом под обманом понимается как сознательное искажение истины (активный обман), так и умолчание об истине (пассивный обман).

Социальная инженерия – совокупность методов хищения данных без использования технических средств.



Чаще всего, злоумышленники используют слабости человека или негативные черты характера – **жадность**(предложение о работе с высоким окладом), желание получить что-либо бесплатно, **страх** (за себя, за своих близких, когда говорят об угрозе их здоровья и тд.), **невнимательность**, излишнюю **доверчивость**.

Ключевой задачей социального инженера является атака на подсознание, т.е. фактически временный перевод жертвы в такое состояние, в котором она не способна рационально мыслить, и, таким образом, шире открывает окно возможностей для атаки.

ПОПУЛЯРНЫЕ ТИПЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ:

Телефонные звонки, в ходе которых злоумышленник пытается втереться в доверие к жертве и склонить её к совершению действий в своих интересах.

Фишинг - использование злоумышленником электронной почты для мошенничества, кражи денег или учетных данных жертвы.

Отправка жертве текстовых сообщений с целью вынудить её действовать в интересах атакующего.
В настоящее время термин часто подразумевает социальную инженерию посредством любого сервиса обмена текстовыми сообщениями, включая мессенджеры.

В 2022 году, с началом специальной военной операции на Украине мошенничество на основе социальной инженерии с территории Украины и не только стало масштабным – **используются не только технические средства для подмены номеров входящих звонков, но и полноценные контакт-центры с большим количеством задействованных сотрудников.**

Большое количество мошеннических звонков гражданам осуществляется от имени МВД, Центрального Банка и других государственных структур.

В 2023 г. Банк России предупредил о новой схеме.

Теперь злоумышленники не только звонят, но еще и отправляют на электронную почту сообщения с приглашением "на личный прием в Банк России".

Часто мошенники меняют электронный адрес того, кто отправляет сообщение, на вызывающий доверие. В этом случае злоумышленники указывают домен Банка России cbr.ru.

Такое приглашение на личный прием - один из поводов вступить в контакт с потенциальной жертвой и вывести ее на доверительный диалог.

Будьте бдительны, по своей инициативе Банк России
❌не приглашает граждан на личный прием,
❌его работники не звонят людям,
❌не направляют никому копии каких-либо документов,
❌не запрашивают персональные и банковские сведения,
❌не предлагают совершить какие-либо операции со счетом.

✅По любым банковским вопросам самостоятельно позвоните в банк по номеру телефона, указанному на оборотной стороне карты или на сайте кредитной организации.

✅ Расскажите о новых схемах своим близким.

Схемы постоянно меняются, мы будем держать вас в курсе: