Мошенники приспособили старые виды мошенничеств под новые экономические условия

Аферисты подстраиваются под текущую повестку дня и активно начали использовать социально-экономическую ситуацию в стране и мире для выманивания сбережений у населения. Вместе с экспертом Центра финансовой грамотности НИФИ Минфина Ольга Дайнеко разберемся что надо знать, чтобы не попасть на удочку мошенника.

«Мошенничество с открытием счетов в «надежных иностранных банках» появилось не сегодня, сменились лишь аргументация по «открытию счета» для потенциального «клиента» или, вернее сказать, жертвы. Если раньше это происходило чаще под предлогом получения большого дохода (лже-брокеры с инвестиционными счетами), то сегодня предлагают таким образом скрыть доходы и накопления в «далеких валютных офшорах»», - говорит Ольга.

К делу такие мошенники нередко подходят серьезно, создавая целую бизнес-модель: запускают страницу веб-сайта якобы «банка», организовывают «горячую линию» кредитной организации, где действительно отвечают на вопросы. Все это делается, чтобы создать образ солидной и надёжной организации. Однако при открытии счета начинают появляться триггеры, которые должны насторожить. Как говорит эксперт, они предлагают открыть счет только удаленно и напирают на надежность тем, что находятся вне контроля мегарегулятора – Банка России, ИФНС и прочих надзорных органов. Результатом «открытия» таких счетов, в лучшем случае будет гарантированное похищение личных и персональных данных (в том числе реальных банковских), в худшем – добавится кража денежных средств.

Какую информацию требуют аферисты?

Злоумышленники выманивают личные данные своей жертвы:

- данные паспорта – по словам «представителя банка» эта информация необходима для присвоения индивидуального кода счета (без имени)
- данные существующих банковских счетов/карт).

Мошенники предупреждают, что для безопасности деньги на новый «счет» будут поступать через посредника. Вводя в заблуждения клиента в процессе переговоров, будут потребоваться и СМС или пуш-уведомления (для «подтверждения транзакции» на созданный «счет»). Каждый раз мошенники могут придумывать новые уловки с одной целью – добраться до сбережений жертвы. Ряд афер даже сложно распознать изначально, так как изначально жертва может увидеть свои деньги на счету в лже-банке. Однако далее наступает череда проблем: что-то идет не так, то «нужно немного подождать», сложности с переводов ввиду санкций, проверка платежа, необходимость открыть еще один «резервный счет» и т.д..

Как обезопасить себя?

В этой ситуации важно вовремя сказать себе «СТОП», а лучше при первых словах собеседника по телефону о «безопасных счетах» положить трубку. Предлагаемая «услуга» попросту невозможна - чудес не бывает.

«Память о 90-х прошлого века сыграет плохую службу, поскольку законодательство с тех пор совершенствовалось все эти десятилетия. Важно понимать, что для мошенника это высокооплачиваемая работа, которая предполагает высокий уровень навыков социальной инженерии, психологии и владение цифровыми технологиями. Искать правду, оставшись у разбитого корыта, будет чрезвычайно сложно», - предупреждает Ольга Дайнеко. Помните - высокотехнологичное мошенничество имеет сложный алгоритм доказывания совершения противоправных действий. Кроме того, зачастую все посредники мошеннических действий находятся вне досягаемости правоохранительных структур, вне их юрисдикции и вернуть украденные деньги будет практически невозможно.

Аферисты подстраиваются под текущую повестку дня и начали использовать социально-экономическую ситуацию в стране и мире.

Эксперт Центра финансовой грамотности НИФИ Минфина Ольга ДАЙНЕКО о том, что надо знать, чтобы не попасть на удочку мошенника.

Мошенничество с открытием счетов в «надежных иностранных банках» появилось не сегодня, сменились лишь аргументация – сегодня жертве предлагают таким образом скрыть доходы и накопления в «далеких валютных офшорах».

СХЕМА ОБМАНА:
мошенники запускают страницу веб сайта якобы «банка»
организовывают «горячую линию» кредитной организации.
открыть счет предлагается только удаленно и жертву убеждают в надежности тем, что находятся вне контроля мегарегулятора – Банка России, ИФНС и прочих надзорных органов.
результат «открытия» таких счетов – гарантированное похищение личных и персональных данных (в том числе-реальных банковских) + кража денежных средств.

Какую информацию требуют аферисты?
✓данные паспорта – по словам «представителя банка» эта информация необходима для присвоения индивидуального кода счета (без имени)
✓данные существующих банковских счетов/карт)

МОШЕННИКИ ПРЕДУПРЕЖДАЮТ, ЧТО ДЛЯ БЕЗОПАСНОСТИ ДЕНЬГИ НА НОВЫЙ «СЧЕТ» БУДУТ ПОСТУПАТЬ ЧЕРЕЗ ПОСРЕДНИКА.
Вводя в заблуждения клиента в процессе переговоров, будут потребоваться и СМС или пуш-уведомления (для «подтверждения транзакции» на созданный «счет»). Каждый раз мошенники могут придумывать новые уловки с одной целью – добраться до сбережений жертвы. Однако далее наступает череда проблем: что-то идет не так, то «нужно немного подождать», сложности с переводов ввиду санкций, проверка платежа, необходимость открыть еще один «резервный счет» и т.д..

КАК ОБЕЗОПАСИТЬ СЕБЯ?
Важно вовремя сказать себе «СТОП», а лучше при первых словах собеседника по телефону о «безопасных счетах» положить трубку.

Помните - высокотехнологичное мошенничество имеет сложный алгоритм доказывания совершения противоправных действий. Кроме того, зачастую все посредники мошеннических действий находятся вне досягаемости правоохранительных структур, вне их юрисдикции и вернуть украденные деньги будет практически невозможно.