Каспийский Трубопроводный Консорциум
Caspian Pipeline Consortium
Каспий Құбыр Консорциумы

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ КТК

№ 98

В ПРЕДДВЕРИИ НОВОГО ГОДА МОШЕННИКИ АКТИВИЗИРОВАЛИ СВОЮ РАБОТУ ПО ОТЪЕМУ ДЕНЕЖНЫХ СРЕДСТВ У ДОБРОПОРЯДОЧНЫХ ГРАЖДАН. ПРИ ЭТОМ ПРИДУМЫВАЮТСЯ НОВЫЕ УЛОВКИ ДЛЯ ВЫМАНИВАНИЯ ДЕНЕГ И ПЕРСОНАЛЬНЫХ ДАННЫХ.

Ниже Управление Корпоративной Безопасностью (УКБ) расскажет о некоторых распространенных сценариях, которые используют злоумышленники по телефону.

СТРАХОВАНИЕ ЕДИНОГО МЕЖБАНКОВСКОГО СЧЕТА

Абоненту звонят от имени правоохранительных органов или сотрудников банка и пугают тем, что его персональные данные скомпрометированы. Преступники сообщают, что списание денег производилось не со счета банка, а по «единому внутрибанковскому счету», который доступен только «сотрудникам» кредитной организации. Далее с жертвой якобы связывается «работник» банка. Чтобы вернуть средства, он предлагает застраховать общую сумму на «едином счете», которого на самом деле не существует. Для этого жертву вынуждают перевести деньги на «безопасный счет», который на самом деле принадлежит мошенникам.

УГОЛОВНОЕ ДЕЛО

Во время звонка мошенники представляются сотрудниками Центрального банка или правоохранительных органов и сообщают абоненту об уголовном деле, которое на него завели по заявлению Банка России. Чтобы убедить жертву в правдоподобности истории, мошенник может направить в мессенджер или на электронную почту фото поддельного документа о проведении оперативно-разыскных мероприятий. Жертва раскрывает запрошенные данные о себе, своих счетах и последних операциях. С помощью этой информации злоумышленники могут похитить деньги или взять кредит.

ОФОРМЛЕНИЕ КРЕДИТА

Злоумышленники звонят от имени банка и сообщают об одобренном кредите. Но есть условие: чтобы получить деньги, клиент должен внести первый платеж на погашение кредита или оплатить страховку. Мошенники настаивают на дистанционном оформлении договора из-за того, что рядом с клиентом нет отделения нужного «банка». В результате клиент сообщает личные данные и лишается средств.

ЧУЖОЙ ДОЛГ

Мошенники звонят от имени сотрудника Центрального банка или полиции и сообщают собеседнику, что на него взят кредит. Жертва заявляет об ошибке. В качестве выхода из ситуации злоумышленники предлагают оформить новый заем на максимальную сумму, что якобы поможет «обнулить» возможность брать кредиты на имя клиента третьими лицами. По такому же сценарию жертву могут вынудить раскрыть личные данные и перевести средства на «безопасный счет».

ИСПОЛЬЗОВАНИЕ VPN

Схема заключается в том, что мошенники уговаривают потенциальных жертв заходить на их заблокированные сайты (нелегальные сайты, финансовые пирамиды) с использованием VPN-сервисов. Мошенники в телефонном разговоре убеждают перейти на их сайт только через VPN, аргументируя это якобы необходимостью специального шифрования. Не включайте VPN при доступе к электронной почте или финансовой информации; тот, кто контролирует VPN-сервер, может контролировать и трафик. При использовании финансовых сервисов отключайте VPN на своем телефоне или планшете. Даже с учетом того, что обмен информацией, в частности, с банковскими приложениями происходит в шифрованном виде, все равно остаются риски компрометации.

КАК РАСПОЗНАТЬ ОБМАН?

Прервите разговор, заблокируйте номер мошенника и перезвоните в банк самостоятельно по номеру, указанному на официальном сайте, чтобы перепроверить полученную информацию.

Если звонок показался вам сомнительным и возникло малейшее подозрение:

- не сообщайте данные банковской карты;
- не поддавайтесь на угрозы;
- не вступайте в переписку;
- не перезванивайте на подозрительный номер.

Будьте бдительны!