«Звонок сотрудника банка или правоохранительного органа»

Звонок на телефон сотовой связи любого оператора. Мошенники звонят, представляются сотрудниками банка или правоохранительных органов и спокойным, очень уверенным, поставленным голосом начинают говорить, что со счётом потерпевшего происходят какие-то операции. Преступники чётко понимают, что разговор может идти по нескольким направлениям, поэтому всегда готовы поддержать диалог в зависимости от того, как будет вести себя потенциальная жертва. Для придания достоверности могут создать шум работающего офиса, переключать одного представителя псевдобанка на другого, соединять якобы с сотрудниками правоохранительных органов. При этом чаще звонят через мессенджеры «Ватсап», «Вайбер», «телеграмм». Для придания достоверности могут использовать символику Центробанка, МВД или других правоохранительных структур. Может быть использована технология подмены номеров.

Важно помнить, что ни следователь, ни оперуполномоченный, ни сотрудник прокуратуры, ФСБ или другого государственного органа не будет вам звонить по телефону. Если вам представляются так, сразу же положите трубку. Никто из банка не будет звонить и говорить, что с вашим счётом происходят какие-то сомнительные операции. Если остаются сомнения - позвоните по номеру телефона, указанному на оборотной стороне карты. Если сомнения не развеялись, то следует прийти в банк и убедиться, что со счётом ничего не происходит.

«Программа удаленного доступа»

Мошенник под видом сотрудника банка или правоохранительного органа (портала госуслуг, МФЦ, оператора сотовой связи и пр.) якобы для защиты от несанкционированного кредита или списания со счета жертвы денежных средств, предлагает установить программу удаленного доступа. При этом преступник будет называть эту программу как «Приложение по борьбе с мошенничеством», «Техническая поддержка банка», «Программа защиты от мошеннических действий» и т.п.

После того как гражданин установит эту программу, от него потребуют назвать id – уникальный идентификатор, который поступит в СМС-сообщении. Передав эти данные мошеннику, человек предоставит ему все права на любые действия в своем компьютере или телефоне, в своих личных кабинетах. Неизвестные смогут оформить кредит, перевести денежные средства на подконтрольный им счет, отключить услуги у оператора сотовой связи и пр.

Чтобы не стать жертвой преступников:

- не устанавливайте по указанию неизвестных какие-либо программы, приложения в своих устройствах;
- не сообщайте никому коды, пароли, идентификаторы, имя пользователя для банковской учетной записи, иные личные пароли;
- если гражданин осознал, что совершил недопустимые действия по установке программ удаленного доступа, необходимо удалить программу из устройства (сбросить систему до заводских настроек), обратиться в банк для блокирования платежных средств, сообщить в полицию.

«Заработок на бирже»

Потерпевший находит в сети Интернет предложение пассивного дохода (инвестиции в акции, игра на курсе при покупке-продаже валюты, в том числе и цифровой, или иные активы), оставляет свои данные (ФИО, номер телефона). Позже на связь выходят лица, которые уверяют в возможности получения прибыли с минимумом усилий. Для этого переключают на «брокеров» («трейдеров», «дилеров»), которые за небольшую плату будут якобы от лица жертв «заключать сделки», «торговать активами».

Потерпевшему они предлагают зарегистрироваться на сайте, создать личный кабинет, криптокошелек. Жертва вносит денежные средства и видит на экране «пополнение счета». В первый раз клиент при обращении к такому «брокеру» даже сможет обналичить небольшую сумму якобы заработанных средств. Но это уловка мошенников, для того чтобы продемонстрировать «работоспособность схемы», войти в еще большее доверие к потерпевшему и получить с него как можно больше денег.

Если потерпевший в дальнейшем пожелает вывести уже большие «заработанные» деньги со счета, под различными предлогами «брокеры» попытаются получить с него дополнительные средства (на оплату налогов, комиссий, страховок, услуг инкассации и.т.п.), но вывода средств не произойдет. В конечном итоге связь с «брокерами» прекратится, денежные средства останутся у них.

Полиция рекомендует не верить предложениям в сети Интернет по получению легкого, быстрого и высокого дохода. Помните, что такого просто не бывает. Нельзя доверять свои деньги незнакомцам. Для получения реального дохода в этой сфере требуются определенные знания и навыки в биржевых торгах, игре на фондовом рынке.

«Родственник в беде»

На домашний телефон поступает звонок. Потенциальной жертве кажется, что она узнает в звонящем голос близкого человека, либо собеседник представляется сотрудником полиции (ГИБДД, следователя). В разговоре сообщается о том, что родственник или знакомый жертвы стал виновником ДТП, либо совершил иное противоправное деяние. Для помощи самому родственнику, за невозбуждение в отношении него уголовного дела или на лечение пострадавших необходимо передать крупную сумму курьеру. После передачи денег курьер переводит деньги на счета кураторов, оставляя себе оговоренный процент.

- Необходимо проинструктировать своих пожилых родственников, а потом систематически напоминать им о подобных попытках обмана;
- не передавать, не переводить деньги незнакомцам;
- при получении информации о возникших неприятностях с родственником - связаться с ним, со своими родными, иными близкими;
- настоящие сотрудники правоохранительных органов никогда не потребуют для урегулирования вопросов с вас денежные средства, так поступают только мошенники!

КИРОВСКАЯ ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

ТАК МОШЕННИКИ ОБМАНЫВАЮТ СВОИХ ЖЕРТВ ПО ТЕЛЕФОНУ:

«СОТРУДНИК БАНКА»:
«КТО-ТО ПЫТАЕТСЯ ПОХИТИТЬ СБЕРЕЖЕНИЯ СО СЧЕТА И ОФОРМИТЬ КРЕДИТ ОТ ВАШЕГО ЛИЦА. ПЕРЕВЕДИТЕ ВСЕ ДЕНЬГИ НА «РЕЗЕРВНЫЙ» СЧЕТ».

«СОТРУДНИК ПОЛИЦИИ»:
«ВЫ ДОЛЖНЫ ПОМОЧЬ НАМ НАЙТИ ПРЕСТУПНИКОВ! ВЫПОЛНЯЙТЕ ИНСТРУКЦИИ ЗАКРЕПЛЕННОГО ЗА ВАМИ СПЕЦИАЛИСТА!»

НЕ ВЕРЬТЕ: ЭТО ОБМАН!

☑ Преступники часто звонят в мессенджерах (WhatsApp, Viber, Telegram), подменяя свой номер телефона на номер полиции или банка. Они могут знать ваши личные данные и номер карты.

☑ Настоящие сотрудники полиции и банка не требуют от граждан переводить сбережения куда-либо.

☑ При любых сомнениях завершите разговор и перезвоните самостоятельно в полицию или банк. Номер телефона банка обычно указан на банковской карте.

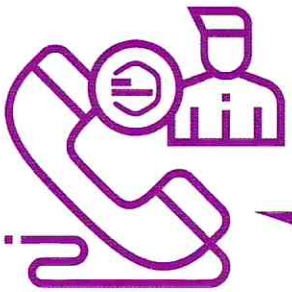
ЕСТЬ ПРОБЛЕМЫ? ЗВОНИТЕ В ПОЛИЦИЮ!

☎ 02/ 102

УМВД России по Кировской области
Правительство Кировской области

КИРОВСКАЯ ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

ТАК МОШЕННИКИ ОБМАНЫВАЮТ СВОИХ ЖЕРТВ ПО ТЕЛЕФОНУ:



«НАЗОВИТЕ ЛОГИН И ПАРОЛЬ ОТ ЛИЧНОГО КАБИНЕТА ПОРТАЛА **«ГОСУСЛУГИ»**, А ТАКЖЕ КОД ИЗ СМС ДЛЯ ПОЛУЧЕНИЯ ПИСЬМА».

НЕ ВЕРЬТЕ: ЭТО ОБМАН!

☑ Передавать логин, пароль от личного кабинета и коды из смс от «Госуслуг» нельзя никому!

☑ С их помощью преступники смогут завладеть информацией о ваших документах, оформить от вашего лица займы в микрокредитных организациях и похитить деньги.

☑ Сотрудники центров «Мои документы» или сервиса «Госуслуги» не звонят гражданам с такими просьбами.

ЕСТЬ ПРОБЛЕМЫ? ЗВОНИТЕ В ПОЛИЦИЮ!

☎ 02/ 102

УМВД России по Кировской области
Правительство Кировской области