Одни из самых популярных видов мошенничества сегодня – телефонные и через сеть Интернет. Практически ежедневно люди становятся жертвами злоумышленников. Чтобы уберечь себя и своих близких, необходимо знать и помнить наиболее распространенные схемы присвоения Ваших денег.

Мошенники придумали очередные схемы обмана. Будьте начеку!

ОПАСНОЕ «ДА»

Мошенник звонит и задаёт нейтральный вопрос. Например, уточняет, с тем ли человеком он разговаривает: «Татьяна Ивановна?» Или: «Вы хорошо слышите меня?» Конечно, вы, не задумываясь, отвечаете «да». Потом аудиозапись слова «да» монтируют с другими фрагментами записанного разговора так, чтобы результат можно было использовать для голосового подтверждения транзакции. И с ваших счетов пропадают деньги.

Что делать?

Никогда не говорите «да» в телефонных разговорах неизвестным людям. Если вам звонят незнакомцы, лучше вообще не вступать в диалог.

СМЕНА ТЕЛЕФОНА

Вам звонят из «банка», часто очень известного, клиентом которого вы, возможно, являетесь, и говорят, что поступила заявка на смену телефона, привязанного к онлайн-банку. Вы, конечно, отвечаете, что не подавали такую заявку, после чего вас переводят на службу безопасности, которая выуживает из вас данные, необходимые для взлома личного кабинета.

Что делать?

Даже если номер телефона, с которого звонят, совпадает с банковским, не ведите диалогов. Сразу сами перезванивайте в банк и уточняйте информацию. Мошенники подменяют номера при звонках и даже умеют присылать с них СМС.

ПРОСТО ОПРОС

Под видом опроса от банка или предложения новых услуг мошенник выманивает у жертвы конфиденциальные данные банковской карты, или код из СМС, или пароли из мобильного приложения банка.

Что делать?

Не нужно участвовать ни в каких опросах по телефону

ДВА ЗВОНКА

Жертве звонят «из банка» и предлагают взять кредит. Человек отказывается. Через пару дней поступает второй звонок из того же «банка» и сотрудник говорит, что кредит одобрен и скоро деньги будут переведены на его счёт. Человек связывает в уме эти два звонка и думает, что его подставили. Он сообщает «оператору», что не брал кредит. Тогда его переводят на «службу безопасности», она убеждает жертву всё-таки взять уже одобренный заем и перевести на «безопасный счёт», чтобы деньги не достались мошенникам, которые вот-вот возьмут кредит на его имя. Таким образом человек берёт кредит и переводит его мошенникам.

Что делать?

Запомните, что нет никаких безопасных счетов. Узнайте название банка и сами позвоните туда, чтобы убедиться, что на ваше имя никто не берёт кредит.

РОБОТ-МОШЕННИК

Мошенник, звонящий якобы от банка, хочет выудить у вас нужную информацию, но, чтобы у вас не закрались подозрения, говорит: «Вы не должны сообщать данные мне, это конфиденциально! Я сейчас переключу вас на робота, назовите код (или пароль) ему. Система защищена, это безопасно!» Конечно, это враньё.

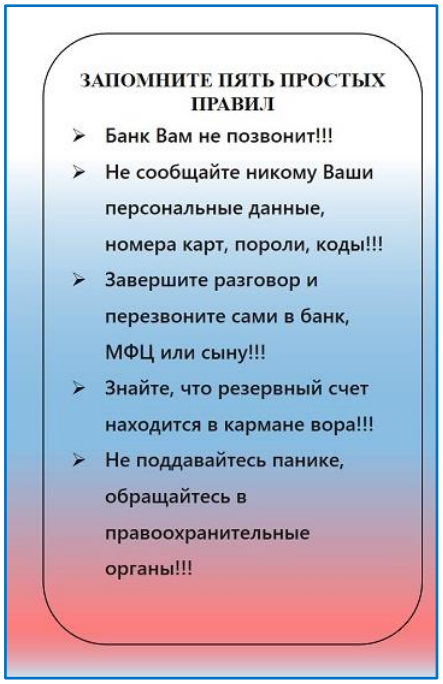
Что делать?

Ни людям, ни роботам – никому не сообщайте данные своей карты, пароли и коды из СМС.

ВАЖНО!

Если вы всё-таки попались на удочку мошенников, срочно обращайтесь в банк, от имени которого вам звонили! Возможно, там смогут остановить транзакцию.

Рекомендации
Надежды Кузнецовой, юриста



Наш адрес:
с. Юсьва,
ул. Красноармейская, 21
тел. 2-71-88, 2-84-33
E-mail: bib- uswa@mail.ru
Сайт библиотеки: http://usvalib.ru/
Режим работы:
С 09.00 до 18.00 ч.
Суббота: с 10.00 до 16.00 ч.
Выходной день: воскресенье
Тираж: 10 экз.
Составитель: Казанцева Л.Н.,
заведующий информационно-библиографическим сектором

Муниципальное бюджетное учреждение культуры «Юсьвинская централизованная библиотечная система»

Новые
телефонные аферы
Будьте бдительны!

с. Юсьва
2022