УВД ГОМЕЛЬСКОГО ОБЛИСПОЛКОМА
УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ
КРИМИНАЛЬНОЙ МИЛИЦИИ

ОПОРНЫЙ ПЛАН-КОНСПЕКТ

Тема:
«**ВИШИНГ**»

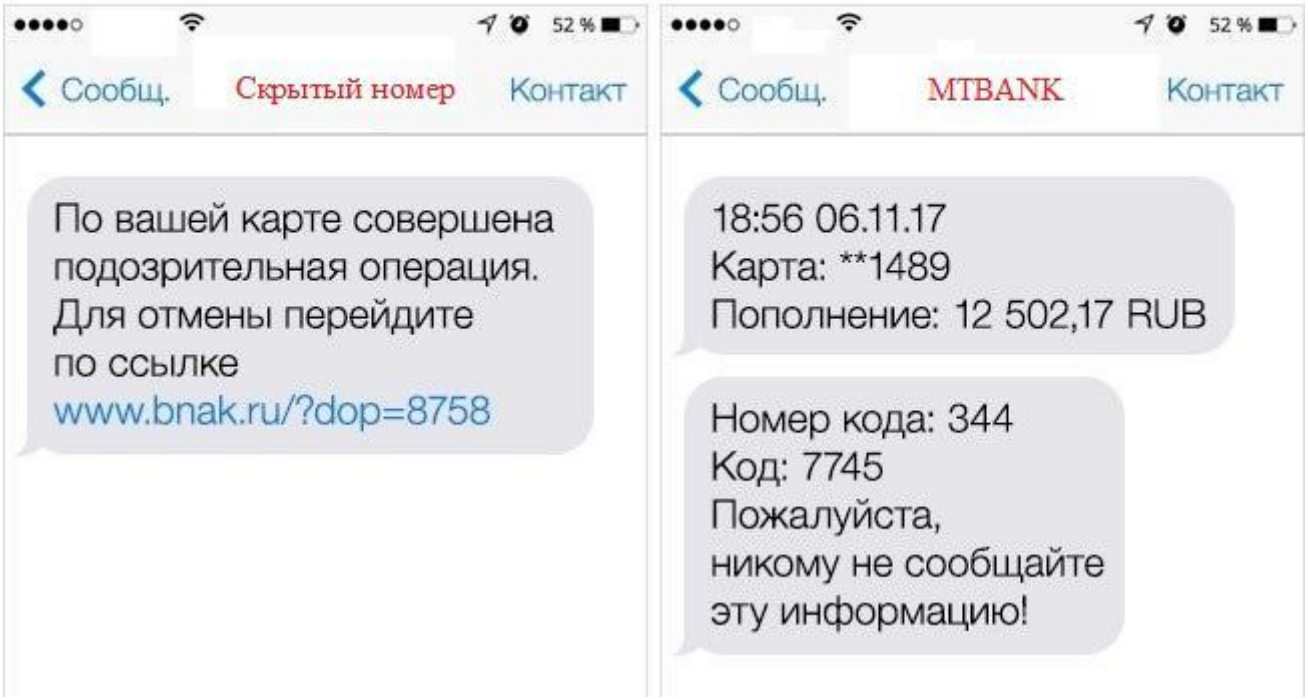
Гомель

«**ВИШИНГ**» — это один из методов совершения противоправных деяний с использованием социальной инженерии, который заключается в том, что злоумышленник, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т.д.), под разными предлогами выманивает у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определенных действий со своим карточным счетом/платежной картой.

ЗВОНОК ПОСТУПАЕТ С АНОНИМНОГО НОМЕРА ИЛИ НОМЕРА СХОЖЕГО С НОМЕРОМ БАНКА.

Сотрудники банка не вправе выяснять входе телефонной беседы конфиденциальные сведения о клиенте (полный номер банковской платежной карты, срок ее действия, CVV-код, личный номер паспорта клиента, содержание СМС-сообщений от банка, и т.п.).

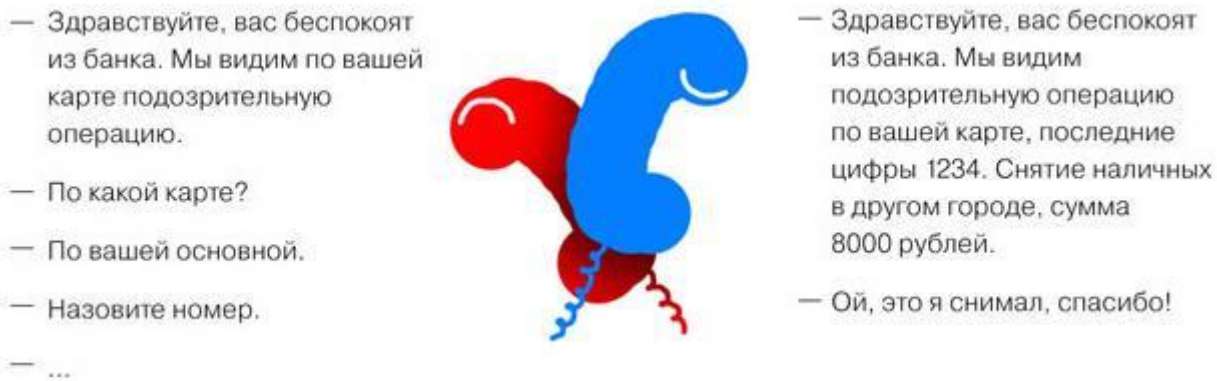
СМС ЯКОБЫ ОТ БАНКА ПРИХОДИТ В НОВУЮ ПЕРЕПИСКУ.



Слева — мошенник, справа — банк.

Смс из банка тоже приходят с одного, двух номеров, которые вам уже знакомы. В любом случае не спешите переходить по ссылкам в сообщении.

СОБЕСЕДНИК НЕ МОЖЕТ ОТВЕТИТЬ НА ПРОСТЫЕ ВОПРОСЫ.

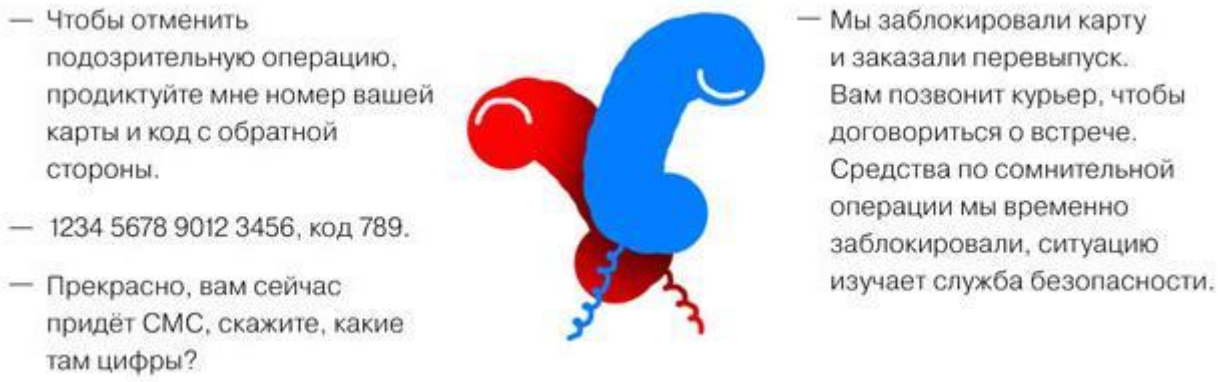


Слева — мошенник, справа — банк.

Сотрудник банка видит на экране компьютера всю информацию о клиенте, которая есть в базе банка.

Если собеседник не готов ответить на простой вопрос, например, назвать остаток по карте или последнюю операцию, то вероятно это мошенник.

СОБЕСЕДНИК СПРАШИВАЕТ ДАННЫЕ КАРТЫ ИЛИ СМС-КОД.

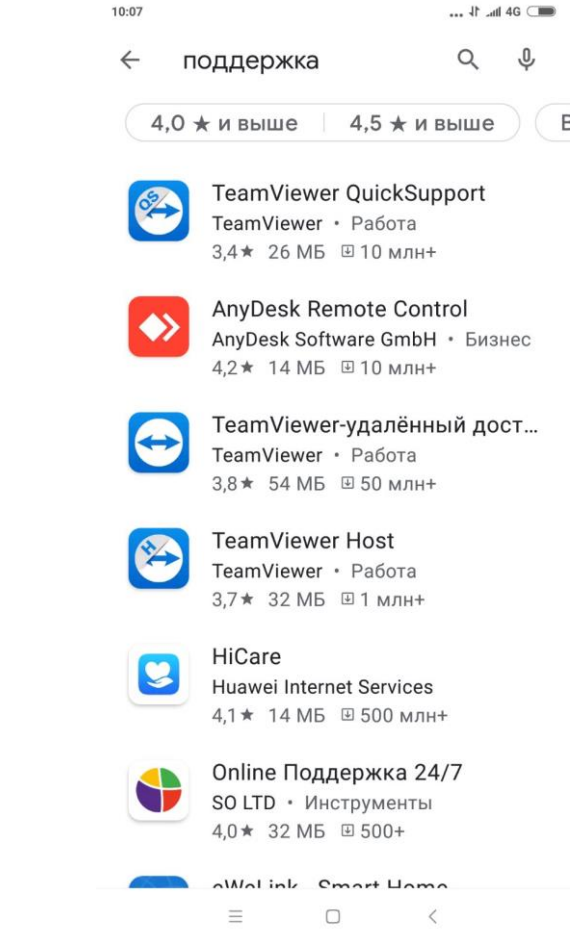


Слева — мошенник, справа — банк.

Смс-код — один из главных паролей. Сотрудники банка никогда его не спросят, так же как и CVV на обратной стороне карты.

Если вам позвонили якобы из банка, и вы хотите убедиться в надёжности собеседника, спросите его имя. После этого перезвоните по официальному номеру банка — тому, который указан на карте и на сайте, — и попросите переключить на человека, который вам звонил.

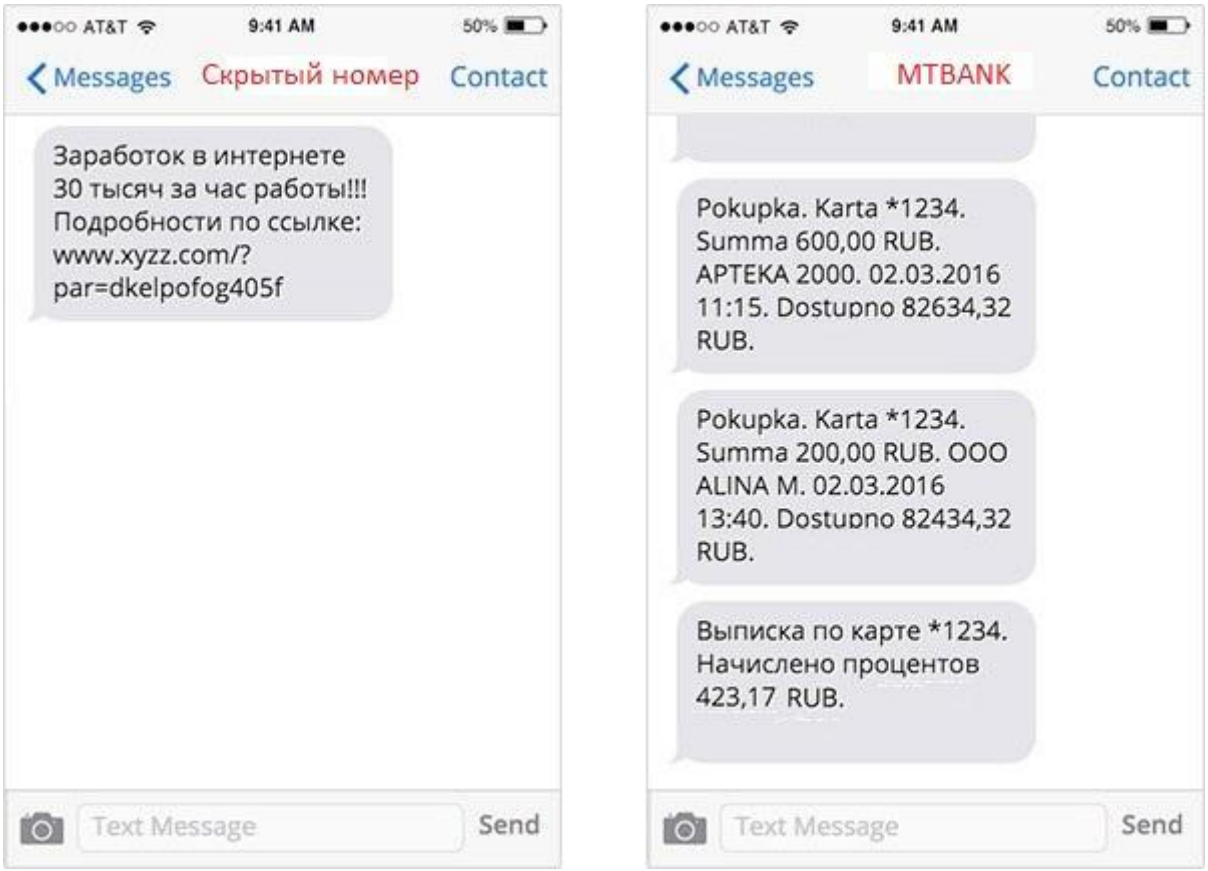
СОБЕСЕДНИК ПРОСИТ ВАС СКАЧАТЬ КАКИЕ-ЛИБО ПРИЛОЖЕНИЯ С МАГАЗИНА ПРИЛОЖЕНИЙ “PLAY MARKET” ИЛИ “APP STORE”.



Программное обеспечение “Any Desk” и “TeamViewer” — предназначены для удаленного доступа и управления компьютерами и другими устройствами под управлением Windows, MacOS и Linux. Сотрудники банка никогда не просят устанавливать какие-либо приложения.

Если вам позвонили якобы из банка и сообщают о попытках совершения подозрительных в отношении Вас операций, убеждая при этом, что отменить данные операции возможно только после скачивании с использованием магазина приложений “Play Market” и “App Store” программ под названием “Any Desk”, “TeamVeiwer”, введя для этого в командной строке слово “поддержка”. При поступлении звонка с подобным предложением, прекратите данный разговор, и перезвоните по официальному номеру банка — тому, который указан на карте и на сайте, — для того чтобы убедиться, что никакой сотрудник вам не звонил.

ВАМ ОБЕЩАЮТ ВЫГОДУ БЕЗ УСИЛИЙ.



Слева — мошенник, справа — банк.

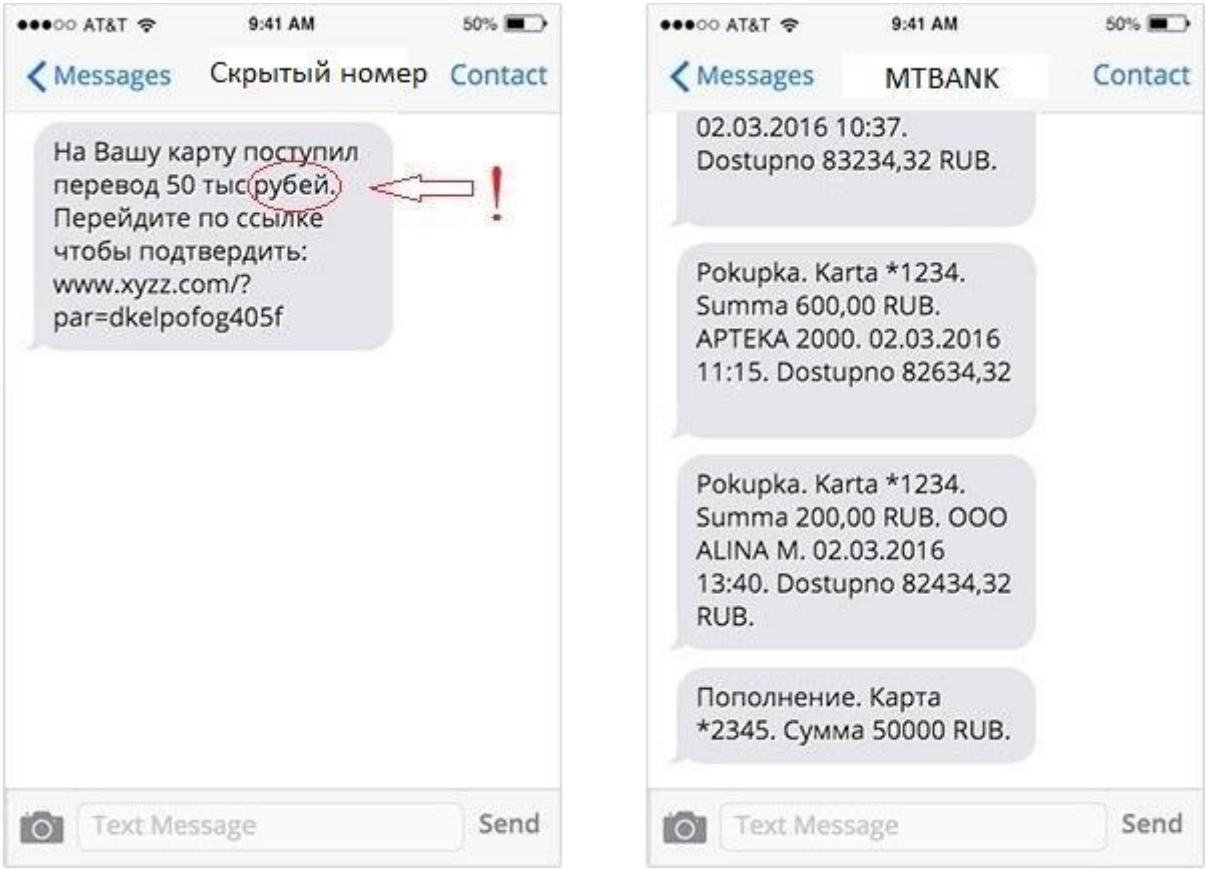
Чтобы завлечь жертву, мошенники обещают солидный доход быстро и без усилий: суперприбыльную работу, беспроигрышные конкурсы, курсы, которые сделают всех богатыми. Но мошенники могут взять предоплату за обучение и пропадут. Или посулят приз и выманят у вас данные карты якобы для перевода выигрыша.

СОБЕСЕДНИК ТОРОПИТ ВАС ИЛИ ПЫТАЕТСЯ ПЕРЕУБЕДИТЬ.

Слева — мошенник, справа — банк.

Сотрудник банка никогда не будет настаивать или торопить клиента.

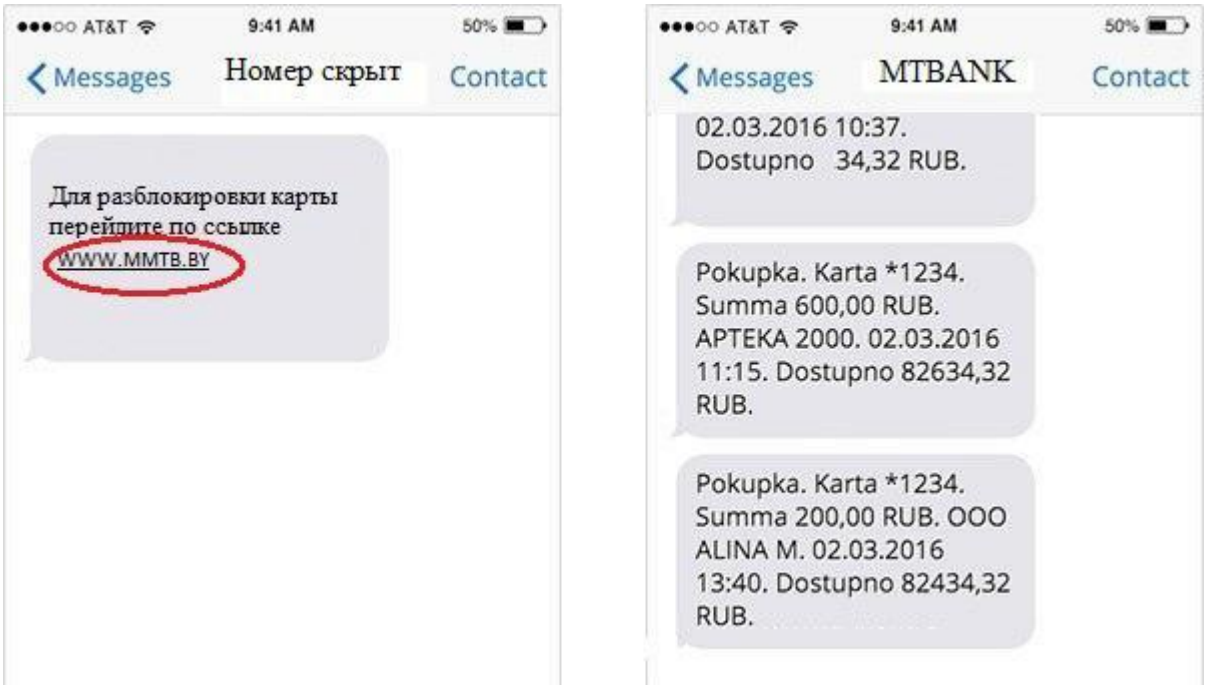
ОШИБКИ В СООБЩЕНИИ.



Слева — мошенник, справа — банк.

У банка есть бдительные редакторы, а вот мошенники пишут с ошибками. Не дайте неграмотному преступнику вас обмануть.

ИМЯ ОТПРАВИТЕЛЯ НАПИСАНО НЕПРАВИЛЬНО.



Слева — мошенник, справа — банк.

Мошенники регистрируют адреса, похожие на названия банков. Тут срабатывает особенность восприятия: мы считываем смысл слов даже, если буквы в них перепутаны. Когда приходит такое смс, вас должно насторожить ещё и то, что сообщение оказалось в новой переписке.

ПРОСТЫЕ ПРАВИЛА БЕЗОПАСНОСТИ:

- Если вы хотите убедиться в надёжности собеседника, спросите его имя, а после перезвоните в банк по официальному номеру и попросите переключить на человека, который вам звонил.
- Если не уверены в собеседнике, попросите его назвать номер карты или остаток на счёте.
- Не паникуйте, если вам сообщают о блокировке счета. Позвоните в банк по номеру, указанному на сайте или на карте.
- Не обращайте внимание на обещания лёгких денег или выгоды без усилий.
- Если собеседник торопит вас или спрашивает смс-код, то вы говорите с мошенником!
- Внимательно читайте сообщения из банка. Мошенники используют имена отправителей, похожие на названия банков, и допускают ошибки в тексте.