УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНЕОСТИ
КРИМИНАЛЬНОЙ МИЛИЦИИ
УВД ГОМЕЛЬСКОГО ОБЛИСПОЛКОМА

ОПОРНЫЙ ПЛАН-КОНСПЕКТ

Тема:
«**ВИШИНГ**»

Гомель 2023 г.

«**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.

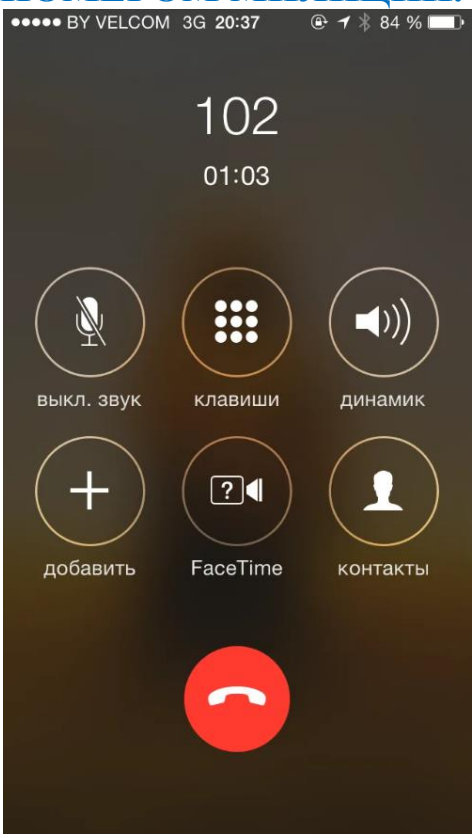
ЕСЛИ ПОСТУПАЕТ ЗВОНОК В МЕССЕНДЖЕРЕ С АНОНИМНОГО НОМЕРА ИЛИ НОМЕРА СХОЖЕГО С НОМЕРОМ БАНКА.

Аферист звонит по телефону и представляется сотрудником безопасности банка. Сообщает, что с карты клиента был совершён платёж, который вызвал подозрения. Уточняет, делал ли человек такую операцию (естественно, нет). Предлагает вернуть деньги, для чего просит сообщить номер карты, срок действия и код безопасности — то есть то, что сообщать нельзя. Нередко мошенники отправляют SMS с текстом: «Ваша карта заблокирована, отправьте код для разблокировки», «Вам положена компенсация, для получения пришлите код». Также под надуманным

предлогам убеждают установить программу удаленного доступа «AnyDesk», «RustDesk», говоря, что она нужна для отмены незаконного платежа, а потом с помощью данной программы осуществляют переводы денежных средств с банковских карт потерпевших.

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 либо иные личные данные), а также просить установить какие-либо программы на устройство (телефон, компьютер).

ЕСЛИ ПОСТУПАЕТ ЗВОНОК В МЕССЕНДЖЕРЕ С АНОНИМНОГО НОМЕРА ИЛИ НОМЕРА СХОЖЕГО С НОМЕРОМ МИЛИЦИИ.



Не редки случаи когда звонивший может представится сотрудником милиции или следственного комитета (при этом называет фамилию, имя и отчество реально существующего сотрудника), и предложить поучаствовать в «СПЕЦОПЕРАЦИИ» по поимке преступников из банка. При этом злоумышленник убеждает человека перевести деньги (либо свои сбережения, либо обратиться в банк для получения кредита) на расчетный счет, который он ему предоставит. По легенде «лжемилиционера» – это необходимо для того, что бы когда сотрудник банка будет осуществлять их снятие, его задержали с поличным. При это потерпевшего убеждают в

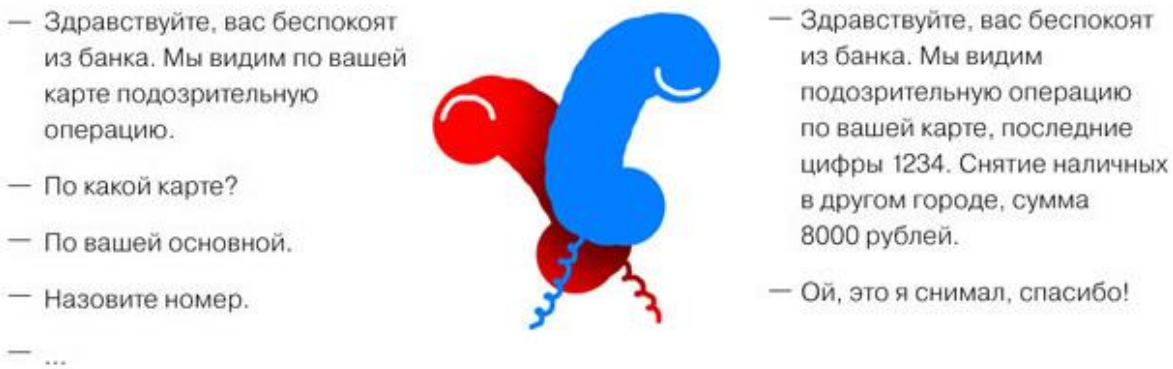
том, что деньги, взятые в кредит в банке, будут возвращены без каких-либо вычетов процентов за его пользование.

Также от «лжемилиционеров» может поступить информация, что в отношении гражданина в настоящее время совершаются противоправные действия со стороны злоумышленников, которые хотят оформить на его имя кредит и попытаться завладеть предоставленными банком денежными средствами. При этом собеседник никаких личных данных у человека не спрашивает и все время акцентирует внимание на то, что в республике в настоящее время совершаются очень много звонков от интернет-мошенников. Затем «лжемилиционеры» переключают потерпевшего на якобы сотрудника «Ассоциации белорусских банков» для того чтобы заблокировать открытый на его имя кредит, и в этот момент уже данный сотрудник, начинает уточнять паспортные данные либо выманивать реквизиты банковской платежной карты, чтобы в дальнейшем осуществить доступ к его расчетному счету и совершить хищение денежных средств.

Сотрудники правоохранительных органов никогда не предлагают гражданам участвовать в каких-либо операциях, не осуществляют переключение на сотрудников «Ассоциации белорусских банков».

Во всех ситуациях когда Вам звонят по телефону и уточняют какую-либо личную информацию (реквизиты паспорта, банковской карты и т.п.) необходимо ***ПОЛОЖИТЬ ТРУБКУ ТЕЛЕФОНА*** и самому перезвонить в банк либо милицию.

ЕСЛИ СОБЕСЕДНИК НЕ МОЖЕТ ОТВЕТИТЬ НА ПРОСТЫЕ ВОПРОСЫ.

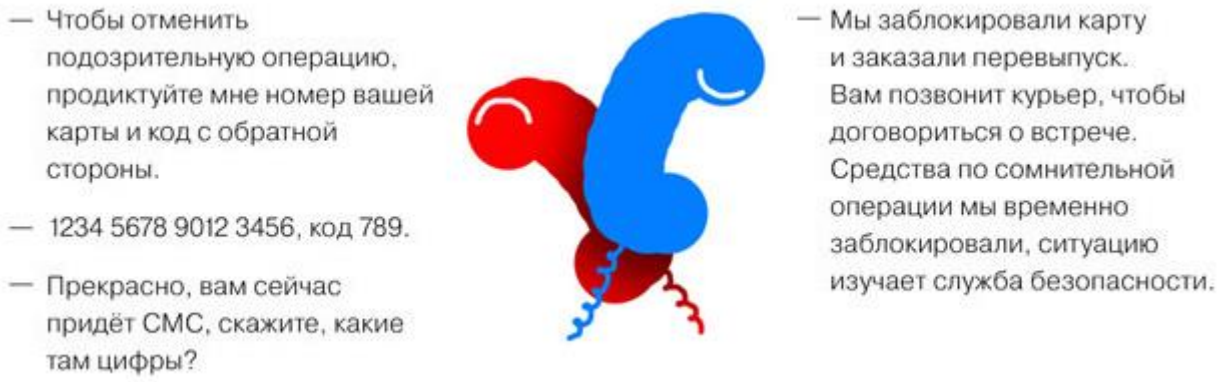


Слева — мошенник, справа — банк.

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.

ЕСЛИ СОБЕСЕДНИК СПРАШИВАЕТ ДАННЫЕ КАРТЫ ИЛИ СМС-КОД.

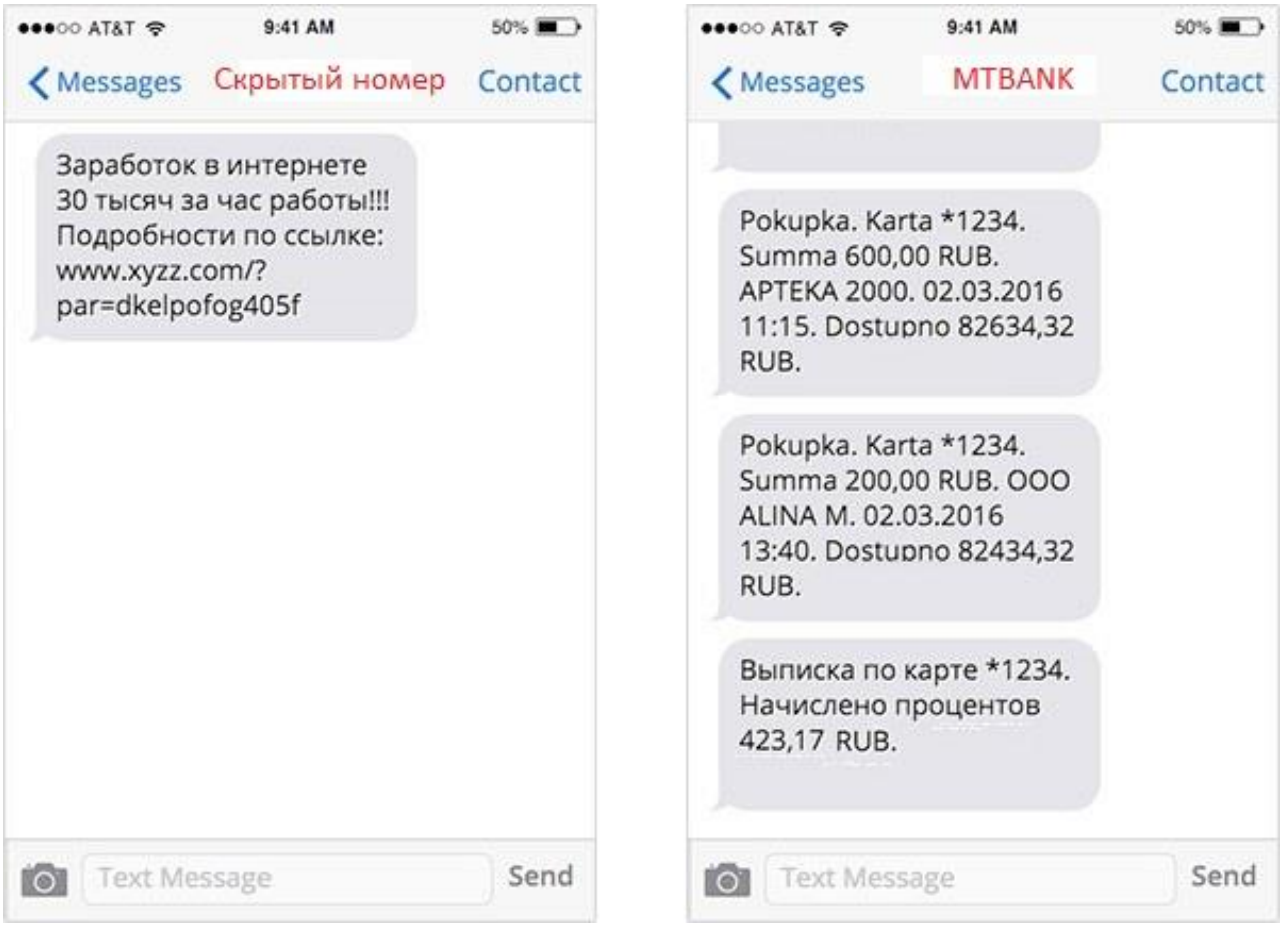


Слева — мошенник, справа — банк.

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.

ЕСЛИ ВАМ ОБЕЩАЮТ ВЫГОДУ БЕЗ УСИЛИЙ.



Слева — мошенник, справа — банк.

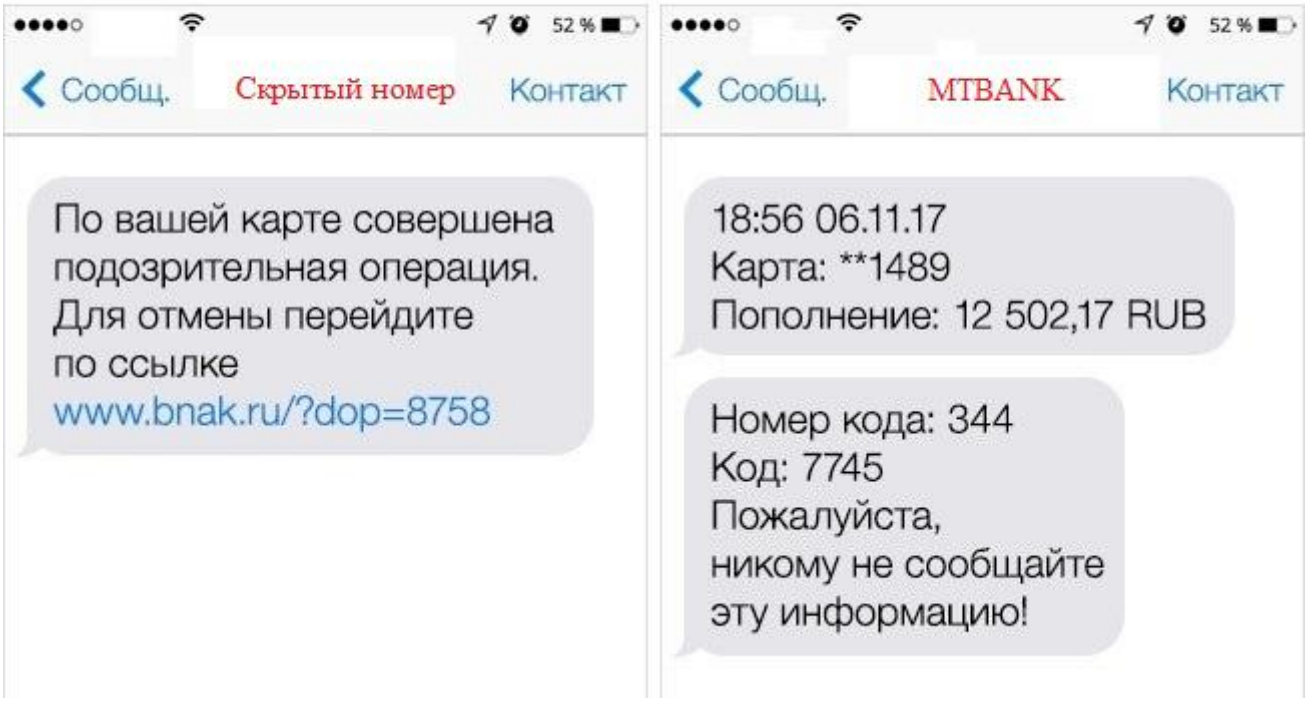
Чтобы завлечь жертву, мошенники обещают солидный доход быстро и без усилий: суперприбыльную работу, беспроигрышные конкурсы, курсы, которые сделают всех богатыми. Но мошенники могут взять предоплату за обучение и пропадут. Или посулят приз и выманят у вас данные карты якобы для перевода выигрыша.

ЕСЛИ СОБЕСЕДНИК ТОРОПИТ ВАС ИЛИ ПЫТАЕТСЯ ПЕРЕУБЕДИТЬ.

Слева — мошенник, справа — банк.

Сотрудник банка никогда не будет настаивать или торопить клиента.

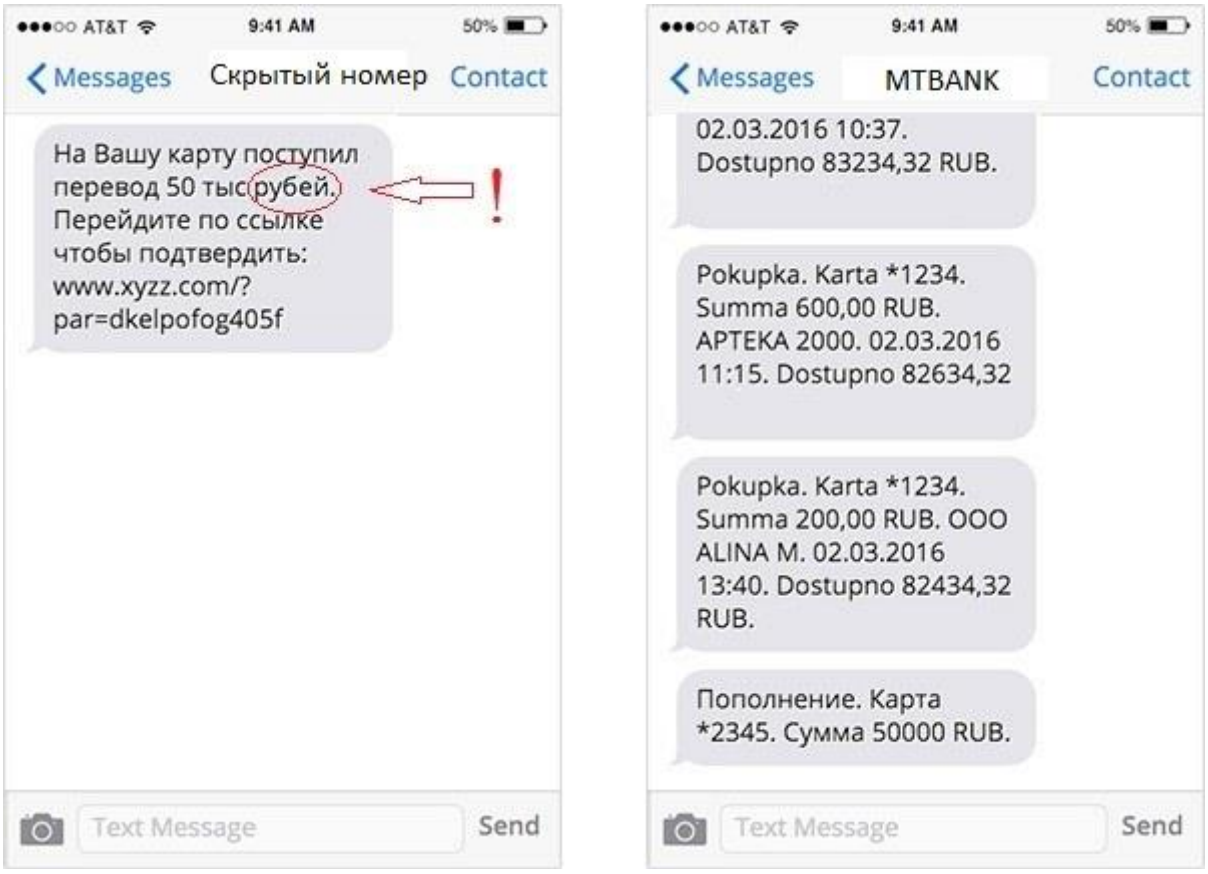
ЕСЛИ ВАМ ПОСЛЕ ОБЩЕНИЯ С ЛЖЕБАНКИРАМИ СТАЛИ ПОСТУПАТЬ СМС ЯКОБЫ ОТ БАНКА С ПРЕДЛОЖЕНИЕМ ПЕРЕЙТИ ПО ССЫЛКЕ ДЛЯ ОТМЕНЫ ОПЕРАЦИИ.



Слева — мошенник, справа — банк.

Не переходите по ссылкам в сообщении. Данные действия могут привести к тому, что гражданин попадет на «фишинговый» сайт, где необходимо будет ввести реквизиты своей банковской платежной карты, и после ввода данных реквизитов произойдет списание денежных средств с расчетного счета.

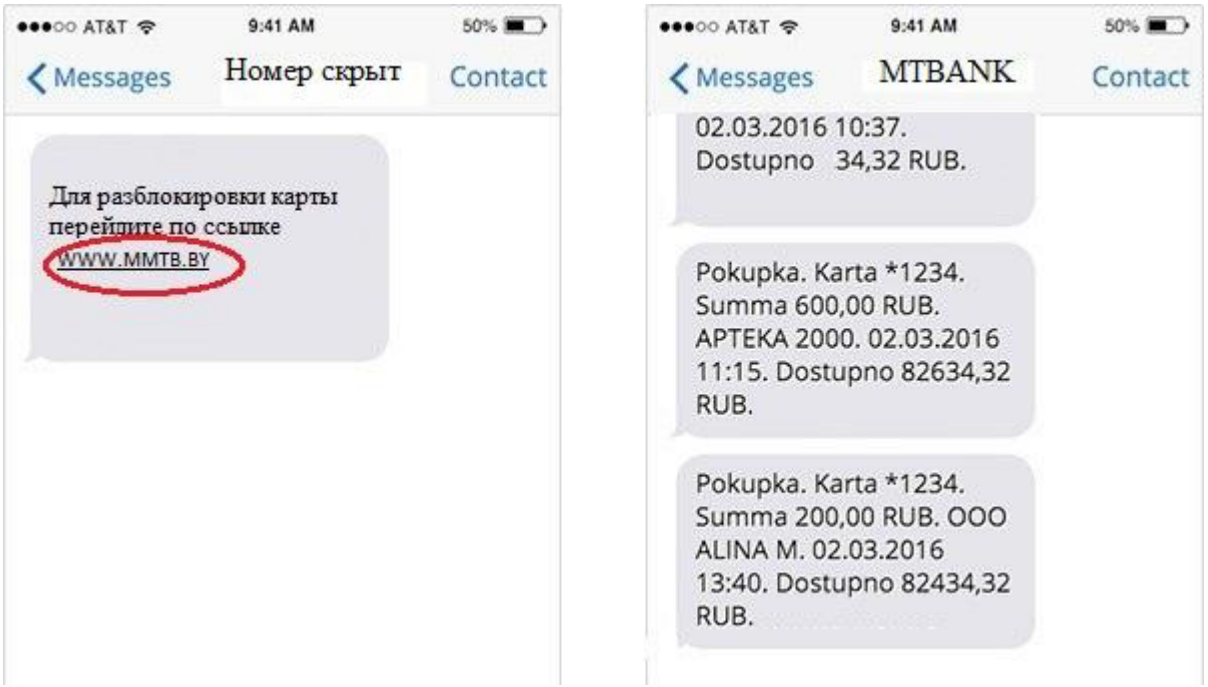
ОШИБКИ В СООБЩЕНИИ.



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.