«Профилактика преступлений и правонарушений в сфере высоких технологий»

В настоящее время Беларусь находится на первом месте среди стран СНГ и Юго Восточной Европы по осуществлению безналичных платежей. Вследствие чего произошел рост операций, совершенных в сети Интернет. Банковские учреждения, для удобства внедряют множество услуг для повышения безопасности электронных платежей, однако необходимо соблюдать элементарные правила безопасности.

Реквизиты карты — это информация, которую Вы можете увидеть (прочитать) на самом «пластике»:номер из 16 цифр, имя и фамилия владельца, срок действия и трехзначный код безопасности на обратной стороне.
По правилам платёжных систем реквизиты категорически запрещено сообщать посторонним. Если банк узнает, что Ваши реквизиты попали в чужие руки, то сразу заблокирует карту. Но кое-что сообщать всё-таки можно.
Разберёмся на примере, какую информацию содержит Ваша пластиковая карта.

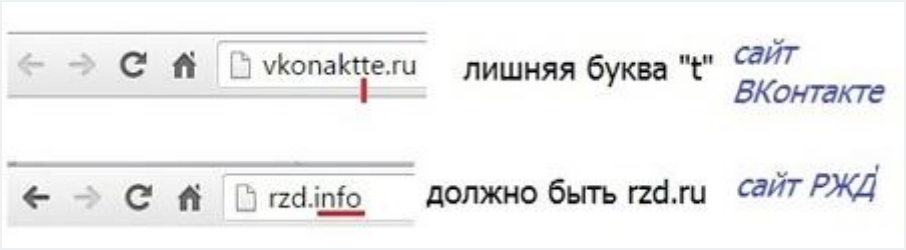
1. **Четырёхзначный номер** печатается прямо под 1-й группой цифр номера карты. Все цифры полностью совпадают с 1-й группой цифр эмбоссированного номера карты.
2. Здесь **имя и фамилия** указываются в латинской транскрипции.

3. **Срок действия карты**находится ниже номера. Карта действует до последнего дня месяца, указанного на лицевой стороне.
4. **Логотип и голограмма**платёжной системы говорят о том, какая система предоставляет услуги по проведению платёжных операций по этой карте.
5. **Номер карты** – это индивидуальный набор цифр именно вашей карты, номер доступа к банковскому счету.
6. **Чип** – это миникомпьютер, который помнит всю информацию по карте. Карты с чипом более безопасны, чем те, у которых есть только магнитная полоса.
7. **Технология PayPass/PayWave**. Это система бесконтактных платежей.
8. Здесь красуется **логотип** банка-эмитента.
9. **Магнитная полоса** – полоса, содержащая необходимые данные для проведения расчётов с использованием платёжной карточки.
10. **CVV2 (CVC2)** – трехзначный код на оборотной стороне карточки.
11. **Полоса для подписи** – место, где держатель ставит свою подпись.

Фишинг- один из видов интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам, паролям, данным лицевых счетов и банковских карт. В основном, используется метод проведения массовых рассылок от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих.

«Похожий» URL

Обратите внимание на адресную строку браузера. Адрес фальшивого сайта может отличаться всего одним символом.

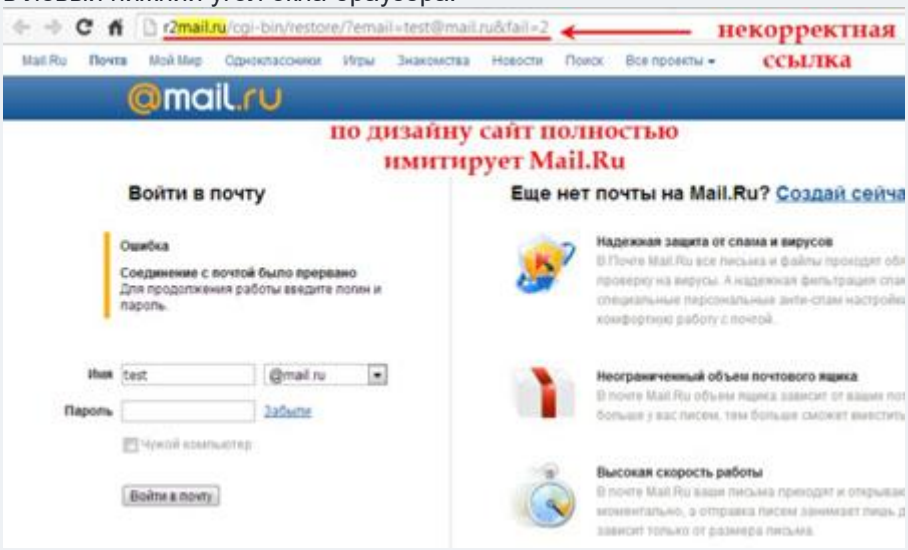


Безопасное соединение

Прежде чем вводить логин и пароль от учетной записи или платежные данные убедитесь, что соединение защищено. Адресная строка страницы интернет-сайта начинается не с аббревиатуры https, а с более короткой http. Это соединение менее безопасное, чем https. Кстати, буква “S” в названии https, как раз и означает “Secure” — защита.

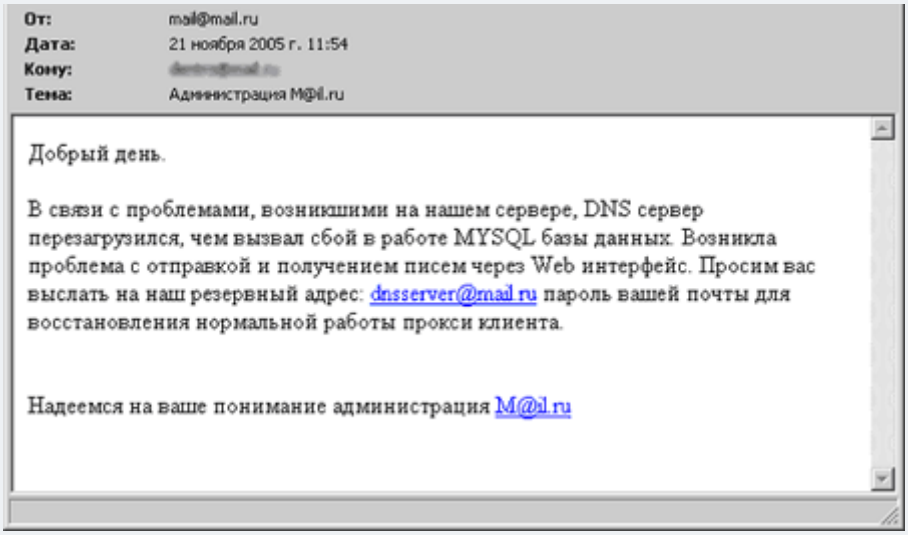
Фальшивые ссылки

Получив подозрительное письмо, не торопитесь переходить по ссылкам. Сначала разберитесь, куда они ведут на самом деле. На ПК или ноутбуке достаточно навести курсор мыши и посмотреть в левый нижний угол окна браузера.



Обезличенные обращения

Мошенники делают рассылки по огромному количеству адресов и не знают, как вас зовут. Поэтому их письма начинаются со слов «Уважаемый пользователь» или «Здравствуйте», «Добрый день».



Защититесь от фишинга

- **Следуйте принципам безопасного поведения в интернете и не переходите по ссылкам, присланным в подозрительных или непонятных сообщениях электронной почты.**
- **Не загружайте вложенные файлы из сообщений электронной почты, которых вы не ожидали.**
- **Обеспечьте надежной защитой свои пароли и не сообщайте их никому.**
- **Не сообщайте никому свои персональные данные - будь то по телефону, лично или в сообщении эл. почты.**
- **Внимательно проанализируйте адрес сайта (URL), на который вы были переадресованы. В большинстве случаев фишинга, несмотря на то, что сайт выглядит идентично настоящему, URL-адрес может отличаться от оригинального (например, заканчиваться на .com вместо .gov).**
- **Поддерживайте свой браузер обновленным и своевременно устанавливайте обновления безопасности.**

Социальная Инженерия (СИ)– это совокупность способов психологического воздействия на поведение человека с целью получения выгоды - личной информации, денежных средств и т.д

Существует множество разнообразных техник социальной инженерии, но их объединяет одно: в основе лежат *когнитивные искажения*, то есть человеческая глупость и невнимательность.
Самыми распространёнными способами использования мошенниками социальной инженерии являются:

- Фишинг
- Претекстинг
- Троянские вирусы
- Мошенничество с использованием брендов известных корпораций
- Мошенничество в соц. сетях и т.д

Фишинг – это вид интернет-мошенничества, целью которого является получение доступа к персональным данным пользователей. Это самая популярная схема социальной инженерии на сегодняшний день.
Ни одна крупная утечка персональных данных не обходится без волны фишинговых рассылок, предшествующих ей. Наиболее ярким примером такой атаки может служить сообщение, отправленное жертве по электронной почте и подделанное под официальное письмо - от банка или платёжной системы - требующее проверки определённой информации или совершения определённых действий.
Такие письма обычно содержат ссылку на фальшивую веб-страницу, в точности похожую на официальную и содержащую форму, требующую ввести конфиденциальную информацию.

Претекстинг – это действие, отработанное по заранее составленному сценарию (претексту). В результате цель (жертва) должна выдать определённую информацию, или совершить определённое действие. Этот вид атак применяется обычно по телефону.
Чаще эта техника включает в себя больше, чем просто ложь, и требует каких-либо предварительных исследований, как: день рождения, ИНН, номер паспорта либо последние цифры счета, для того, чтобы не вызвать подозрений у жертвы. Обычно реализуется через телефон или электронную почту.

Троянские вирусы - это техника эксплуатирует любопытство, либо алчность цели. Злоумышленник отправляет e-mail, содержащий во вложении важное обновление антивируса, или даже свежий компромат на сотрудника. Такая техника остаётся эффективной, пока пользователи будут слепо кликать по любым вложениям.

Мошенничество с использованием брендов известных корпораций - в таких фишинговых схемах используются поддельные сообщения электронной почты или веб-сайты, содержащие названия крупных или известных компаний.
В сообщениях может быть поздравление с победой в каком-либо конкурсе, проводимом компанией, о том, что срочно требуется изменить учётные данные или привязать карту к учётной записи для участия.
Подобные мошеннические схемы от лица службы технической поддержки также могут производиться по телефону.

Как распознать приемы социальной инженерии

Необходимо остерегаться любых не известных предложений помощи, в особенности предлагающих переход по сторонним ссылкам. Как правило, в подобных случаях речь идет об уловках социальной инженерии. Данное правило тем более актуально, если от пользователя требуется указать учетные или банковские данные. В таком случае без всяких сомнений речь идет о мошенничестве, так как уважающие себя финансовые организации ни при каких обстоятельствах не будут запрашивать учетные данные посредством сообщения эл. почты. Кроме того, настоятельно рекомендуем проверить адрес отправителя, кажущегося вам подозрительным сообщения эл. почты и убедиться в его легитимности.

Как защитить свои данные?

Для проведения своих атак злоумышленники, применяющие техники социальной инженерии, зачастую эксплуатируют доверчивость, лень, любезность и даже энтузиазм пользователей. Защититься от таких атак непросто, поскольку их жертвы могут не подозревать, что их обманули. Злоумышленники, использующие методы социальной инженерии, преследуют, в общем, такие же цели, что и любые другие злоумышленники: им нужны деньги или личные данные.

Ниже перечислены методы действий социальных инженеров:

- представление сотрудником банка, партнерской компании, представителем закона
- предложение помощи в случае возникновения проблемы и последующее провоцирование возникновение проблемы, которое принуждает жертву попросить о помощи
- использование внутреннего сленга и терминологии для возникновения доверия

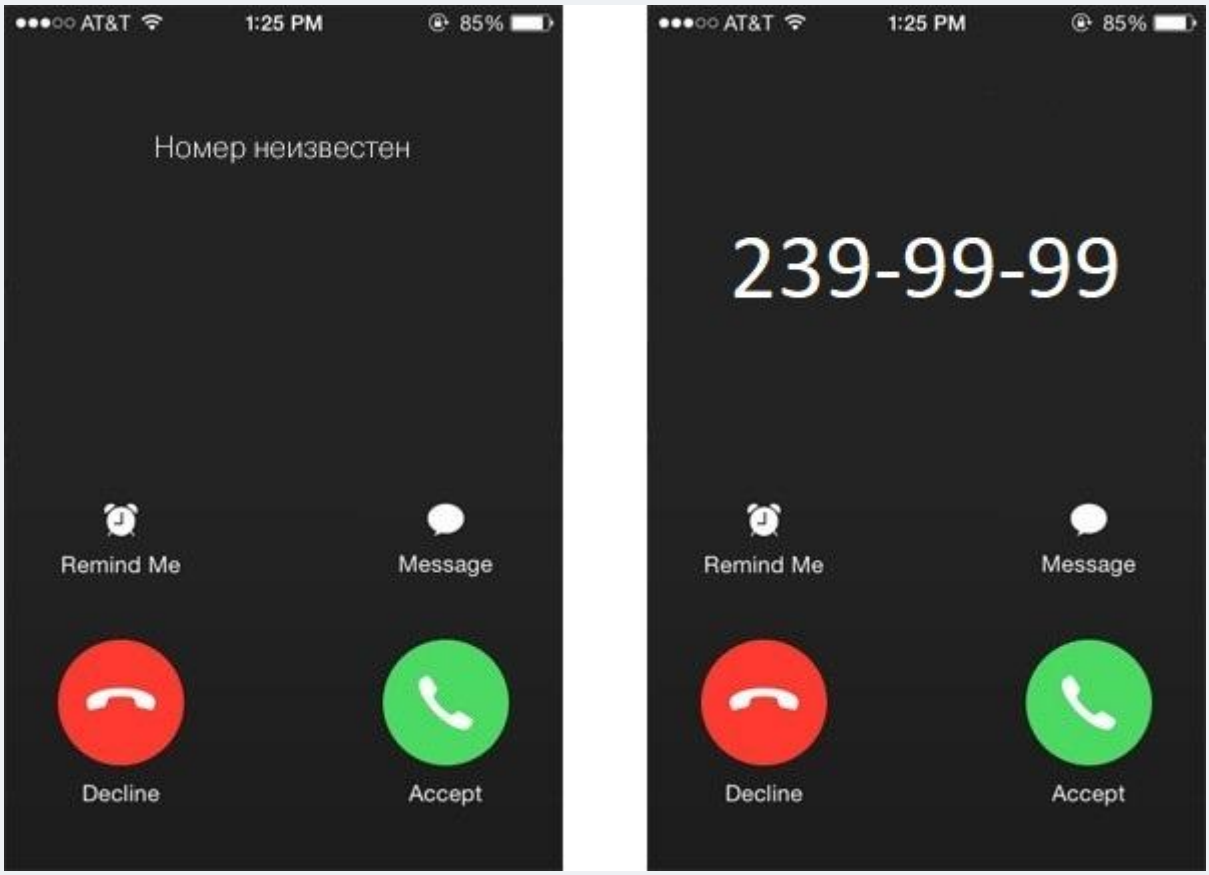
- отправка вирус или троянского коня в качестве приложения к письму
- использование фальшивого pop-up окна, с просьбой аутентифицироваться еще раз, или ввести пароль
- предложение приза за регистрацию на сайте с именем пользователя и паролем
- подбрасывание диска или флешки с вредоносным ПО на стол жертвы и т.д

Исходя из вышесказанного, можно выделить несколько полезных правил, которые помогут не стать жертвой социальной инженерии:

1. При разговоре по телефону с незнакомым человеком следует быть внимательным и принимать какие-либо решения обдуманно, поскольку чаще всего социальный инженер будет ставить вас в ситуацию, где надо быстро принять решение. Излишняя спешка может привести к потере ценной информации или личным данным
2. Проверяйте ваш компьютер на вирусы
3. Не вводите свои платёжные данные на сомнительных сайтах
4. Не стоит переходить по странным ссылкам, пришедшим вам на почту от неизвестных источников. Пример: “Хотите новый IPhonXвсего за 1 доллар?”
   Не сообщайте ваши личные данные в социальных сетях или по телефону.

«Вишинг» — это телефонное мошенничество, при котором преступник связывается с жертвой по телефону (в виде звонка или СМС) и уговаривает предоставить данные банковской карты под определённым убедительным предлогом. Например, представляясь сотрудником банка или какого-то государственного органа.

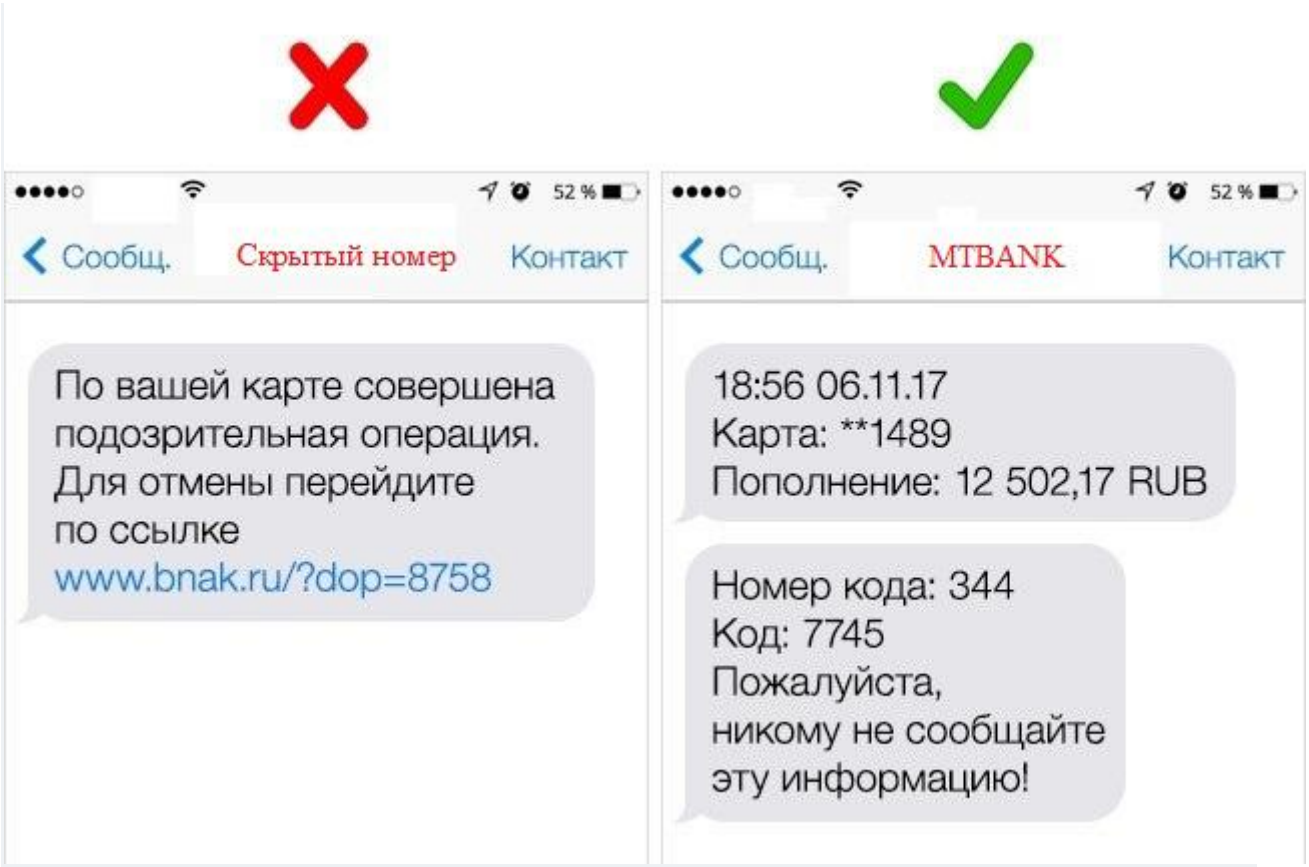
1. Звонок поступает с незнакомого номера или с мобильного.



Слева — мошенник, справа — банк.

Из банка всегда звонят с официальных номеров, указанных на сайте. Необязательно помнить номер, но он должен быть хотя бы местным.

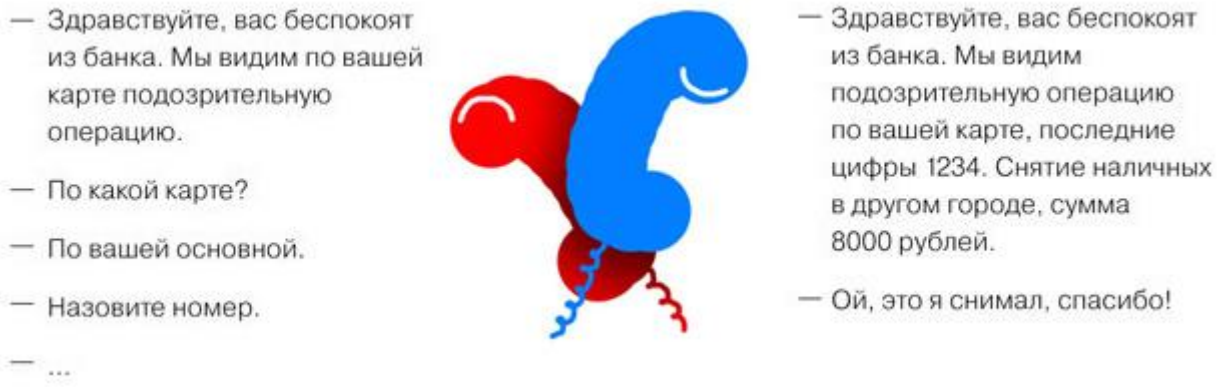
2. Смс якобы от банка приходит в новую переписку.



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.

3. 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.

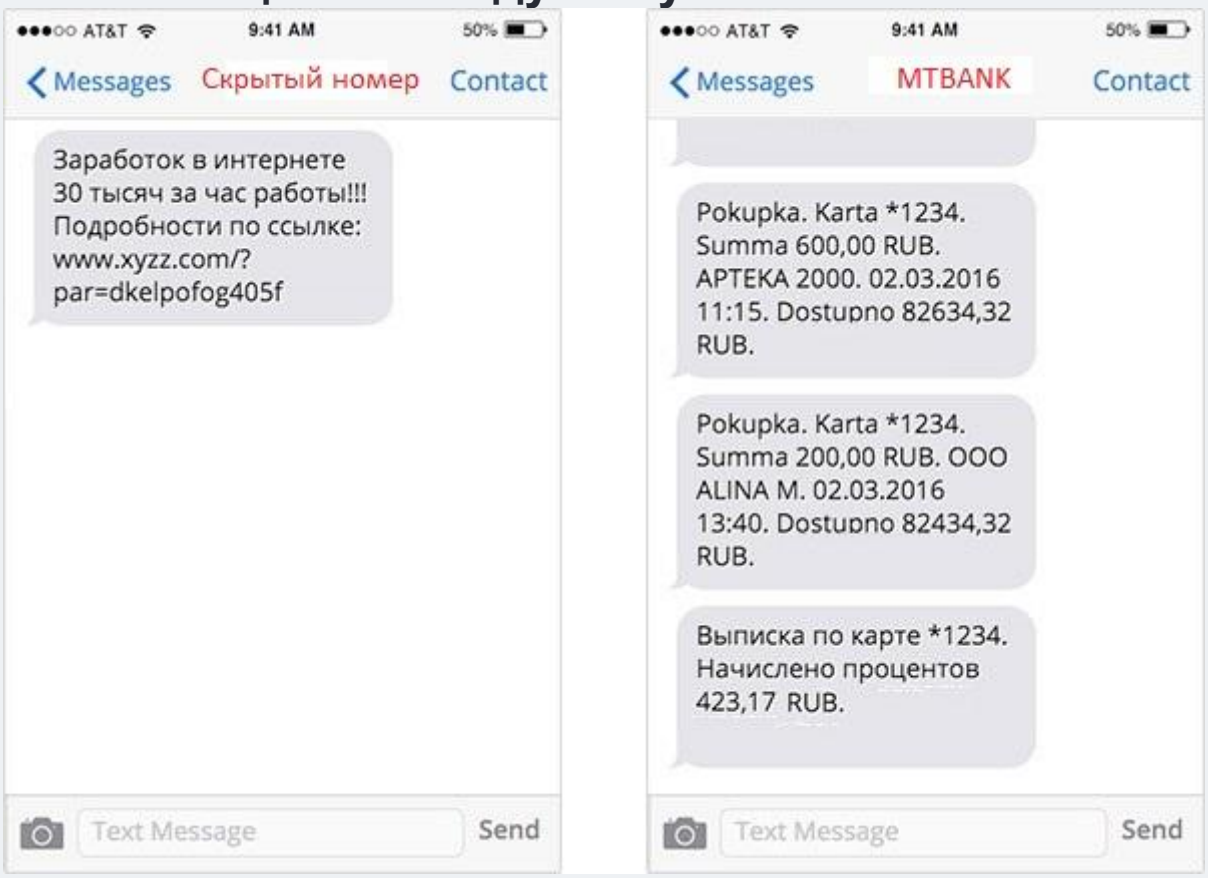
4. Собеседник спрашивает данные карты или смс-код.

Слева — мошенник, справа — банк.

Смс-код — один из главных паролей. Сотрудники банка никогда его не спросят, так же как и CVVна 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.

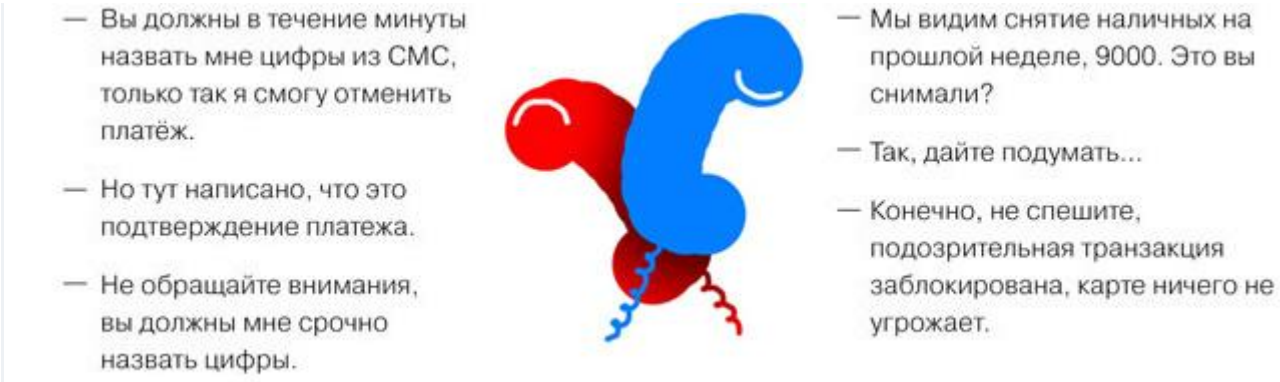
5. Вам обещают выгоду без усилий.



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.

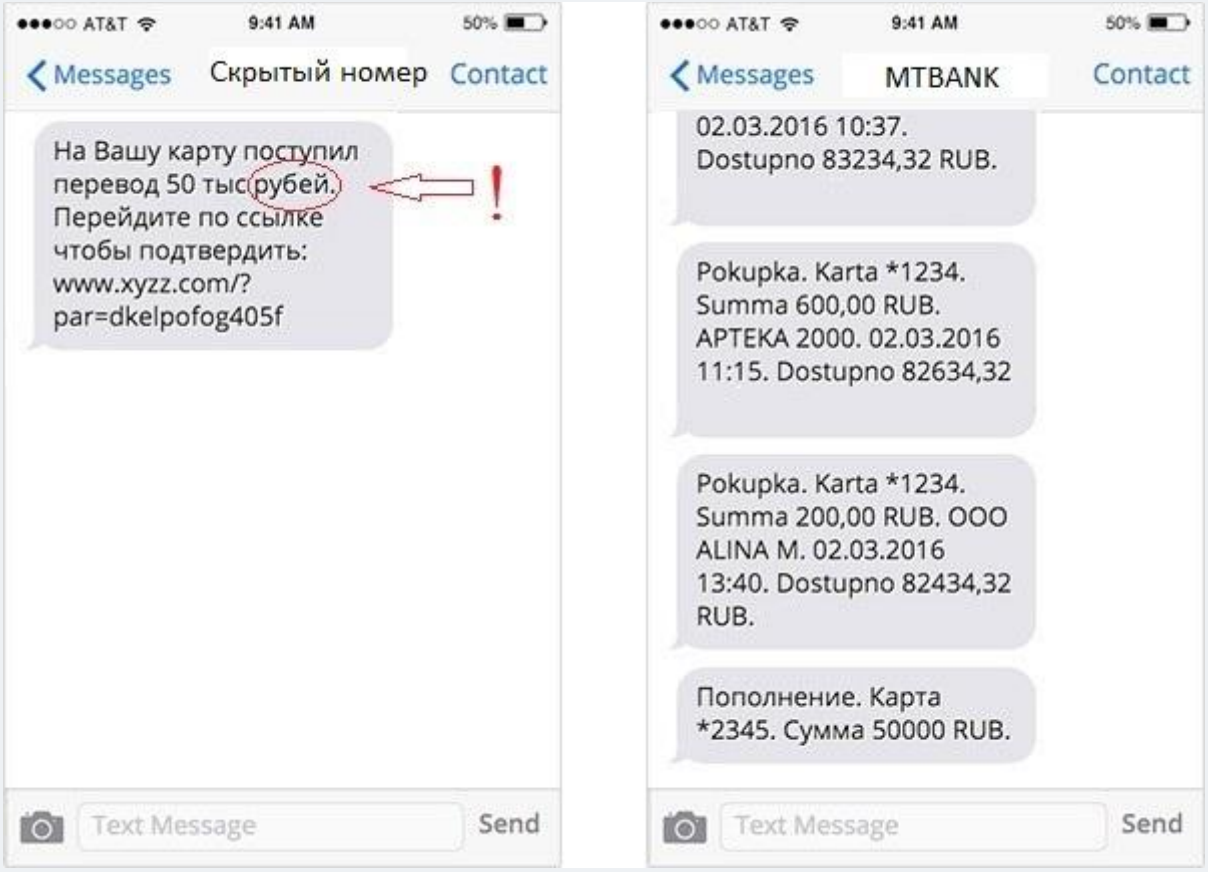
6. Собеседник торопит вас или пытается переубедить.



Слева — мошенник, справа — банк.

Сотрудник банка никогда не будет настаивать или торопить клиента.

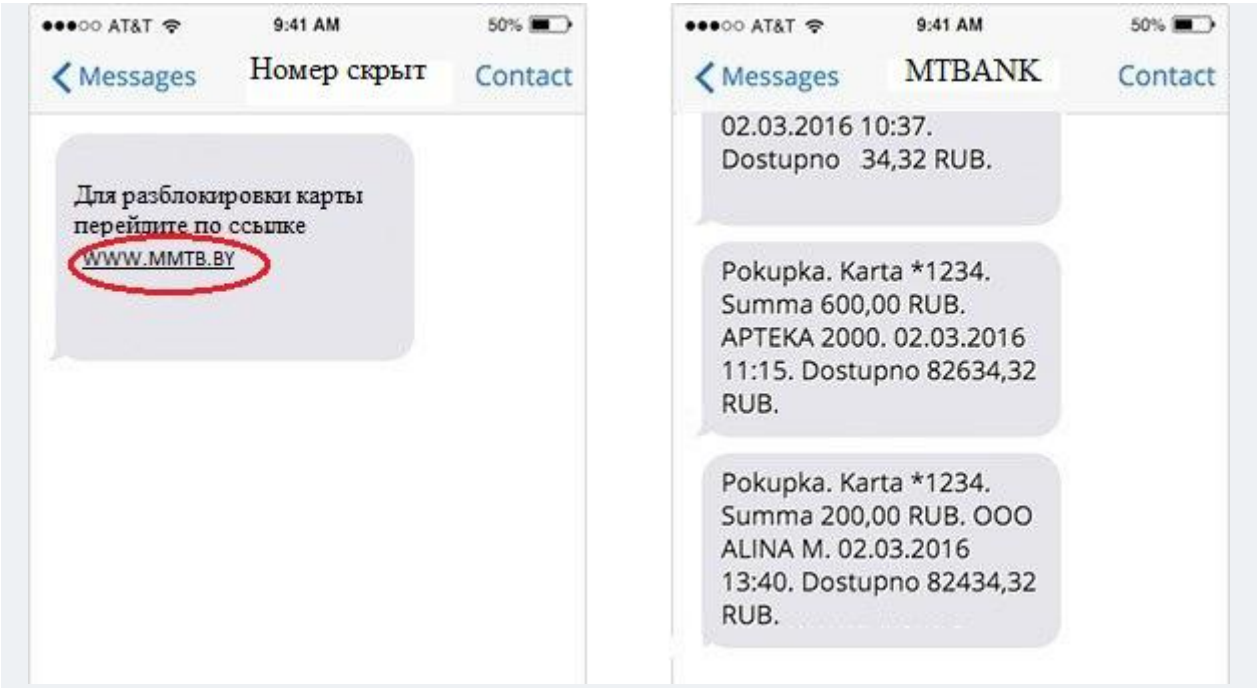
7. Ошибки в сообщении



Слева — мошенник, справа — банк.

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

8. 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.

Вывод:

1. 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.
2. Если не уверены в собеседнике, попросите его назвать номер карты или остаток на счёте.
3. Не паникуйте, если вам сообщают о блокировке счета. Позвоните в банк по номеру, указанному на сайте или на карте.
4. Не обращайте внимание на обещания лёгких денег или выгоды без усилий.
5. Если собеседник торопит вас или спрашивает смс-код, то вы говорите с мошенником!
6. Внимательно читайте сообщения из банка. Мошенники используют имена отправителей, похожие на названия банков, и допускают ошибки в тексте.

Начальник Октябрьского РОВД г. Могилева
Сильванович А.С.