*Приложение № 2*

*к Регламенту взаимодействия сотрудников Банка*

*при обработке отдельных видов платежей.*

**Памятка для Клиентов**

**Рекомендации по снижению рисков перевода денежных средств без добровольного согласия клиента**

ООО КБ «ГТ банк» прилагает все усилия для того, чтобы обеспечить безопасное использование клиентами систем дистанционного банковского обслуживания, банковских карт и обеспечить сохранность персональных данных и денежных средств клиентов. Тем не менее полная безопасность невозможна без соблюдения клиентом следующих правил безопасности и увеличения защиты персональных данных и финансовых средств:

**ЗАЩИТА ОТ МОШЕННИЧЕСТВА С ПОМОЩЬЮ НЕДОСТОВЕРНОЙ РЕКЛАМЫ (СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ)**

В сети Интернет на ряде ресурсов действуют мошенники, которые обещают помочь с выдачей кредитов (открытием кредитных лимитов) или гарантий. При вступлении в переписку по электронной почте мошенники пытаются выманить у потенциальных жертв персональные данные, включая паспортные данные и номер телефона. Впоследствии жертве приходит SMS якобы от Банка, в котором сообщается, что кредит/кредитный лимит или гарантия одобрена, и для его/ее активации/получения необходимо либо перечислить определенную сумму на некий телефонный номер (который является номером мошенника) либо выслать комплект документов, содержащих персональные данные. В случае перечисления денег или пересылки документов мошенники пропадают.

ПОМНИТЕ, ООО КБ «ГТ банк» не принимает решений о выдаче кредитов (открытии кредитных лимитов) и гарантий заочно, не действует через посредников и просит не поддаваться на действия подобных мошенников.

**ЗАЩИТА ОТ МОШЕННИЧЕСТВА С ПОМОЩЬЮ СМС**

СМС используется мошенниками для сбора информации и убеждения клиента осуществить финансовые операции в пользу третьих лиц под различными предлогами. Данные сообщения часто похожи на настоящие официальные сообщения от Банка и могут содержать в тексте название ООО КБ «ГТ банк».

Следующие признаки свидетельствуют о том, что пришедшее сообщение прислано мошенниками:

* содержит информацию, что на банковский счёт поступили деньги, которые не ожидаются;
* содержит информацию о том, что Банком одобрен кредит/кредитный лимит и для его активации необходимо перечислить деньги на определенный номер;
* запрашиваемые в нем действия требуют срочного ответа. Например, «Ваш счет будет закрыт или временно заблокирован»;
* содержит форму для ввода персональных данных;
* требует предоставить, обновить или подтвердить персональные данные (кодовое слово, ПИН-код и т.д.);
* содержит текст типа "Ваша банковская карта заблокирована" и номер телефона, на который нужно перезвонить. После того, как абонент звонит по номеру, мошенники сообщают, что на банковском сервере произошел сбой и просят сообщить реквизиты банковской карты для устранения неполадок;
* просит перезвонить или отправить СМС-сообщение на короткий номер, который обещает разблокировку/продление действия банковской карты;
* рассылка осуществлялась не с официального номера ООО КБ «ГТ банк».

ПОМНИТЕ, ООО КБ «ГТ банк» никогда не отправляет электронные письма или СМС-сообщения с предложением сообщить номер банковской карты или перезвонить по какому-либо номеру. Для рассылок СМС-сообщений ООО КБ «ГТ банк» использует только префикс GTBANK.

Если от имени ООО КБ «ГТ банк» поступило подозрительное СМС-сообщение следует связаться с Банком по телефону +7 (861) 279-03-05 для уточнения подлинности полученного сообщения.

**ЗАЩИТА ОТ МОШЕННИЧЕСТВА ПО ТЕЛЕФОНУ**

Телефонные звонки, наряду с сообщениями электронной почты и СМС, часто используются мошенниками для неправомерного получения персональной информации и убеждения клиента осуществить финансовые операции в пользу третьих лиц под различными предлогами. Такие телефонные звонки очень часто похожи на «настоящие» звонки.

Мошенники могут предлагать:

* перевести деньги на «безопасный» (резервный, временный, дополнительный) счет, чтобы якобы застраховать накопления от любых ситуаций в экономике, и с этой целью сообщить им номер банковской карты и/или код CVV либо перевести деньги на личную карту или ввести данные карты на каком-либо сайте;
* защитить личные сбережения от отключения SWIFT;
* вложить деньги и спасти их от кризиса, девальвации или катастрофы или получить высокую доходность;
* оформить кредиты по сниженной ставке;
* обеспечить «выгодный» (ниже курса биржи или по курсу ЦБ) курс конвертации;
* совершить какую-нибудь операцию в ближайшем банкомате;
* участие в специальных государственных программах.

ЗАПОМНИТЕ, сотрудники Банка никогда не будут предлагать действовать по таким схемам.

Не доверяйте звонящему от имени сотрудника банка, Банка России, полиции, прокуратуры, ФСБ и других ведомств. Мошенники могут представляться разными организациями и использовать скрытые или подменные телефонные номера — это значит, что на экране отобразится телефонный номер банка, а звонит на самом деле мошенник.

Не сообщайте никакие данные, даже если угрожают уголовным делом или другими последствиями. Даже если Вас называют по имени-отчеству и знают другую личную информацию, Вы можете повесить трубку без предупреждения, не прощаясь, и сразу перезвонить в банк самостоятельно.

Во время разговора возьмите паузу. Вас будут торопить и говорить, что деньги могут украсть или заблокировать на счете в любой момент. Противостоять этому напору трудно: звонок от банка или госструктуры — стрессовая ситуация. Но перед тем как продолжить разговор с мошенником, сделайте паузу, чтобы успокоиться, разобраться в ситуации и выйти из-под влияния мошенников, а лучше всего повесьте трубку. Не бывает ситуаций, в которых Вам нужно быстро провести операцию, даже если это действительно звонок из банка.

Не сообщайте никому информацию о Вашем счете и остатке денежных средств. Если сотрудник банка звонит Вам сам, он никогда не станет спрашивать у Вас личные и/или банковские данные (например, сообщить ПИН-код или секретный код CVV2 банковской карты, кодовое слово, номер счета, номер договора, номер банковской карты, паспортные данные, логин и пароль, одноразовые пароли в системах дистанционного банковского обслуживания, одноразовые пароли для осуществления операций в Интернете). Данная информация сотруднику Банка не требуется.

Если от имени ООО КБ «ГТ банк» поступил подозрительный телефонный звонок следует уточнить цель звонка и отдел, после чего обязательно самостоятельно связаться с Банком по телефону +7 (861) 279-03-05 для уточнения подлинности поступившего звонка. Связаться с сотрудником Банка также можно по телефонам, указанным на официальном сайте Банка.

**ЗАЩИТА ОТ МОШЕННИЧЕСТВА С ПОМОЩЬЮ ЭЛЕКТРОННОЙ ПОЧТЫ**

Фишинг (phishing) – это искаженное слово fishing (ловить рыбу). Этим термином называют наиболее распространенную форму мошенничества в сети Интернет. Мошенники используют сообщение электронной почты, отправленное огромному количеству пользователей Интернет, и надеются, что кто-нибудь «попадется» в расставленные сети размером с Интернет и отправит им свои данные. Сообщения электронной почты, которые используются в качестве приманки, часто похожи на настоящие официальные сообщения. Однако их целью является заманить клиента на фальшивые веб-сайты, замаскированные под сайты известных организаций, например, банков, чтобы получить персональные данные (номер банковской карты, пароль, ПИН-код) и использовать данную информацию для кражи средств с банковского счета.

ЗАПОМНИТЕ, не отправляйте никакую персональную и/или конфиденциальную информацию по электронной почте.

Даже при простом переходе по ссылке на фальшивый сайт и не согласии передать мошенникам персональные данные компьютер может быть заражен вирусом, который будет сканировать нажатие клавиш клавиатуры и передавать злоумышленникам данные, вводимые на подлинном сайте.

Наиболее характерные признаки того, что письмо прислано мошенниками:

* запрашиваемые в них действия требуют срочного ответа. Например, «Ваш счет будет закрыт или временно заблокирован»;
* сообщения содержат ссылки на страницы Интернет, которые похожи на настоящие (они могут содержать название ООО КБ «ГТ банк» или написаны похожим образом), однако ведут на фальшивый сайт или открывают всплывающее окно, которое запрашивает или требует подтвердить персональные данные;
* содержит предложение принять участие в розыгрыше призов, при этом организатор просит заполнить анкету, в которой помимо Ф.И.О. и контактных данных просят указать паспортные данные, а также номер (кредитной, дебетовой) карты, срок ее действия, секретный код CVV2 и название банка-эмитента.

Такие сообщения могут содержать явные опечатки или орфографические ошибки, что позволяет им обходить «spam»-фильтры, установленные у Интернет провайдеров.

ПОМНИТЕ, ООО КБ «ГТ банк» никогда:

* не отправляет сообщения с просьбой подтвердить, обновить или предоставить персональные данные, такие как номер банковской карты и срок ее действия, ПИН-код, имя пользователя и пароль, кодовое слово;
* не отправляет сообщения с формой для ввода персональных данных;
* не просит зайти в систему дистанционного банковского обслуживания по ссылке в письме, так как это противоречит соображениям безопасности.

При возникновении сомнений в достоверности письма, пришедшего по электронной почте, ни при каких обстоятельствах не переходите по ссылкам, указанным в письме, не открывайте прикрепленные к письму файлы и обязательно свяжитесь с Банком по телефону +7 (861) 279-03-05.

**БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ БАНКОМАТОВ**

Для предотвращения незаконных списаний с банковской карты Банк рекомендует применять следующие меры безопасности:

* в случае если, при проведении операции с банковской картой в банкомате, банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует связаться ООО КБ «ГТ банк» по телефону +7 (861) 279-03-05 и следовать рекомендациям специалиста;
* не использовать незнакомые банкоматы, расположенные в затемненных, немноголюдных местах, поскольку они наиболее удобны для мошенников. Старайтесь снимать деньги в одних и тех же банкоматах внутри банковских отделений или хорошо просматриваемых помещениях и по возможности запомните их внешний вид. Как правило, любые усовершенствования никак не затрагивают внешний вид банкомата. Будучи за границей, снимать деньги следует в банкоматах крупных банков с мировым именем;
* перед использованием банкомата следует осмотреть его на наличие дополнительных ("неродных") устройств, не соответствующих его конструкции и расположенных в месте набора ПИН-кода (например, наличие неровно установленной клавиатуры набора ПИН-кода), в месте (прорезь), предназначенном для приема карт или козырьке банкомата. Если банкомат кажется подозрительным, неисправным или что-то иное вызывает подозрение, следует воздержаться от использования такого банкомата и совершения операции в нем, а также оповестить кредитную организацию по телефону, указанному на банкомате;
* при возникновении возле банкомата затруднительной ситуации и предложении помощи кого-либо из находящихся поблизости сердобольных свидетелей, следует быть внимательным, не передавать банковскую карту кому-то в руки и сообщать ПИН-код от нее. Это вполне могут быть мошенники, которые и подстроили такой «случайный сбой в работе». При возникновении затруднительной ситуации следует незамедлительно позвонить в кредитную организацию по телефону, указанному на банкомате;
* набирать ПИН-код быстро, заученными движениями и желательно несколькими пальцами, так злоумышленникам труднее разобрать, на какие именно кнопки нажимаются. При наборе ПИН-кода следует прикрывать клавиатуру свободной рукой, сумочкой или кошельком;
* периодически проверять балансы банковских счетов по выписке, в банкомате или в системе дистанционного банковского обслуживания.