

**РЕКОМЕНДАЦИИ КЛИЕНТАМ ООО «Примтеркомбанк»
по соблюдению мер информационной безопасности и защите информации в целях
противодействия незаконным финансовым операциям**

1. Общие положения

В соответствии с Методическими рекомендациями Банка России от 28 февраля 2024г. № 3-МР «Методические рекомендации по усилению кредитными организациями информационной работы с клиентами в целях противодействия осуществлению переводов денежных средств без добровольного согласия клиента, а также заключению договоров на получение кредитных (заемных) денежных средств под влиянием обмана или при злоупотреблении доверием и осуществлению операций с использованием указанных денежных средств, а также вовлечению граждан в деятельность по выводу и обналичиванию средств, полученных преступным путем» ООО «Примтеркомбанк» доводит до Вашего сведения основные рекомендации и информацию по соблюдению мер финансовой и информационной безопасности.

Рекомендации по соблюдению информационной безопасности (совокупности мер, применение которых направлено на непосредственное обеспечение защиты информации, процессов, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты не гарантируют обеспечение конфиденциальности, целостности и доступности информации, но позволяют в целом снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации.

Задачами Рекомендаций является доведение до Клиентов ООО «Примтеркомбанк» следующей информации:

- о потенциальных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- о мерах, направленных на предотвращение несанкционированного доступа к защищенной информации, включая случаи утери (потери, кражи) устройства клиентом, с которого выполнялись финансовые операции; о контроле конфигурации такого устройства и своевременном выявлении воздействия вредоносного кода.

Для удобства клиентов информация о вышеуказанных рисках и мерах защиты регулярно обновляется и размещается на сайте ООО «Примтеркомбанк» (<https://www.ptkb.ru/>) в разделах "Новости" и "Документы". Рекомендуем периодически проверять эти разделы для получения актуальной информации и рекомендаций.

2. Рекомендации по защите информации от воздействия вредоносного кода.

2.1. Не открывайте письма и вложения от незнакомых отправителей, а также не переходите по ссылкам, содержащимся в таких сообщениях, при работе с электронной почтой.

2.2. Используйте персональные компьютеры и мобильные устройства с установленным лицензированным программным обеспечением.

2.3. Регулярно обновляйте установленное программное обеспечение и операционную систему, включая установку критически важных обновлений.

2.4. Не используйте права администратора (или Root-права), если это не обязательно. В повседневной жизни входите в систему с обычной учетной записью без административных прав.

2.5. Активируйте системный аудит событий, который будет фиксировать возникающие ошибки, вход пользователей и запуск программ. Периодически проверяйте журнал и реагируйте на выявленные ошибки.

2.6. На устройстве, предназначенном для доступа к системе дистанционного обслуживания ООО «Примтеркомбанк», не следует использовать средства удаленного администрирования.

2.7. Обязательно установите и регулярно обновляйте антивирусное программное обеспечение на своем компьютере и мобильном устройстве. Рекомендуется установить максимальный уровень политики безопасности по умолчанию, что позволит избежать необходимости реагирования пользователя при обнаружении вирусов. Лечение (удаление) зараженных файлов будет производиться антивирусом в автоматическом режиме.

2.8. Полная проверка жесткого диска персонального компьютера и мобильного устройства на наличие вирусов и вредоносного программного обеспечения должна проводиться в автоматическом режиме не реже одного раза в неделю. Проверка осуществляется в соответствии с расписанием, заданным в настройках антивирусной программы.

2.9. Антивирусное программное обеспечение должно запускаться автоматически при загрузке операционной системы.

2.10. Рекомендуется проводить антивирусную проверку всей информации, которая передается или принимается через телекоммуникационные каналы, а также на съемных носителях (магнитных дисках, CD/DVD, USB-накопителях и т. д.). Если есть техническая возможность, сканирование следует выполнять в автоматическом режиме.

2.11. При подключении к Интернету используйте файрволы, разрешая доступ только к надежным ресурсам сети.

2.12. Не соглашайтесь на установку сомнительных программ, приложений и расширений во время работы в Интернете. Устанавливайте приложения исключительно из проверенных источников.

2.13. Обеспечьте защиту от установки несанкционированных «шпионских» программ посторонними лицами (гостями, посетителями) на ваш компьютер или мобильное устройство.

2.14. Рекомендуем ограничить обмен информацией в Интернете только безопасными порталами и проверенными электронными адресами. По возможности, не используйте компьютер, с которого вы проводите финансовые транзакции и обмен данными с ООО «Примтеркомбанк», для общения в социальных сетях или посещения развлекательных и сомнительных сайтов (игровых, сайтов знакомств, а также ресурсов, распространяющих ПО, музыку и фильмы), поскольку именно через такие ресурсы чаще всего распространяются вирусы.

2.15. В письмах от предположительно знакомых людей часто можно увидеть вредоносные ссылки, выданные за "интересные материалы". Также такие программы нередко маскируются под рекламные всплывающие окна на сайтах.

2.16. Если у вас возникли подозрения на наличие вирусов на компьютере или мобильном устройстве (например, замечены неожиданные зависания, перезагрузки или подозрительная сетевая активность), следует временно прекратить использование устройства до устранения проблемы.

2.17. После удаления вирусов и восстановления нормальной работы компьютера рекомендуется сменить пароли на новые.

2.18. Учтите, что ООО «Примтеркомбанк» не несет ответственности за возможные финансовые потери, понесенные Клиентом из-за ненадлежащего исполнения или нарушения требований к защите своих устройств (компьютера, мобильного устройства) от вредоносных программ.

3. Рекомендации по защите информации от несанкционированного доступа с использованием ложных ресурсов Интернета

Риски несанкционированного доступа к данным в основном связаны с «фишингом», который включает в себя использование поддельных интернет-ресурсов для кражи конфиденциальной информации, такой как личные данные, логины и пароли, а также воздействием вредоносного программного обеспечения.

Фишинг представляет собой попытку захвата личной информации пользователя. Один из наиболее распространенных методов фишинга включает отправку электронных писем от злоумышленников, которые выдают себя за представителей известных компаний. Обычно такие письма содержат ссылку на небезопасный веб-сайт, где пользователь может быть вынужден ввести свои личные данные, полагая, что это происходит в безопасной среде, в то время как на самом деле информация попадает в руки мошенников.

Мошеннический или поддельный веб-сайт — это небезопасный ресурс, который под разными предложениями требует от вас ввода конфиденциальной информации. Часто такие сайты выглядят почти идентично ресурсам, которым вы доверяете, и предназначены для мошеннического сбора секретной информации.

Если вы обнаружили поддельный сайт, который копирует дизайн официального сайта ООО «Примтеркомбанк», пожалуйста, немедленно сообщите об этом по контактным номерам Банка. Вход в личный кабинет системы дистанционного обслуживания ООО «Примтеркомбанк» необходимо осуществлять только с сайта <https://www.ptkb.ru/>. Обращайте внимание, что в адресной строке браузера присутствует именно этот адрес, остерегайтесь похожих названий. Не вводите данных для аутентификации на любых других сайтах.

Общие рекомендации:

3.1. Перед просмотром электронного письма всегда проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса настоящей компании. Изменить адрес электронной почты отправителя очень просто, поэтому будьте бдительны.

3.2. Внимательно читайте текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это - электронное письмо, отправленное мошенниками.

3.3. Старайтесь сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Вас действовать быстро и необдуманно. Многие поддельные сообщения электронной почты пытаются убедить Вас в том, что Вашему счету или ценным бумагам угрожает опасность, если Вы немедленно не обновите критически важные данные.

3.4. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности, не переходите по этой ссылке.

4. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

4.1. Рекомендуется регулярно обновлять пароли для доступа к своим учетным записям в системе дистанционного банковского обслуживания ООО «Примтеркомбанк» (далее ДБО) и других подобных системах. Пароль должен содержать не менее 8 символов и включать комбинацию строчных и заглавных букв, цифр и спецсимволов.

4.2. Рекомендуется использовать разные уникальные пароли для каждого веб-сайта и системы, на которых вы вводите личные данные (например, портал Госуслуг, интернет-банкинг, личный кабинет и т. д.).

4.3. В случае утечки или подозрения на компрометацию пароля, следует немедленно сменить пароль на новый, соответствующий указанным требованиям.

4.4. Ни в коем случае не передавайте и не раскрывайте свои пароли третьим лицам.

4.5. Рекомендуется устанавливать пароли на учетные записи пользователей операционной системы на вашем компьютере.

4.6. Рекомендуется установить антивирусное программное обеспечение на ваш телефон и своевременно обновлять его.

4.7. Рекомендуется активировать блокировку экрана на мобильных устройствах и отключить отображение паролей во время их ввода.

4.8. Рекомендуется исключить возможность физического доступа посторонних лиц к компьютерам или мобильным устройствам, которые вы используете для работы.

4.9. Рекомендуется применять специализированное программное и аппаратное обеспечение для защиты ваших компьютеров и мобильных устройств: средства защиты от несанкционированного доступа, персональные межсетевые экраны, антивирусные и антишпионские программы и т. д., а также обеспечивать регулярные автоматические обновления для этих средств.

4.10. Не стоит посещать веб-сайты с сомнительным содержанием и загружать или устанавливать нелицензионное программное обеспечение на свои компьютеры или мобильные устройства.

4.11. Использование нелицензионного программного обеспечения увеличивает риск несанкционированного доступа злоумышленников для кражи информации.

4.12. Не отправляйте файлы с конфиденциальной информацией по электронной почте, через SMS или социальные мессенджеры.

4.13. Не допускается работать на компьютерах или мобильных устройствах в Интернет-кафе или на других компьютерах общего пользования (вокзалы, аэропорты, библиотеки и т.п.). Работа с гостевых рабочих мест увеличивает риск неправомерного использования конфиденциальной информации и другой аутентификационной информации.

4.14. При утрате мобильного телефона, на который Вы получаете сообщения или используется для входа в ДБО следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты, а также необходимо обратиться в Банк для блокировки соответствующей учетной записи.

4.15. Будьте внимательны — не оставляйте свой телефон и компьютер без присмотра, чтобы избежать несанкционированного доступа.

4.16. При работе с ключами электронной подписи необходимо:

- использовать для хранения ключей электронной подписи внешние носители, настоятельно рекомендуется использовать специальные защищенные носители ключевой информации (ключевые носители), например: e-token, смарт-карта и т.п.;

- крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они (ключевые носители) не используются для работы;

- использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи/ключевым носителям, не хранить пароли в открытом виде на компьютере/мобильном устройстве.

5. Меры безопасности при общении по телефону

В последнее время мошенники активно используют телефонные звонки для сбора личной информации и убеждения клиентов в необходимости срочных действий, которые приводят к незаметному переводу денежных средств или активов в пользу третьих лиц под различными предложениями (например, разблокировка банковской карты или получение ценного приза). Цель таких мошенников – похитить деньги со счета клиента, применяя различные психологические приемы, такие как страх, жалость или обещания ценных выигрышей. Наиболее эффективный способ защититься от этого вида мошенничества – немедленно прекратить разговор.

Характерные признаки мошенничества по телефону:

- Собеседник требует от Вас принятия немедленного действия или срочного ответа. В качестве причин, как правило, приводятся следующие: техническое блокирование Вашего доступа к Личному кабинету.
- От Вас требуется назвать Ваши персональные данные (например, номер банковской карты полностью, ПИН-код карты, CVV/CVC, логин и пароль к Личному кабинету).

Помните, ООО «Примтеркомбанк» никогда и ни при каких обстоятельствах не запрашивает эту информацию у Клиентов.

- Собеседник путается или ведет себя нетерпеливо при уточнении с Вашей стороны его ФИО, контактного номера, цели звонка, подразделения (отдела, департамента и т.д.), в котором он работает, фамилии руководителя.
- При разговоре Вас просят произвести вход в ДБО (или, например, сменить ПИН-код в банкомате или пароль). В этом случае спросите у собеседника контактный номер телефона, по которому Вы сможете перезвонить позже, закончите разговор и свяжитесь с сотрудником Банка. Ваше обращение позволит предотвратить инциденты мошенничества в будущем.

6. Заключение

Чтобы избежать инцидентов, связанных с несанкционированным использованием вашей компьютерной техники при работе с информационными сервисами ООО «Примтеркомбанк», настоятельно рекомендуем строго следовать указанным выше правилам безопасности. Только полное соблюдение этих мер поможет вам защититься от мошенников и других злоумышленников, а также обеспечит безопасность ВАШИХ ДАННЫХ.