Общество с ограниченной ответственностью Микрокредитная компания «Гиллион» (ООО МКК «Гиллион»)

ИНН 2465177117, КПП 246501001, ОГРН 1182468006016
660131, Красноярский край, город Красноярск, Ястынская улица, дом 19а помещение 213, кабинет 1

РЕКОМЕНДАЦИИ
по противодействию совершения незаконных финансовых операций

1. ВВЕДЕНИЕ

Настоящий документ предназначен для ознакомления Клиентов ООО МКК «Гиллион» (далее по тексту - *«Общество»*) с рекомендациями по предотвращению доступа злоумышленников к информации, которая может позволить им совершить незаконные финансовые операции от имени Клиентов Общества.

В настоящее время активно осуществляется внедрение современных цифровых технологий в различные сферы жизни и производства. Финансовые организации предлагают своим Клиентам большой выбор инструментов для удаленного взаимодействия, позволяющий Клиентам экономить своё время и совершать финансовые операции без личного обращения в офис финансовой организации.

Необходимо отметить, что использование технологий удаленного взаимодействия, несет с собой определенные риски, главным из указанных рисков является незаконное совершение злоумышленниками финансовых операций от имени Клиентов финансовых организаций с целью хищения денежных средств Клиентов.

Цель злоумышленников является кража персональных данных. Для того чтобы осуществить противоправные действия, мошенники придумывают всё новые и новые схемы. В настоящее время самые распространённые схемы злоумышленников заключаются в следующем:

- **Телефонные мошенники:** Телефонные мошенники придумывают различные сценарии для кражи персональных данных и используют методы психологического давления, чтобы человек не успел принять обдуманное решение. Представиться могут кем угодно — сотрудником полиции, ФСБ, Следственного комитета, Центробанка, службы безопасности Компании.

- **Использование сайтов-двойников, фейковые страницы в социальных сетях, фейковые аккаунты в мессенджерах:** мошенники с целью получения персональных данных могут создать полную копию сайта, страницы в социальных сетях либо фейковые аккаунты в мессенджерах. Иногда пользователи мессенджеров, чьи номера телефонов не сохранены в вашем списке контактов, могут рассылать подозрительные или мошеннические сообщения, пытаясь обманом вынудить вас сообщить им личную информацию или платежные данные.

- **Вирусные электронные письма:** мошенники рассылают электронные письма от имени государственных учреждений, интернет-магазинов, банков, сайтов знакомств и т.п. Они призывают открыть вложенный в письме файл или перейти по ссылке.

Выполнение несложных рекомендаций, указанных в настоящем документе, позволит Клиентам Общества свести риск совершения незаконных финансовых операций от их имени к минимуму.

2. РЕКОМЕНДАЦИИ

2.1. Мобильный телефон

Мобильный телефон используется Клиентами Общества для получения Кода подтверждения, Уникального кода, одноразовых паролей в SMS-сообщениях.

При использовании мобильного телефона следует придерживаться следующих советов:

1. При взаимодействии с Обществом указывайте в качестве основного номера телефона номер, который принадлежит Вам лично (договор на услуги сотовой связи, заключен на Ваше имя);

2. Включите запрос пин-кода SIM – карты при включении телефона;

При поддержке телефоном соответствующей функции, выполните следующие действия:

- включите блокирование экрана телефона после определенного времени неактивности;
- включите запрос пин-кода телефона, отпечатка пальца или графического ключа для разблокировки телефона;
- установите запрет на отображение информации из вновь поступивших сообщений на экране блокировки;
- включите и настройте функцию поиска, удаленного блокирования и удаленной очистки потерянного телефона;
- установите запрет на установку в телефон приложений из ненадлежащих источников.

3. При установке новых приложений на телефон обращайте внимание за запрашиваемые ими разрешения. Не давайте приложениям разрешения на чтение SMS, если такой доступ не нужен им для выполнения их основных функций.

4. Не переходите по ссылкам из SMS и сообщений, особенно если ВЫ не ждали такие сообщения.

5. Регулярно обновляйте операционную систему телефона и установленные в телефоне приложения (не отключайте автоматическое обновление).

6. В случае утраты телефона воспользуйтесь функцией поиска телефона, если ранее ее активировали. Если с использованием функции поиска найти телефон не удалось или Вы ранее не активировали эту функцию, обратитесь с паспортом в офис своего сотового оператора для блокирования утерянной вместе с телефоном SIM-карты и выпуска новой.

2.2. ПИН-код

ПИН-код - это секретная комбинация цифр, используемая для подтверждения операций с Вашей банковской карты международной платежной системы MasterCard, Visa или МИР.

При использовании ПИН-кода рекомендуется: не сообщать ПИН-код третьим лицам, включая сотрудников Общества, не записывать его на Вашей банковской карте, не хранить записанный ПИН-код там, где он будет доступен третьим лицам.

2.3. Защита от вирусов

Вирусы — это программы для компьютеров или мобильных устройств, предназначенные для нанесения вреда. Функционал вирусов может быть разным: показ нежелательной рекламы, кража паролей (в том числе, из SMS — сообщений) и данных банковских карт, совершение незаконных финансовых операций от имени клиента.

Практически все вирусы имеют функцию собственного распространения или заражения всех доступных им устройств.

Отсутствие вирусов на устройствах (компьютерах, сотовых телефонах, планшетах), с

которых Вы работаете с системами дистанционного обслуживания Обществом, является залогом безопасности Ваших денежных средств.

2.4. Если Вам позвонили сотрудники полиции, ФСБ, Следственного комитета, Центробанка, службы безопасности Компании и т.д.:

• Не торопитесь выполнять указания звонившего.

• Если во время телефонного разговора неустановленное лицо просит Вас назвать какие-либо Ваши персональные данные, банковские реквизиты, PIN-код (в том числе направленные Вам посредством sms-сообщения во время разговора), а также иную личную информацию, то необходимо срочно закончить разговор.

• При любых подозрениях откажитесь от дальнейшего взаимодействия с посторонним лицом и самостоятельно свяжитесь с организацией, от имени которой оно обращается.

• Если неустановленное лицо обращается к Вам от имени Вашего родственника, близкого человека или знакомого с информацией о том, что он попал в неприятную ситуацию, в результате которой ему грозит возбуждение уголовного дела, и, если звонящий просит передать взятку якобы сотруднику правоохранительных органов, готовому урегулировать вопрос, следует задать уточняющие вопросы ответы, на которые знаете только вы оба. В случае появления сомнений, необходимо прекратить взаимодействия и постараться самостоятельно связаться с лицом, от имени которого Вам звонили.

• Воспользуйтесь опцией, которая заблокирует нежелательные звонки. Некоторые сервисы просто блокируют незнакомые номера, другие же более избирательны. Есть программы, которые при входящем звонке указывают, что это может быть нежелательный номер. Если вам звонили с незнакомого номера и сбросили, то перезванивать не стоит. Возможно, это мошенническая махинация, из-за которой потом будут списаны деньги.

2.5. Использование сайтов-двойников, фейковые страницы в социальных сетях, фейковые аккаунты в мессенджерах:

• Всегда обращайте внимание на адрес сайте. В нем может быть изменения только одна буква или отличаться доменый адрес (.com вместо .ru).

• Если сайт или страница в соцсети, а также предлагаемые на ней условия выглядят подозрительно, немедленно покиньте её.

• При получении сообщения или звонка посредством мессенджеров обратите внимание: знаком ли номер, с которого Вам пишут (звонят)? Вас торопят при получении от Вас информации? Вам угрожают или просят поверить на слово? Вас просят перевести деньги, сообщить код, пароль, PIN-код или другие личные данные?

• Завершите звонок либо перестаньте отвечать этому пользователю. Если вы не можете подтвердить личность отправителя, не сообщайте ему никаких личных или платежных данных.

• Заблокируйте пользователя, чтобы он больше не мог с вами связаться, и пожалуйтесь на него администратору мессенджера, социальных сетей.

2.6. Вирусные электронные письма:

• Основные признаки фишинговых писем:

✓ Письмо от компании, с которой вы никогда не взаимодействовали;

✓ Предлагается купить качественный товар с невероятной скидкой;

✓ Содержится уведомление о выигрыше ценных призов и подарков;

✓ Предлагается высокооплачиваемая работа, в т.ч. без наличия специальных знаний;

✓ Содержится информация о наличии претензий со стороны государственных учреждений, банков и т.п.

✓ Ссылки в письме содержат подозрительные имена сайтов;

✓ Подозрительный адрес отправителя.

• Никогда не переходите по ссылкам и не открывайте вложенные файлы если письмо вам кажется подозрительным. Ссылка или файл как правило содержат вирус, который даёт мошенникам полный доступ ко всем данным на вашем устройстве.

Во избежание мошенничества с использованием Ваших персональных данных:

1. Не принимать вызовы от незнакомых и скрытых номеров.
2. Регулярно обновляйте операционную систему и установленные в ней приложения (включите автоматическое обновление);
3. Не сообщайте никому PIN-коды, коды из sms-сообщений и тп.;
4. Не публикуйте персональные данные в открытом доступе в интернете;
5. Не передавайте документы посторонним лицам без обоснованной причины;
6. Не оставляйте оригиналы и копии документов без присмотра;
7. В случае утери паспорта — незамедлительно обратитесь в правоохранительные органы для оформления заявления об утере паспорта для внесения его в реестр недействительных паспортов РФ;
8. Не сообщайте и не подтверждайте персональные данные посторонним лицам по телефону (мессенджерах, соцсетях и пр.);
9. Не давайте фотографировать, переписывать информацию из документов;
10. Не оставляйте данные своих документов и банковских карт на подозрительных сайтах.
11. Не открывайте файлы и не переходите по ссылкам, пришедшим в сообщениях электронной почты, служб мгновенных сообщений (Skype, WhatsApp, Viber и т. п.) и социальных сетей, которые Вы не ждете;
12. Установите запрет на установку в телефон приложений из ненадлежащих источников;
13. Регулярно запрашивайте отчёт о кредитной истории. Законодательно закреплено право граждан 2 раза в год бесплатно запрашивать отчёт о кредитной истории.

Если вы столкнулись с действиями мошенников, незамедлительно обратитесь

в ООО МКК «Гиллион»:

1. Обращение может быть направлено посредством почтового отправления по адресу: 660131, Красноярский край, город Красноярск, Ястынская улица, дом 19а помещение 213, кабинет 1 либо по адресу электронной почты: gillion24@yandex.ru;
2. В обращении укажите каким образом неустановленное лицо воспользовалось Вашими персональными данными с целью оформления договора потребительского займа.
3. Приложите документы, подтверждающие факт оформления договора потребительского займа третьим лицом (например: скан документа, удостоверяющего личность, Ваше фото, ответ оператора сотовой связи о непринадлежности Вам абонентского номера телефона, использованного при оформлении договора и т.п.). Указанные документы необходимы для проведения внутренний проверки, сравнительного анализа с документами, предоставленными при оформлении договора.

Для получения дополнительной информации Вы можете обратиться по номеру телефона: 8-800-333-37-03.

Будьте бдительны и осторожны!
Не доверяйте тому, кого впервые слышите!
Сохраняйте рациональность!

Редакция 2024 г.