ООО «Южный ломбард» ИНН 6154069878

347927, Ростовская обл., г. Таганрог, ул. Чехова 307 А литера М, комнаты 1-6

Утверждены
приказом директора
№3-ИБ от 27.05.2019г.,
действуют с 01.06.2019г.

Рекомендации по защите информации для наших клиентов ООО «Южный ломбард»
(о мерах по предотвращению несанкционированного доступа к информации,
о рисках несанкционированного доступа к информации), далее - "Рекомендации"

1. Общие положения.

1.1. Под защищаемой информации следует понимать, в частности: ваши (клиента) персональные данные, ваши паспортные данные, информация о регистрации по месту жительства (пребывания), информация о вашем счете в банке, о ваших кредитных и дебетовых карточках - особенно номер карты и пин код, информация о вашем номере телефона и электронной почте.

Отсюда, **советуем защищать любую информацию, используя которую недобросовестные третьи лица, читай - мошенники, могут получить доступ к вашим деньгам или иным образом вам навредить**.

К примеру, без вашего ведома взять на ваше имя кредит (в банке, в микрофинансовой организации, у иного кредитора), деньги получит мошенник - а платить по кредиту вам.

1.2. В целях исполнения "Положения об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций" (утв. Банком России 17.04.2019 № 684-П, зарегистрировано в Минюсте РФ 16 мая 2019 г.) уведомляет клиентов ООО «Южный ломбард» (ИНН 6154069878, далее - "Ломбард") о возможных рисках получения несанкционированного доступа к защищаемой информации:

2. Риски.

Доступ к вашей информации со стороны третьих лиц может повлечь за собой:

2.1. риски разглашения информации конфиденциального характера: сведений об операциях, активах, состоянию счетов, подключенных услугах, персональных данных, иной значимой информации. **Ваши данные и информация, в т.ч. интимного характера, "утекут" в сеть, станет доступна каждому.**

2.2. риски совершения операций с доступными активами, подключение и отключение услуг (в том числе платных), внесение изменений в регистрационные данные клиента, использование счетов и находящихся на них активов для прикрытия иных действий, носящих противоправный характер, совершения иных действий против воли клиента. **У вас могут украсть деньги с карточки, взять на вас кредит, или открыть на вас фирму (юр. лицо) - для последующих преступных целей.**

2.3. Разрушительное воздействие на носители информации и саму информацию, обернется как минимум утратой информации.

3. Общие рекомендации.

Для защиты информации от воздействия шпионских, вредоносных программ (вирусы), а также программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия

незаконным финансовым операциям, а также для предотвращения несанкционированного доступа к защищаемой информации, в том числе при утрате клиентом устройства, с использованием которого клиент проводил финансовые операции, контролю конфигурации устройства, с использованием которого клиент действовал в целях проведения финансовой операции, и своевременному обнаружению воздействия вредоносного кода, советуем:

3.1. Организуйте режим использования устройства, с которого вы совершаете финансовые операции, так, чтобы исключить доступ третьих лиц. Не бросайте сотовый телефон, где попало. Не допускайте к своему рабочему компьютеру (или ноутбуку) кого попало. Установите пароль на включение и разблокировку устройства. В идеале - купите телефон со сканером отпечатков пальцев, чтобы пользоваться могли только вы.

3.2. Используйте на вашем устройстве только лицензионное программное обеспечение. Не ставьте программное обеспечение, полученное из сомнительных источников (торренты и прочие "файлопомойки").

3.3. Своевременно устанавливайте на ваше устройство обновления безопасности операционной системы и интернет-браузера. Советуем использовать операционную систему Windows версии не ниже 7, а операционную систему Андроид - не ниже 6.

3.4. Используйте дополнительные програмные средства защиты - межсетевой экран, брандмауэр, программу защиты "огненная стена" (firewall). Также используйте антивирус самой последней версии. Из бесплатных хорош Avast.

3.5. Если вы системный администратор, урежьте права пользователя до необходимого минимума, чтобы работник мог исполнять трудовую функцию - и не более того. Пользователь не должен обладать полномочиями администратора.

3.6. Если вы вдруг утратили устройство, с которого вы делаете финансовые операции (телефон, смартфон), советуем **СРОЧНО**:

1). связаться с вашим банком и заблокировать банковские карточки; *и*

2). связаться с вашим оператором сотовой связи и заблокировать СИМ-карту; *и*

3). сменить все пароли, к которым могут получить доступ злоумышленники, используя ваше устройство; *и*

4). написать заявление в полицию о краже, в заявлении указать IMEI (уникальный номер) вашего телефона (указан в документах к телефону); *и*

5). сообщить нам любым возможным способом.

4. Защита информации паролями.

4.1. **НЕ ИСПОЛЬЗУЙТЕ ПРОСТЫЕ ПАРОЛИ** типа 12345, qwerty,][poiuy, дату своего рождения, номер вашего автомобиля (мотоцикла) и т.д. По общепринятой классификации, пароли бывают четырех степеней защищенности (сложности): слабый, средний, сильный, очень сильный.

К примеру, пароль "avalon" - слабый. Однако, если добавить цифры - 546807, то получится avalon546807, и этот пароль уже будет средним. Если помимо цифр добавить одно или два слова, к примеру, написать "avalon546807_V_zemLe_bez_radosty!!!" - то этот пароль будет как минимум сильным. **Уровень вашего пароля должен быть как минимум сильный**.

4.2. Как сделать сильный пароль:

1). длина пароля - не менее 8 символов; *и*

2). пароль должен состоять из символов латинского алфавита в разных регистрах, т.е. маленькие буквы и БОЛЬШИЕ ВОТ ТАКИЕ БУКВЫ; *и*

3). используйте не только буквы и цифры, но и спец. символы - точки, запятые, знаки пунктуации.

Примеры сильных паролей:

_lombard_3_KrOkODil_leTit_4_na_seVer__ *или*
3000_brunetka!_Alchet&_KrEdiT_} *или*
789_zalzil_cha!!!sy_do_zarplaty_@

4.3. В идеальном пароле слова не имеют смысла. Однако такой пароль сложно запомнить. Поэтому советуем закладывать в пароль смысла ровно столько, чтоб вы могли запомнить пароль, как в примерах выше.

4.4. Не записывайте пароли в общем доступе - бумажка на мониторе, под клавиатурой, на календаре, прочие легкодоступные места. Не говорите пароли третьим лицам, включая друзей и родственников.

4.5. **Не храните пароли в текстовых файлах на компьютере (ином устройстве)**!

4.6. Не используйте один и тот же пароль везде. Злоумышленники крадут учетные данные на сайтах со слабой безопасностью, а затем пытаются использовать те же пароли и имена пользователя, чтобы получить доступ к более защищенным ресурсам, например, банковским сайтам.

4.7. Старайтесь регулярно менять пароли - хотя бы раз в месяц. Установите автоматическое напоминание, которое будет уведомлять вас о необходимости сменить пароли на используемых вами ресурсах.

5. Антивирусная защита.

5.1. Используйте ТОЛЬКО лицензионное программное обеспечение, далее - "ПО".

5.2. Ваш антивирус должен постоянно обновляться, не реже раза в неделю, а лучше - раз в день.

5.3. Если какая-то программа или человек просят вас отключить антивирусную программу, чтобы поставить другую программу, посмотреть картинку, открыть архив с файлом - **НЕ СОГЛАШАЙТЕСЬ!!!**.

5.4. Как минимум раз в месяц проверяйте ваше устройство антивирусом - в идеале, полная проверка с максимальным уровнем эвристики.

5.5. Если в вашем антивирусе не такой функции, установите программу, которая позволяют отслеживать так называемые "фищинговы" и шпионские программы.

6. Азы безопасности в сети Интернет.

6.1. Заведите надежный почтовый ящик на приличном сайте с хорошей репутацией - гугл, маил ру, яндекс.

6.2. Настройте черный список, куда вносите все подозрительные письма (спам).

6.3. Не открывайте подозрительные письма.

6.4. Настройте двухуровневую проверку для входа в почтовый ящик. Так, чтобы для входа в почтовый ящик нужно было не только ввести пароль, но и дополнительный код, который вам шлют на телефон по СМС при попытке входа в почтовый ящик.

6.5. Вырабатывайте иммунитет к стандартным уловкам мошенников, письма в духе "вы выиграли миллион!", "вы получили наследство от давно помершего дедушки", "вас беспокоит ваш банк" (с "левого" почтового адреса") - стирайте сразу и безжалостно, отправителя - в черный список.

6.6. Крайне осторожно относитесь к файлам в сети. Помните: если вам предлагают скачать что-то бесплатно, вирус почти всегда идет в комплекте.

6.7. Предыдущие два пункта применимы и к СМС-сообщениям.

7. Проверяйте свою кредитную историю.

Если мошенники все же тайком от вас взяли на вас кредит, это можно отследить через "Национальное бюро кредитных историй". Мало кто знает, но два раза в год выписку из указанного бюро можно получить бесплатно. Как:

7.1. Зайдите на сайт "Национальное бюро кредитных историй" по адресу: https://person.nbki.ru

7.2. Создайте на этом сайте свою учетную запись.

7.3. Дождитесь письма со ссылкой для активации учетной записи. Письмо придет на ваш электронный ящик, указанный при регистрации. Активируем запись по ссылке из письма.

7.4. Заходим в учетную запись. Заполняем в личном кабинете паспортные данные. Нажимаем на кнопку "Проверить через Госуслуги". (вы должны быть зарегистрированы на Госуслугах, тут: https://www.gosuslugi.ru).

7.5. Нажимаем на кнопку "Получить КИ". Открывается выписка в виде .PDF файла - обязательно сохраните! - где видны ваши долги (если есть).

КОНЕЦ ДОКУМЕНТА