ПАМЯТКА ДЛЯ КЛИЕНТОВ

О мерах по обеспечению информационной безопасности

Уважаемый Клиент!

ООО СК «Паритет-СК» (Общество с ограниченной ответственностью), далее – «Страховая компания», напоминает Вам о необходимости соблюдать принципы обеспечения информационной безопасности с целью защиты информации от воздействия вредоносного кода и исключения случаев несанкционированного доступа к Вашему электронному устройству.

Риски получения несанкционированного доступа к информации прежде всего связаны с «фишингом» (использованием ложных ресурсов сети Интернет с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами), а также воздействием вредоносного кода.

«Фишинг» – попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

Антивирусная защита осуществляется с целью исключения возможностей появления на электронных устройствах, с которых осуществляется оплата услуг, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения (далее – ПО) либо на перехват информации, в том числе паролей.

1. Рекомендации по защите информации от воздействия вредоносного кода

1.1. На персональном компьютере Клиента должно быть установлено лицензионное антивирусное программное обеспечение (ПО).

1.2. Антивирусное ПО должно регулярно обновляться. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т. е. не требующий ответов пользователя при обнаружении вирусов. Лечение (удаление) зараженных файлов производится антивирусным средством в автоматическом режиме.

1.3. Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка жесткого диска персонального компьютера (электронного устройства) на предмет наличия вирусов и вредоносного программного кода. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного средства.

1.4. Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (CD/DVD дисках, USB-накопителях и т. п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.

1.5. При использовании сети Интернет для обмена почтовыми сообщениями необходимо применять антивирусное ПО, разработанное специально для почтовых клиентов.

1.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа ПО, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т. п.) рекомендуется приостановить работу с системой до полного устранения неисправностей.

1.7. Старайтесь не использовать компьютер (электронное устройство), с которого Вы осуществляете переводы денежных средств, доступы к Вашим личным кабинетам для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.

1.8. Не открывайте файлы, полученные по электронной почте от неизвестных отправителей.

2. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

2.1. Мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете (например, Банка), и предназначены для сбора конфиденциальной информации обманным путем.

2.2. 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.

2.3. 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.

2.4. Опасайтесь безличных обращений, таких как «Уважаемый пользователь», или обращения по адресу электронной почты. В настоящем электронном письме Банк всегда приветствует Вас, обращаясь по имени и фамилии либо по названию компании. Типичное фишинговое письмо начинается с обезличенного приветствия.

2.5. 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 угрожает опасность, если Вы немедленно не обновите критически важные данные.

2.6. 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 (например, начинается с http:// вместо https://), не переходите по этой ссылке.

3. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

3.1. Рекомендуем регулярно менять пароль для работы со своими учетными данными. Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

3.2. Рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, на которых Вы вводите конфиденциальные данные (например, сведения о Вашем банковском счете и т. д.).

3.3. Не записываете пароли на бумажных листках (или в текстовых файлах на компьютере), оставляйте их в легкодоступных местах (на рабочем столе), не передавайте неуполномоченным лицам.

3.4. Рекомендуем исключить возможность физического доступа к электронному устройству, с которого Вы осуществляете работу, посторонних лиц.

4. Рекомендации по безопасности использования платёжных карт

Соблюдение рекомендаций, содержащихся в Памятке, позволит обеспечить максимальную сохранность банковской карты, ее реквизитов, ПИН и других данных, а также снизит возможные риски при совершении операций с использованием банковской карты.

4.1. Никогда не сообщайте свои ПИН-коды третьим лицам, в том числе родственникам и знакомым.

4.2. ПИН необходимо запомнить и не хранить его на материальных носителях, особенно совместно с банковской картой.

4.3. Никогда ни при каких обстоятельствах не передавайте банковскую карту для использования третьим лицам, в том числе родственникам.

4.4.С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета целесообразно установить ежемесячный лимит на сумму операций по банковской карте и одновременно подключить электронную услугу оповещения о проведенных операциях (например, оповещение посредством SMS-сообщений или иным способом).

4.5. При получении просьбы сообщить персональные данные или информацию о банковской карте (в том числе ПИН) не сообщайте их. Перезвоните эмитенту банковской карты (организацию, выдавшую карту) и сообщите о данном факте.

4.6. Не рекомендуется отвечать на электронные письма, в которых от банка предлагается предоставить персональные данные. Не следуйте по «ссылкам», указанным в письмах (включая ссылки на сайт банка), т. к. они могут вести на сайты-двойники.

4.7. В целях информационного взаимодействия с банком — эмитентом банковской карты рекомендуется использовать только реквизиты средств связи, которые указаны в документах, полученных непосредственно в банке.

4.8. Помните, что в случае раскрытия ПИН, персональных данных, утраты банковской карты существует риск совершения неправомерных действий с денежными средствами на вашем банковском счете со стороны третьих лиц.

4.9 В случае если имеются предположения о раскрытии ПИН, персональных данных, позволяющих совершить неправомерные действия с вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться к эмитенту банковской карты и следовать указаниям сотрудника данной кредитной организации.

5. Рекомендации при совершении операций с банковской картой через сеть Интернет

5.1. Не используйте ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.

5.2. Не сообщайте персональные данные или информацию о карте или банковском счёте через Интернет, на пример: ПИН, пароли, срок действия карты, лимиты, история операций.

5.3. Рекомендуется для оплаты покупок в сети Интернет использовать отдельную банковскую карту (виртуальную карту) с предельным лимитом.

5.4. Следует пользоваться интернет-сайтами только известных и проверенных организаций, проверять правильность написания адреса сайта в строке браузера, т. к. похожие адреса могут использоваться для осуществления неправомерных действий.

5.5. Рекомендуется совершать покупки только со своего компьютера (электронного устройства). Если покупка совершается с использованием чужого компьютера (электронного устройства), не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились.