УТВЕРЖДЕНО ПРИКАЗОМ
АО «Банк ДАЛЕНА»
от 10.06.2024 №2-ОД

РЕКОМЕНДАЦИИ
Клиенту (пострадавшему) - юридическому лицу, индивидуальному предпринимателю или физическому лицу, занимающемуся в установленном законодательством порядке частной практикой, в случае попытки или хищения денежных средств в системе дистанционного банковского обслуживания (далее - Рекомендации)

Клиенту в случае попытки несанкционированного списания денежных средств с расчетного счета Клиента необходимо руководствоваться пунктами 1-5, 15 Рекомендаций, в случае хищения денежных средств с расчетного счета Клиента - пунктами 1-15 рекомендаций:

1. Немедленно прекратить любые действия с электронными устройствами (далее - ЭУ): персональный компьютер, ноутбук, планшетный компьютер и т.п., подключенным к системе дистанционного банковского обслуживания (далее – ДБО), обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь все аккумуляторные батареи из ноутбука и т.п.), отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi, Dial-Up и др.) или перевести в режим гибернации ("спящий" режим). При отсутствии возможности обесточивания ЭУ, осуществить отключение по штатной процедуре и запротоколировать указанный факт.

2. Отозвать перевод денежных средств, обратившись немедленно к специалисту отдела операционного обслуживания в АО «Банк ДАЛЕНА» по телефону с требованием о блокировке доступа Клиента к системе ДБО, приостановке исполнения платежа или на номер Службы поддержки клиентов АО «Банк ДАЛЕНА» 8 (495) 673-10-10.

3. Проинформировать все банки, с которыми Клиент имеет договорные отношения, предусматривающие использование ДБО, о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой информации.

4. Дополнительно обратиться в АО «Банк ДАЛЕНА» с письменным заявлением об отзыве платежа, приостановлении платежа, блокировании доступа к системе ДБО (Приложение № 1), а также о компрометации ключей и необходимости смены пароля (закрытого ключа). Копия заявления должна быть направлена в банк плательщика незамедлительно по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в Банк в течение одного рабочего дня.

5. Направить в АО «Банк ДАЛЕНА» Справки по факту инцидента информационной безопасности в системе ДБО (Приложение № 2), а также подтверждающие документы при их наличии (Приложение № 3) в срок не позже следующего рабочего дня после фиксирования инцидента.

6. В целях сохранения доказательной базы не предпринимать никаких действий для самостоятельного или с привлечением сторонних ИТ-специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности ЭУ, не отправлять ЭУ в сервисные службы ИТ для восстановления работоспособности.

7. **Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (глава 21 УК РФ) (Приложение № 4). Копию заявления предоставить в отдел операционного обслуживания Банка в срок не более 2 рабочих дней со дня выявления факта хищения денежных средств.**

8. Оперативно обратиться в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить копию заявления о возбуждении уголовного дела либо копию талона, содержащего порядковый номер из книги учета сообщений о преступлениях (далее - КУСП) содержащую отметку правоохранительного органа о его приеме, а также документы, подтверждающие неправомерность списания денежных средств с расчетного счета. Обращаем внимание на то, что ходатайство необходимо направлять в суд по почте либо нарочно (отправка ходатайства через сервис «Мой арбитр» недопустима).

9. При возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи (Приложение № 5) для получения в электронной форме журналов соединений с Интернет с электронного устройства Клиента или из его локальной вычислительной сети (далее - ЛВС) как минимум за три месяца, предшествовавшие факту хищения денежных средств.

10. Произвести фотосъемку ЭУ (с подключенными кабелями и иными периферийными устройствами), рабочего места и его расположения в помещении. Обеспечить сохранность (целостность) ЭУ как возможного средства совершения преступления, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин, мастичная печать, пломбы и т.п.) и по возможности зафиксировать средства контроля целостности фотографированием со всех ракурсов. Если позволяют размеры ЭУ, следует поместить его в непрозрачный пакет (мешок) и заклеить горловину. При необходимости ведения хозяйственной деятельности - задействовать другое ЭУ.

11. Предпринять меры для обеспечения сохранности и неизменности записей с внутренних и внешних камер систем видеонаблюдения, журналов систем контроля доступа, средств обеспечения и разграничения доступа в сеть Интернет (при наличии таковых) за максимальный период времени, как до, так и после даты совершения хищения денежных средств.

12. Провести сбор записей с межсетевых экранов и других средств защиты информации, серверов баз данных и иных компонент клиентского приложения системы ДБО, систем авторизации пользователей (AD, NDS и т.д.), коммуникационного оборудования (включая АТС), ЭУ, используемых для управления денежными средствами через систему ДБО Банка, устройств, которые могут использоваться для удаленного управления указанными ЭУ.

13. Зафиксировать в протокольной форме значимые действия и события, в том числе имена лиц, имеющих доступ к ЭУ, действия с ЭУ, подключенным к системе ДБО, предшествовавшие факту хищения денежных средств, подготовить объяснения Клиента (работников Клиента) об использовании ЭУ в целях, отличных от осуществления операций в системе ДБО, посещаемых сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в банк плательщика, о сторонних лицах, побывавших в месте расположения ЭУ и т.д.

14. Все действия, указанные в пп. 1, 10, 11, 12, 13 настоящего раздела, производить с привлечением специалистов соответствующих служб Клиента, протоколировать и документировать, в т.ч. с использованием фотосъемки.

15. После окончания процедуры смены ключей не возобновлять деятельность на данной рабочей станции без проведения соответствующих технических мер, которые гарантируют полное уничтожение вирусных объектов. Если средствами антивирусных программ они не обнаружены, рекомендуется провести переустановку операционной системы с полным

форматированием жесткого диска, но только в том случае, когда уже не требуется сохранение доказательной базы в целях проведения расследования инцидента правоохранительными органами и рассмотрения судебного иска. В случае необходимости сохранения персонального компьютера в текущем состоянии, использовать в работе другой компьютер с установленным лицензионным программным обеспечением (операционные системы, офисные пакеты и пр.) и его автоматическим обновлением. Рекомендуемые для проверки, а в дальнейшем и еженедельные, следующие средства: https://virusdesk.kaspersky.ru/, http://freedrweb.com