Памятка по предотвращению хищения денежных средств системе дистанционного банковского обслуживания.

Для предотвращения хищений денежных средств, в результате компрометации электронных средств дистанционного банковского обслуживания (ДБО) необходимо:

1. Обслуживать и сопровождать средства вычислительной техники (СВТ), сетевое и телекоммуникационное оборудование, а также системное и прикладное программное обеспечение (ПО) только с привлечением доверенных, проверенных, компетентных людей и/или организаций.
2. Исключить организационными мероприятиями использование внутри сети организации не доверенных СВТ и ПО.
3. Для работы с финансовыми и платежными приложениями использовать отдельный компьютер (отдельный сегмент сети организации).
4. Обязательно использовать средства защиты с актуальными обновлениями безопасности. Антивирус, межсетевые экраны, токены.
5. Компьютер (отдельный сегмент сети организации), используемый для работы с финансовыми и платежными приложениями максимально ограничить в доступе к сети интернет.
6. Компьютеры не оставлять без присмотра и блокировать в случае отсутствия ответственного работника.
7. Регулярно обновлять системное и прикладное ПО.
8. Для защиты платежной информации использовать индивидуальные токены с электронно-цифровыми подписями (ЭЦП).
9. Исключить использование индивидуальных токенов несколькими работниками, а также передачу токенов третьим лицам.
10. Токен с ЭЦП использовать только при совершении платежей. Не держать подключенным к компьютеру постоянно. В период неиспользования хранить в запираемых шкафах, индивидуальных сейфах или опечатанных тубах.
11. Для работы с Клиент-Банком (дистанционным банковским обслуживанием) использовать выделенные, статические IP адреса, информацию о которых сообщить в Банк для проведения мониторинга и контроля при проведении платежей.

В случае обнаружения атаки на информационную инфраструктуру организации, компрометацию отдельных СВТ, подозрении хищения денежных средств:

12. Отключить USB-токены с ЭЦП от компьютеров.
13. Запретить физический доступ к рабочим местам.
14. Изменить пароли доступа к системному и прикладному ПО
15. Уведомить Банк о подозрениях и ситуации.
16. Заблокировать ЭЦП
17. Получить выписку по счету
18. Инициировать замену ЭЦП
19. Провести инвентаризацию денежных средств и операций
20. Инициировать внутреннее расследование
21. Подготовить СВТ для проведения расследования (собрать данные, сделать образы жестких дисков и дампы памяти скомпрометированных компьютеров, журналы сетевого оборудования и средств защиты информации).
22. Привлечь компетентных экспертов для сбора доказательств и проведения

расследования.

23 Подать заявление в полицию, предоставив информацию об инциденте (раскрытие хищения с высокой вероятностью не приведет к возврату денежных средств) для поиска преступников.

24 Изучить условия договора с Банком. Сотрудничать при проведении расследования.

25 Получить от МВД постановление об отказе в преследовании виновных (в случае затягивания).

26 Собрать и подать в ФНС комплект документов для возврата или зачета налогов (возможна камеральная проверка и запрос дополнительных материалов).