ЧТО ДЕЛАТЬ, ЧТОБЫ ХИЩЕНИЕ НЕ ПРОИЗОШЛО?

Для предотвращения хищения в клиент-банке и связанных с ним неприятных последствий вам необходимо:

1. Использовать USB-токены для каждого сотрудника, имеющего ключ ЭП

2. Для дополнительной защиты использовать код подтверждения из МАС-токена или SMS

3. Не держать USB-токены постоянно подключенными

4. Выбирать банки, использующие систему Fraud-мониторинг

5. Использовать отдельный ПК для работы с клиент-банком

6. Не использовать рабочий ПК для сёрфинга в Интернете

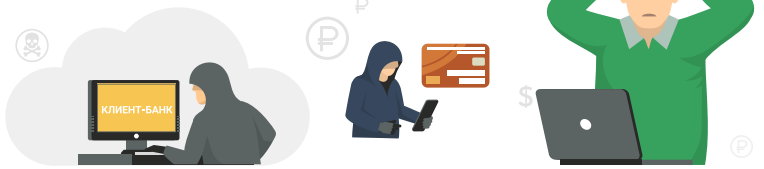
7. Не оставлять ПК без присмотра

8. Своевременно обновлять средства защиты, системное и прикладное ПО

9. Помнить, что антивирус не дает 100% защиты от вирусов

Украли деньги в клиент-банке! Что делать?

Порядок действий после обнаружения хищения средств в клиент-банке



956,1 млн. руб.
сумма хищений через клиент-банк за год

По статистике Group IB
средняя сумма одного хищения 1 250 000 руб.
сумма хищений в день 2 500 000 руб.

1 ЭКСТРЕННЫЕ МЕРЫ НА РАБОЧЕМ МЕСТЕ

- Немедленно отключить USB-токен
- Запретить доступ к рабочему месту

• Запрещается:

- Проверять компьютер с клиент-банком антивирусом
- Переустанавливать клиент-банк или операционную систему
- Продолжать работать в клиент-банке

Невозможно пользоваться своим счетом, пока нет новых ключей ЭП.

2 УВЕДОМИТЬ БАНК

- Уведомить свой банк о хищении
- Заблокировать ключи ЭП
- Получить выписку по счету
- Заменить ключи ЭП
- Подать заявление о возврате средств
- Провести инвентаризацию денежных средств

Рабочее время тратится непродуктивно.

Используйте ДБО только на компьютерах с установленными средствами антивирусной защиты с возможностью автоматического обновления антивирусных баз и специализированными программными средствами безопасности: персональными межсетевыми экранами, антишпионским программным обеспечением и т.п.