ООО КБ «АРЕСБАНК»

Инструкция о порядке действий клиентов ООО КБ «АРЕСБАНК» в случае выявления хищения денежных средств в системе электронного документооборота «Интернет-Банк»

Клиенту (пострадавшему) – юридическому лицу необходимо:

1. В случае выявления хищения денежных средств в системе ИНТЕРНЕТ-БАНК немедленно прекратить любые действия с электронными устройствами: персональные компьютеры, ноутбуки, планшетные компьютеры (далее по тексту – ЭУ), с помощью которых осуществлялась работа в системе ИНТЕРНЕТ-БАНК, обесточить ЭУ – отключить вилку ЭУ из розетки, извлечь аккумуляторную батарею из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Ethernet, USB).
2. При наличии технической возможности отозвать перевод с использованием иного ЭУ, после чего сообщить в Банк любым доступным способом о компрометации ключа системы ИНТЕРНЕТ-БАНК и о приостановке исполнения платежа и возврате средств.
3. Обратиться в Банк с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к системе ИНТЕРНЕТ-БАНК а также о компрометации ключа и необходимости его замены (Приложение № 1 к Инструкции). Копия заявления должна быть направлена в Банк незамедлительно по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в Банк течение одного дня.
4. Проинформировать все банки, с которыми вы имеете договорные отношения, предусматривающие использование ИНТЕРНЕТ-БАНК, о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой информации.
5. Произвести фотосъёмку рабочего места и его расположения в помещении. Обеспечить сохранность (целостность) ЭУ как возможного средства совершения преступления, поместив его в место с ограниченным доступом, а также в непрозрачный пакет (мешок) и опечатать горловину. При необходимости ведения хозяйственной деятельности – задействовать другое ЭУ.
6. 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.

7. Провести сбор записей с межсетевых экранов, систем авторизации пользователей (AD, NDS и т.д.), ЭУ, используемых для управления денежными средствами через систему ИНТЕРНЕТ-БАНК, устройств, которые могут использоваться для удалённого управления указанными ЭУ.

8. 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.

9. Зафиксировать на бумаге все события, которые могли показаться вам подозрительным при работе ЭУ (сообщения об ошибках, самостоятельное движение курсора мыши и т.п.).

10. В течение одного дня обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств.

11. Подготовить для Банка Справку по факту инцидента информационной безопасности в системе ИНТЕРНЕТ-БАНК (Приложение № 2 к Инструкции).

Приложение № 1
к «Инструкции о порядке действий клиентов ООО КБ «АРЕСБАНК»
в случае выявления хищения денежных средств в системе электронного документооборота «Интернет-Банк»»

ЗАЯВЛЕНИЕ ПЛАТЕЛЬЩИКА В БАНК ОБ ОТЗЫВЕ ПЛАТЕЖА, ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ И БЛОКИРОВАНИИ ДОСТУПА К СИСТЕМЕ ИНТЕРНЕТ-БАНК

_____
должность руководителя

_____
наименование банка

_____
Фамилия И.О.

Уважаемый (ая) _____
имя, отчество руководителя

«___» _____ 201__ года с нашего расчетного счета, открытого в Вашем банке, по системе дистанционного банковского обслуживания были похищены денежные средства, которые, по имеющейся информации были переведены со следующими реквизитами платежа:

Дата платежа: _____
Номер платежного поручения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____

Прошу Вас заблокировать нашу учетную запись в системе Интернет-Банк, провести процедуру компрометации всех ключей ЭП и оказать содействие в возврате денежных средств.

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

Приложение № 2
к «Инструкции о порядке действий клиентов ООО КБ «АРЕСБАНК» в случае выявления хищения денежных средств в системе электронного документооборота «Интернет-Банк»

СПРАВКА ПО ФАКТУ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ИНТЕРНЕТ-БАНК

«___» _____ 20__ неустановленным лицом через систему ИНТЕРНЕТ-БАНК была совершена несанкционированная операция по переводу денежных средств со следующими реквизитами:

Дата платежа: _____
Номер платежного поручения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____

Дополнительно сообщаю:

Количество ЭУ, настроенных для доступа в систему ИНТЕРНЕТ-БАНК: _____.

Для доступа в системы ИНТЕРНЕТ-БАНК хотя бы раз использовались

☐ корпоративные ЭУ
☐ личные ЭУ
☐ ЭУ, находящиеся в общественном пользовании

Периодичность смены ПИН-кода к Смарт-ключу системы ИНТЕРНЕТ-БАНК: _____

Для каких целей кроме системы Интернет-Банк использовалось ЭУ_____

Применяемые элементы безопасности ЭУ включают:

☐ выполняются рекомендации по обеспечению безопасности при работе в интернете https://faktura.ru/b2b/faq/bezopasnost.

☐ используется только лицензионное программное обеспечение

☐ операционная система и приложения обновляются в автоматическом режиме

☐ используется антивирусное программное обеспечение: _____

с какой периодичностью происходит его обновление_____

подключаются ли к ЭУ внешние съемные носители информации (USB-Flash, внешние жесткие диски, мобильные устройства)_____

используется ли ЭУ для работы с электронной почтой_____

☐ используются средства сетевой защиты: _____

используется ли ЭУ для работы в сети Интернет для целей, отличных от работы системы Интернет-Банк.
_____

Количество лиц, имеющих доступ ЭУ _____

Количество лиц, имеющих доступ к ключевым носителям (Смарт-ключу)_____

Иная информация, имеющая отношение к инциденту:
_____
_____
_____
_____

Подтверждаю отсутствие у меня претензий к ООО КБ «АРЕСБАНК»

_____ _____
подпись плательщика

☐ Я намерен обратиться в правоохранительные органы по факту хищения денежных средств.

Заявление в правоохранительные органы принято в ОВД _____
_____
район, округ, город, субъект федерации и иные идентифицирующие ОВД данные

и зарегистрировано за № _____ в КУСП

☐ Я не намерен обращаться в правоохранительные органы по факту хищения денежных средств.

О необходимости предоставления доступа сотрудников правоохранительных органов к электронному устройству, об ответственности за использование нелицензированного и контрафактного программного обеспечения в соответствии со статьей 146 УК Российской Федерации предупрежден.

Заявитель: _____/_____/
Дата: _____/Телефон: _____