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

Клиенту (пострадавшему) – физическому 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 и др. (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.)
2. При работе в Интернете необходимо соблюдать общие правила безопасности, применяющиеся для защиты любых данных, хранящихся на ваших ЭУ, и ваши средства будут недосягаемы для мошенников.
3. При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
4. Своевременно обновлять операционную систему (установка патчей, критичных обновлений).
5. Не использовать права администратора при отсутствии необходимости. В повседневной практике входить в систему как пользователь, не имеющий прав администратора.
6. Включить системный аудит событий, регистрирующий возникшие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.
7. Устанавливать и своевременно обновлять на компьютере антивирусное ПО (NOD32, AVP Kaspersky Symantec AntiVirus и т.д.), приобрести и регулярно обновлять лицензионную версию антивирусного ПО.
8. Антивирусное ПО должно быть запущено постоянно с момента загрузки компьютера.
9. Рекомендована полная еженедельная проверка компьютера на наличие вирусов, удаление обнаруженного вредоносного ПО.
10. При входе в Интернет использовать сетевые экраны (Kerio winroute, Outpost firewall и т.д.), разрешив доступ только к доверенным ресурсам Сети.

11. Запретить в межсетевом экране соединение с интернетом по протоколам ftp, smtp. Разрешить соединения smtp только с конкретными серверами, на которых зарегистрированы Ваши электронные почтовые ящики.

12. Не давать разрешения неизвестным почтовым программам выходить в интернет.

13. При работе в интернете не соглашаться на установку каких-либо дополнительных программ.

14. При наличии технической возможности отозвать перевод с использованием иного ЭУ, после чего сообщить в Банк любым доступным способом о компрометации данных, необходимых для аутентификации в системе ИНТЕРНЕТ-БАНК (логин, пароль, одноразовый смс-пароль), и о приостановке исполнения платежа и возврате средств.

15. Обратиться в Банк с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к системе ИНТЕРНЕТ-БАНК (Приложение №1 к Инструкции).

16. 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.

17. 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.

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

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

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

Приложение № 1
к «Инструкции о порядке действий клиентов (физических лиц) 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

_____

_____
наименование банка

_____
Фамилия И.О.

_____
(паспортные данные)

Уважаемый (ая) _____
имя, отчество руководителя

«___» _____ 201__ года с моего банковского 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 мою учетную запись в системе Интернет-Банк, провести, связанные с данным фактом процедуры 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 (физических лиц)
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
☐ личные ЭУ
☐ ЭУ, находящиеся в общественном пользовании
Периодичность смены пароля для входа в систему 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, указанные в разделе на официальном сайте Системы faktura.ru в разделе для частных клиентов на странице (**https://faktura.ru/b2b/faq/bezopasnost**).

☐ выполняются рекомендации Инструкции о порядке действий клиентов (физических лиц) ООО КБ «АРЕСБАНК», в случае выявления хищения денежных средств в системе электронного документооборота «Интернет-Банк», размещенные на официальном сайте Банка в системе Интернет на странице https://www.aresbank.ru/individuals/528

☐ выполняются Инструкции пользователя клиентов по обеспечению безопасности при работе в интернете, размещенные: Инструкция пользователя Faktura.ru Интернет – банк для частных.

☐ 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 _____

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: _____