Памятка для Клиентов о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендации по мерам безопасности при использовании системы электронного документооборота «Интернет-Банк» (далее - Интернет-Банк)

1. Рекомендуемые меры по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого клиентом осуществляется перевод денежных средств.

Пользователям Интернет-Банк рекомендуется соблюдать организационные меры по обеспечению информационной безопасности:

- пин-код Смарт-ключа и/или пароль для входа в систему Интернет-Банк (https://business.aresbank.ru/), - это Ваша личная конфиденциальная информация, ни при каких обстоятельствах не раскрывать свой Пин-код Смарт-ключа и/или пароль никому, включая сотрудников Банка. Никто не вправе требовать от Вас эту информацию ни для каких целей. Не сохранять их в текстовых файлах на компьютере либо на других электронных носителях информации, это может привести к его краже и компрометации, также не хранить Пин-код вместе с самим Смарт-ключом.
- используйте только доверенные устройства с лицензионным программным обеспечением. Проверяйте свои устройства на вирусы. Регулярно обновляйте программное обеспечение.
- по возможности минимизируйте установку стороннего программного обеспечения используйте только знакомые и проверенные приложения на мобильном устройстве, на котором установлен Интернет-Банк. Устанавливайте мобильное приложение Интернет-Банк «АРЕСБАНК» БИЗНЕС» только из App Store и Google Play (разработчик – ARESBANK Ltd).
- не позволяется установка средств удаленного администрирования (Team Viewer, rAdmin и тд.). Установку новых приложений производите только после их предварительной проверки на вирусы;
- исключите работу с Интернет-Банком в публичных интернет сетях (общедоступные wi-fi сети без паролей для подключения к ним, а также работу с Интернет-Банком, с компьютеров, расположенных в публичных местах;
- выделите отдельный компьютер (ноутбук, нетбук) с лицензионной операционной системой, который будет использоваться только для работы в системе Интернет-Банк.
- ограничьте доступ сторонних лиц к компьютеру, с которого осуществляется работа в системе Интернет- Банк, используйте учетную запись с паролем на вход в операционную систему, блокируйте компьютер перед выходом из помещения.
- своевременно обновляйте операционную систему (устанавливать патчи, критичные обновления). Не используйте устаревшие версии операционных систем;
- включите на компьютере для доступа в Интернет-Банк режим отображения расширений файлов для анализа файлов-вложений, а также системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривайте журнал и реагируйте на ошибки.
- в случае временного перерыва в работе Интернет-Банка на мобильном устройстве – осуществляйте выход из мобильного приложения Интернет-Банк;

- не записывайте и не храните пароли и/или пин-коды от Смарт-ключа и данные для входа в Интернет-Банк на бумажных листках (или в текстовых файлах на компьютере, мобильном телефоне и пр.);
- при подозрении на несанкционированный доступ к Интернет-Банку неуполномоченных лиц, несанкционированный доступ к компьютеру или мобильному устройству, а также утерю или кражу мобильного устройства с установленным мобильным приложением Интернет-Банк и/или Смарт-ключа, паролям или нарушение информационной безопасности Интернет-Банк в других случаях незамедлительно сообщите об этом в Банк по каналам связи, указанным в Договоре с Банком, а также в случаях если вы сменили номер мобильного телефона и/или если вам пришло уведомление о блокировке SIM-карты.
- регулярно контролируйте состояние счета путем просмотра выписки;
- обращайте внимание на дату и время последних входов в Интернет-Банк (данные фиксируются на первой странице после входа в систему, а также в специальном разделе «Безопасность -> Журнал сеансов работы».
- не держите Смарт-ключ постоянно подключенным к компьютеру. Подключайте его только при необходимости работы в Интернет-Банке, в остальное время храните его в сейфе.

2**. Рекомендуемые меры по контролю конфигурации устройства, с использованием которого клиентом осуществляется перевод денежных средств, и своевременному обнаружению воздействия вредоносного кода.**

В рамках обеспечения защиты информации от воздействия вредоносного кода пользователям Интернет-Банк рекомендуется:

- постоянно использовать средства антивирусной защиты на компьютерах, используемых для работы в Интернет-Банк или мобильных устройствах, на которых установлено мобильное приложение Интернет-Банк;
- установить настройки, обеспечивающие запуск антивирусного программного обеспечения в автоматическом режиме, в процессе загрузки операционной системы на компьютерах, используемых для работы в Интернет-Банк, а также постоянное функционирование антивирусного программного обеспечения в фоновом режиме в процессе работы на компьютере, используемом для работы в Интернет-Банк, или мобильном устройстве с установленным приложением Интернет-Банк;
- еженедельно проводить антивирусную проверку компьютеров, предназначенных для работы в Интернет-Банке, а также мобильных устройств с установленным приложением Интернет-Банк;
- регулярно автоматически обновлять антивирусное программное обеспечение и его сигнатурные базы;
- при работе с электронной почтой, онлайн-мессенджерами не открывать письма, сообщения и вложения к ним, полученные от неизвестных отправителей, и не переходить по содержащимся в таких письмах гиперссылкам они могут вести на фишинговые сайты, ресурсы, содержащие вредоносное ПО и тд.;
- не производить установку каких-либо программ и их обновлений загруженных из сети Интернет или из непроверенных источников, кроме лицензионного программного обеспечения по ссылке, полученной от производителя программного обеспечения, Банка или приложений, загружаемых из Apple Store или Google Play;
- При установке или обновлении программного обеспечения для работы в системе Интернет- Банк проверяйте подпись установочного файла InternetBankSetup.exe (для Windows OS) или InternetBankSetup.dmg (для MacOS) в соответствии с

инструкцией, размещенной на официальном сайте системы Интернет- Банк по адресу https://faktura.ru/.

- исключить возможность доступа и установки программного обеспечения (в том числе вредоносных программ (вирусов) посторонними лицами на компьютеры или мобильные устройства, предназначенные для работы с Интернет-Банком;
- не использовать права администратора при отсутствии необходимости. В повседневной работе использовать учетную запись с минимально необходимым набором прав;
- при проведении операций в Интернет-банке на Ваш мобильный телефон приходят сообщения с Одноразовыми секретными паролями для подтверждения операций в SMS и push сообщениях, убедитесь в том, что у посторонних нет доступа к указанным сообщениям. Установите ограничение доступа на телефон используя ПИН-код, графический ключ, пароль или воспользуйтесь другой технологией ограничения доступа к устройству;
- исключить возможность взлома или перепрошивки операционной системы (получение root прав), установленной на мобильном телефоне с установленным приложением Интернет-Банк при подозрениях на наличие вредоносных программ (вирусов) на компьютере, предназначенном для работы с Интернет-Банком, полностью воздержаться от входа и использования Интернет-банк и проведения платежей до исправления ситуации;
- если вам пришло SMS с одноразовым паролем подтверждения для платежа, который вы не совершали, известите Банк! Ни в коем случае не вводите и никому не сообщайте пришедший пароль;
- не указывайте номер мобильного телефона, на который приходят SMS с разовым паролем, в социальных сетях и других открытых источниках;
- организовать доступ в сеть Интернет с использованием межсетевых экранов, разрешив доступ только к доверенным ресурсам сети и Интернет;
- настроить запрет на выход в сеть Интернет неизвестным для Вас программам;
- осуществлять периодический контроль активного программного обеспечения, установленного на компьютере для доступа в Интернет-Банк;
- использовать дополнительные меры защиты, предлагаемые Банком.

3. Рекомендации по защите информации при обнаружении в сети "Интернет" ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемой Банком системы Интернет-Банк, и (или) использующих зарегистрированные товарные знаки и наименование Банка, и рекомендуемых мерах по обнаружению указанных ресурсов и программного обеспечения.

Пользователям Интернет-Банк рекомендуется соблюдать меры предосторожности при использовании сети Интернет для проведения расчетов с использованием Интернет-Банк:

- размещение информационных материалов Банка в сети Интернет осуществляется

только по адресам – https://www.aresbank.ru/, https://tl.aresbank.ru/;

- в случае обнаружения в сети Интернет ложного веб-сайта Банка отличных от

https://www.aresbank.ru/, https://tl.aresbank.ru/, программного обеспечения, имитирующего программный интерфейс Интернет-банка, и (или) использующиеся зарегистрированные товарные знаки и наименование Банка, а также, в случаях, если с Вами пытаются связаться по электронной почте или иным способом лица с

требованиями о предоставлении персональных идентификаторов доступа к Интернет-банку или иной информации, необходимо немедленно сообщить об этом в Банк по телефонам, адресам электронной почты, указанным в договоре с Банком, помните Сотрудники Банка никогда не будут требовать от Вас сообщить или указать где-либо свои учетные данные;

- Банк использует WEB-сайт по адресу https://business.aresbank.ru/ для осуществления электронного документооборота в системе Интернет-Банк для клиентов не являющихся физическими лицами.

4. При выявлении Клиентом компьютерных атак на Клиента, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия Клиента, Клиент вправе направить в Банк Уведомление по компьютерным атакам, согласно Стандарту Банка России СТО БР БФБО-1.5-2023 «Безопасность финансовых (банковских) операций Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности О формах и сроках взаимодействия Банка России с кредитными организациями, некредитными финансовыми организациями и субъектами национальной платежной системы при выявлении инцидентов, связанных с реализацией информационных угроз, и инцидентов операционной надежности».

В Таблице 1 указаны критерии Уведомления по компьютерным атакам. В Таблицах 2, 3 указана форма представления в Банк данных по компьютерным атакам.

К рассмотрению принимаются Уведомления по компьютерным атакам, предоставленные ТОЛЬКО на внешних съемных материальных носителях (DVD/CD диски, usb- flash устройствах), содержащие полную информацию из обязательных полей (условно-обязательных полей) Таблицы 2, Таблицы 3.

Таблица 1

Критерии Уведомления по компьютерным атакам

№ п/п	Тип компьютерной атаки	Наименование компьютерной атаки	Критерий информирования
1	Login attempt	Неуспешные попытки авторизации	Были выявлены факты перебора аутентификационных данных (логинов-паролей), электронных почтовых адресов, папок сервера, URL различных веб-интерфейсов или зафиксирована попытка получения любых иных вышеуказанным методом данных. В ходе реагирования на атаку удалось установить, что перебор НЕ вызван ошибочными действиями легитимного пользователя, ошибками конфигурации или функционированием средств анализа защищенности, используемых участником. Количество неуспешных попыток перебора для одного логина превышает показатели, установленные внутренними регламентами организации (в случае отсутствия такого показателя, превышает 5 неуспешных попыток). **Имеется информация об источниках вредоносной активности**

2	Social engineering	Попытки социальной инженерии	Были выявлены факты использования методов социальной инженерии в отношении Клиента с использованием: - звонка с телефонного номера; - СМС-сообщения; - электронной почты; - систем мгновенного обмена сообщениями (мессенджерами); - иного канала обмена информацией внутри организации или взаимодействия с Банком. **Наличие информации, с использованием которой осуществлялось применение методов социальной инженерии, в том числе номер телефона, e-mail-адрес, технический заголовок письма, текст письма/СМС/сообщения системы мгновенных сообщений и т.д.**
3	Phishing	Выявление фишинговой рассылки или ресурса	Были выявлены ресурсы в сети Интернет, содержащие информацию, вводящую Клиента, а также иных взаимодействующих с ним лиц в заблуждение, вследствие сходства доменных имен, оформления и (или) содержания ресурса с оформлением и (или) содержанием официальных ресурсов Клиента **Наличие URL фишингового ресурса.** Дополнительно выявлены промежуточные инфраструктурные элементы фишинговой инфраструктуры (промежуточные сервера для проксирования пользователя к фишинговой странице) или зарегистрированные, но еще не анонсированные доменные имена с признаками фишинга (хотя де-юре такое доменное имя как бы уже "опубликовано" в регистратуре ТЦИ и т.п.)
4	[Infection attempt]	Попытки внедрения модулей ВПО	Были выявлены ресурсы в сети Интернет, содержащие вредоносный код или информацию, позволяющую осуществить неправомерный доступ к информационным системам Клиента, используемым при получении финансовых услуг, в том числе путем неправомерного доступа к конфиденциальной информации Клиента

Таблица 2

Форма представления в Банк данных по компьютерным атакам

Порядковый номер	Категория элемента данных	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	О	-	[NTF_CA]	Предзаполненное поле
2	Описание компьютерной атаки	Н	-	Текстовое поле	Текстовое описание компьютерной атаки (в том числе дополнительные сведения о способе реализации КА, способе выявления КА и т.д.).
4	Классификация компьютерной атаки	О	-	[Infection attempt] [Login attempt] [Phishing] [Social engineering]	В соответствии с классификатором компьютерных атак, приведенном в Таблице 1
5	Дата	О	-	В соответствии с RFC 3339	По московскому времени [UTC + 03:00]
15	Сведения об объектах или субъектах вредоносной активности	УО	Состав данных зависит от поля "Тип компьютерной атаки" и приведен в Таблице 3 " Сведения об объектах или субъектах вредоносной активности "		
16	Ограничительный маркер TLP	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное

Таблица 3

Сведения об объектах или субъектах вредоносной активности

Наименование компьютерной атаки	**Сведения об объектах или субъектах вредоносной активности**				
	Описание UI	**Обязательность полей**	**Условие обязательности**	**Правило заполнения**	**Примечание**
Попытки внедрения модулей ВПО	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Указываются все выявленные источники вредоносной активности Компьютерной атаки
	IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
	Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
	URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов или файл	
	e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов или файл	
	Файл ВПО	УО	Обязательно заполняется одно из полей	Файл	Заполняется как минимум для одного образца ВПО. Блок заполняется
	URL для скачивания			Текстовое поле	
	Хеш-сумма	Н	-	Текстовое поле	

	Алгоритм хеширования		-	[SHA256] [SHA1] [MD5]	отдельно для каждого образца ВПО
	Количество выявленных попыток внедрения ВПО за период Компьютерной атаки	О	-	Число	-
Неуспешные попытки авторизации	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период Компьютерной атаки
	IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
	Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
	URI-адрес вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
	Количество уникальных (по связке источник вредоносной активности + учетная запись) неуспешных попыток авторизации за период Компьютерной атаки	О	-	Число	-
Выявление фишинговой рассылки или	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей.

ресурса					Указываются все выявленные источники вредоносной активности за период Компьютерной атаки
	IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
	Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
	URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов или файл	
	e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов или файл	
	Дополнительная информация о технике реализации атак	Н	-	Текстовое поле	-
Попытки социальной инженерии	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период Компьютерной атаки
	IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
	Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
	URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов или файл	
	e-mail-адрес вредоносного		Выявлен e-mail-адрес	Список e-mail-адресов или файл	

	объекта или субъекта		вредоносного объекта		
	Номер мобильного телефона вредоносного субъекта		Выявлен номер мобильного телефона вредоносного субъекта	Список номеров мобильных телефонов или файл	
	Дополнительная информация о технике реализации атак с использованием социальной инженерии	Н	-	Текстовое поле	-