Коммерческий банк
Гарант-Инвест

РЕКОМЕНДАЦИИ КЛИЕНТАМ О НЕОБХОДИМЫХ ДЕЙСТВИЯХ В ПЕРИОД ПОВЫШЕННОГО УРОВНЯ УГРОЗЫ ПРОВЕДЕНИЯ КОМПЬЮТЕРНЫХ АТАК

г. Москва, 2022 г.

Уважаемые клиенты

Для минимизации возможного ущерба в период повышенного уровня угроз проведения компьютерных атак и мошеннических операций, рекомендуем Вам уделить особое внимание обеспечению безопасной работы в системе Банк-Клиент (Частный клиент для физических лиц) с использованием персональных компьютеров, планшетов или телефонов.

Компьютер и настройки интернет-банка

- Рекомендуем использовать для работы в системе Банк-Клиент (Частный клиент) защищенный паролем персональный компьютер с установленными антивирусным программным обеспечением и обновлениями безопасности операционной системы и используемого на компьютере программного обеспечения.
- При входе в Банк-Клиент (Частный Клиент) с помощью браузера, в правом нижнем углу или в адресной строке вашего браузера всегда должен отображаться значок защищённого SSL-соединения, а по двойному щелчку на него — информация о том, что сертификат используется для домена gibank.ru.
- Убедитесь, что в настройках Банк-Клиент (Частный клиент) указаны ваши актуальные данные, в том числе номер телефона и адрес вашей электронной почты.
- Всегда корректно завершайте работу в Банк-Клиенте (Частном клиенте) через кнопку «Выйти».

Обеспечение конфиденциальности ваших учётных данных

- Никому не сообщайте ваши данные для входа в интернет-банк (логин, пароль, одноразовые пароли из СМС), в том числе родственникам, коллегам или тем, кто представляется сотрудниками банка.
- Настройте блокировку экрана мобильного телефона и скрытие показа содержимого SMS-сообщений на заблокированном экране телефона. Установите пароль для разблокирования мобильного телефона или планшета.
- Никогда не устанавливайте стороннее программное обеспечение для удалённого администрирования (например TeamViewer, AmmyyAdmin и т.п.), в том числе по просьбе тех, кто представляется сотрудниками банка или сотрудником силовых ведомств.
- Всегда используйте сложные пароли, состоящие из букв, цифр и специальных символов, которые вы сможете запомнить, нигде не записывая.
- Помните, что Банк никогда не рассылает электронных писем, СМС или других сообщений с просьбой уточнить данные платежей. Будьте бдительны и не отвечайте на подобные запросы.

Одноразовые пароли и СМС-сервисы

- Для дополнительной защиты, при входе в систему Частный клиент, помимо указания вашего логина и пароля, необходимо ввести дополнительный одноразовый пароль, присылаемый на ваш телефон по СМС. Телефоном, на который вы будете получать по СМС одноразовые пароли, должны пользоваться только вы. Убедитесь, что доступа к нему больше ни у кого нет.
- Помните, что одноразовый пароль по СМС можете использовать только вы и только для входа в интернет-банк или подтверждения платежа. Ни для чего другого он не используется, и никто не может запрашивать его у вас.

- Всегда проверяйте параметры операции (тип, сумма, получатель) перед вводом кода подтверждения операции из СМС.

Уважаемые клиенты!

- Никогда и никому не передавайте данные для входа в систему;
- Никогда и никому не показывайте одноразовые пароли из СМС;
- Всегда используйте сложные пароли;
- Всегда проверяйте правильность суммы и получателя;
- Всегда заходите в систему Банк-Клиент (Частный клиент) только с выделенного персонального компьютера или со своего личного персонального устройства (планшета или телефона);
- При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам;
- Вход в систему с чужого компьютера, как и с компьютеров в интернет-кафе, не является безопасным;
- В целях снижения возможных рисков рекомендует вам совершать операции безналичной оплаты товаров и услуг в сети Интернет только с использованием протокола безопасности 3D-Secure (подтверждение операций с использованием одноразового кода), что позволит обеспечить максимальную сохранность реквизитов банковской карты и недопущение распространения данных карты в преступных целях.
- При подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), полностью воздержаться от использования систем дистанционного банковского обслуживания и проведения любых платежей до исправления ситуации;

Более подробные рекомендации по безопасной работе с системами дистанционного банковского обслуживания (Банк-Клиент и Частный клиент) и использованию банковских карт, Вы можете найти на нашем сайте по ссылкам https://www.gibank.ru/upload/files/pam_ib.doc и https://www.gibank.ru/upload/files/tarif/pam_use_cards_inet.docx соответственно.

Если вы потеряли ваш телефон или токен, которые используете для переводов в системе Банк-Клиент, или обнаружили в Банк-Клиенте (Частном клиенте) операции, которые не совершали, или подозреваете, что ваши данные для входа (имя пользователя и пароль) стали известны третьим лицам, пожалуйста, незамедлительно обратитесь в банк по телефону +7 (495) 650-90-03.