Правила финансовой безопасности

Уважаемые клиенты,

АО «ПЕРВОУРАЛЬСКБАНК» (далее -Банк) заботится о своих клиентах и предлагает технологичный и надёжный интернет-банк, современное мобильное приложение, широкий выбор каналов связи с сотрудниками Банка. Для Вашей безопасности и обеспечения сохранности Ваших средств используются современные технологии, которые соответствуют стандартам, принятым в мировой практике.

Однако очень многое зависит от Ваших действий и Вашей финансовой грамотности:

1. Обратите, пожалуйста, внимание на несколько важных правил работы с интернет-банком и мобильным приложением во избежание несанкционированного доступа к защищаемой информации. Соблюдение этих правил поможет сохранить Ваши деньги в безопасности:

Запоминайте Ваши логины и пароли для входа в ДБО и нигде не записывайте их. Если пароль стал доступен кому-то ещё, немедленно измените его. Не используйте в качестве паролей номера телефонов, даты рождения, а также последовательность символов, расположенных подряд на клавиатуре.

Не передавайте средства генерации (получения) одноразовых паролей другим пользователям (в том числе ИТ-специалистам) даже для проверки работы Системы или настроек взаимодействия с Банком.

Внимательно читайте тексты СМС-сообщений с кодами подтверждений, проверяйте реквизиты операции.

Подробнее ознакомиться с Памятками по безопасности обслуживания по ДБО можно на нашем сайте:

Для физических лиц

Для юридических лиц и ИПП

2. В целях предотвращения возможных мошеннических операций обращаем Ваше внимание: для Вашего удобства Банк использует широкий набор каналов коммуникации с клиентами: Skype, Viber, WhatsApp и Telegram, но никогда не запрашивает у Клиентов подтверждений финансовых операций, паролей, персональных данных и информации по счетам и вкладам посредством данных каналов!

Не переходите на сайт банка по сомнительным ссылкам. Просим Вас пользоваться только официальными ресурсами Банка: вход в Систему осуществляется ТОЛЬКО через корпоративный сайт Банка https://www.pervbank.ru/ https://dbo.pervbank.ru/ibank2/ https://dbo.pervbank.ru/web_banking/ и официальные мобильные приложения Банка PB.bank и PB.money.

Не переходите по ссылкам на незнакомые ресурсы, не устанавливайте программы для удалённого доступа и управления компьютерами (TeamViewer, AnyDesk, RMS, RDP, Radmin, Ammyy Admin, AeroAdmin): мошенники могут заразить ваш компьютер или

телефон вирусом, получить удалённый доступ к системе ДБО, Вашим личным данным и финансам.

При получении электронных писем от банка обращайте внимание на отправителя, наличие цифровой подписи.

3. Для минимизации риска телефонного мошенничества обращаем Ваше внимание, что сотрудники Банка:

- не осуществляют звонки с просьбой предоставления персональных данных, информации по вашим счетам и вкладам, одноразовых паролей из СМС для подтверждения финансовых операций;
- не просят коды из СМС для отмены совершённых «мошеннических операций»;
- не предлагают для сохранности перевести деньги на специальные счета или установить специальные программы для обеспечения удалённого доступа и управления компьютерами (TeamViewer, AnyDesk, RMS, RDP, Radmin, Ammyy Admin, AeroAdmin).

В случае поступления вам подобного звонка просим оперативно связаться с колл-центром Банка по телефону **+7 804 333 94 97.**

При поступлении с неизвестных номеров звонков от имени «банковских работников», СМС или иных сообщений от якобы «ПЕРВОУРАЛЬСКБАНКА» (например, «Заблокирована сумма оплаты», «Есть проблемы с проведением операции» и т.п.):

- ни в коем случае не перезванивайте на указанные в сообщениях номера,
- не сообщайте по телефону персональные сведения: серия и номер паспорта, адрес регистрации и пр.

В такой ситуации следует считать, что звонки или сообщения приходят от мошенников. Вам нужно прекратить контакт и самостоятельно обратиться в банк по телефонам, указанным на сайте банка или в оригинальных банковских документах.

4. Настоятельно рекомендуем использовать антивирусное ПО, которое поможет уменьшить вероятность попадания в устройство вредоносных программ.

Куда обращаться в случае мошенничества

Если вы получили подозрительное письмо, звонок или обнаружили операцию, которую вы не совершали, а также в случае, когда доступ к вашему компьютеру, смартфону или USB-токену могли получить посторонние лица, незамедлительно обратитесь к персональному менеджеру или в службу поддержки по телефону **+7 804 333 94 97.**

Расскажите подробно, что произошло: номера телефонов, адреса сайтов, скриншоты писем и сообщений помогут нам быстрее разобраться с мошенниками.