

## Памятка по обеспечению безопасности при работе с системой «Телебанк»/«Телеинфо»

Сервис «Телебанк»/«Телеинфо» обеспечивает вас надежной системой безопасности для управления счетами и банковскими картами. Однако для того, чтобы ваше взаимодействие с банком по дистанционным каналам было полностью безопасно, **пожалуйста, выполняйте следующие рекомендации:**

- При входе в систему не вводите переменный код на экране, предназначенном для ввода логина и пароля. Система запрашивает переменный код только на следующем экране и только после правильного ввода логина и пароля.
- В случае неправильного ввода переменного кода при входе в систему не вводите код со следующим порядковым номером. Если первая попытка входа не удалась, при каждой повторной попытке система запрашивает переменный код с тем же номером, что и при первой попытке.
- При входе в систему не вводите номер вашей банковской карты или ее CVC/CVV-код. Система никогда не запрашивает эти данные.
- Если при работе в системе вы используете только переменные коды:
  - убедитесь в том, что соединение установлено именно с сайтом системы по адресу <https://www.telebank.ru>;
  - убедитесь в том, что соединение установлено в безопасном режиме, т.е. адресная строка в браузере начинается с <https://>.
- Если при работе в системе вы используете программу «Inter-PRO Client» и электронные сертификаты:
  - установите в настройках программы «Inter-PRO Client» пароль на доступ к секретному ключу;
  - убедитесь, что соединение установлено именно с сайтом системы по адресу <http://telebank.vtb24.ru>;
  - убедитесь, что на вашем компьютере запущена программа «Inter-PRO Client» (в этом случае при входе в систему на экран выводится сообщение программы «Inter-PRO Client» об обнаружении сертификата).
- Никогда не сообщайте в ответ на телефонные звонки, SMS- или e-mail сообщения, поступившие, якобы, от работников банка, ваш пароль доступа в систему и переменные коды, а также номер вашей банковской карты, ее CVC/CVV- и ПИН-коды. Не выполняйте никаких рекомендаций, особенно связанных с вводом каких-либо данных на любых страницах, открытых вашим браузером. Работники банка никогда не обращаются к клиентам по телефону с предложениями попытаться войти в систему еще раз или ввести еще один переменный код, не пытаются узнать у клиентов пароли, переменные коды или реквизиты банковских карт.
- После окончания работы в системе используйте кнопку «Выход», после чего закройте окно и закройте программу «Inter-PRO Client», если она была запущена.

- Контролируйте посещения системы. Проверьте дату вашего последнего посещения и IP-адрес в разделе «Безопасность» системы. Настройте SMS- или e-mail оповещения в разделе «Система оповещений», и при каждом входе в систему вы будете получать специальное уведомление.
- Если при входе в систему вы заметите какие-либо несоответствия стандартным запросам или вам позвонят от имени банка с предложением попытаться войти в систему еще раз, ввести или сообщить переменный код, не вводите и не сообщайте никаких данных. Незамедлительно обратитесь в круглосуточную Службу поддержки по телефонам:  
**(495) 771-78-24** или **(495) 777-24-24** (для звонков из Москвы);  
**8 800 100-24-24** (для бесплатных звонков из регионов России).  
Далее переведите телефон в режим тонального набора (нажав клавишу **\***) и нажмите цифру **3**.
- Используйте лицензионное программное обеспечение (операционная система, приложения), полученное из проверенных и надежных источников, своевременно устанавливайте все обновления программного обеспечения, повышающие безопасность.
- Установите лицензионную антивирусную программу, своевременно обновляйте антивирусную программу и антивирусные базы данных, проводите периодическое сканирование своего компьютера.
- Установите и настройте персональный брандмауэр (firewall) на вашем компьютере. Это позволит предотвратить несанкционированный доступ по сети к вашему компьютеру.
- Не используйте функцию автозаполнения в установках вашего браузера. Это поможет не сохранять данные (пароль пользователя, имя пользователя и др.) в памяти браузера, что, в свою очередь, предотвратит использование данных сторонними лицами.
- Включите систему фильтрации ложных web-узлов (антифишинг) в своем браузере; если браузер ее не имеет — обновите браузер.
- Не открывайте электронные почтовые сообщения и сообщения систем мгновенного обмена сообщениями (например, ICQ), поступающие от неизвестных отправителей, не открывайте файлы, вложенные в эти сообщения, сразу же удаляйте эти сообщения.