При работе с Интернет-банком следуйте следующим рекомендациям для повышения безопасности:

Установите, обновите и используйте антивирус на вашем компьютере

Вирусные программы могут запоминать и отсылать всю информацию злоумышленникам. Если у вас есть подозрение, что ваши логин и пароль украдены, как можно быстрее смените ваши логин и пароль в Интернет-банке или через телефонный центр МТС Банка. Используйте современное антивирусное программное обеспечение и следите за его регулярным обновлением. Регулярно выполняйте антивирусную проверку на своем компьютере для своевременного обнаружения вредоносных программ.

Проверяйте адрес интернет-банка, он должен быть https://personalbank.ru/

Интернет-банк МТС Банка всегда доступен только по адресу https://personalbank.ru/. Вас могут пытаться обмануть, предлагая оставить ваши пароль и логин на поддельном сайте (например, http:// bankpersonal.net.comm.org). Если вы обнаружите такой сайт, обязательно сообщите об этом через телефонный центр МТС Банка! Проверяйте, используется ли защищенное соединение — https://personalbank.ru/.

Проверяйте, действительно ли соединение происходит в защищенном режиме SSL — в адресной строке вашего веб-браузера должен быть изображен значок закрытого замка (справа или слева, в зависимости от браузера).

Для входа в Интернет-банк нужен только логин и пароль

В Интернет-банке не должно быть никаких дополнительных полей для ввода такой информации как номер вашей карты, проверочный код или номер телефона!

Никому не говорите ваш пароль и одноразовый пароль

Сотрудники МТС Банка никогда не просят сообщить или ввести куда-либо конфиденциальную информацию (ваши персональные данные, номер карты, пароль или одноразовый пароль по SMS).Одноразовый пароль по SMS действует только для подтверждения платежа. Отменить операцию в Интернет-банке невозможно. Никто никогда не попросит у вас ввести одноразовый пароль для отмены операции.

Внимательно проверяйте параметры операции в SMS-сообщении, содержащем одноразовый пароль

Информация в нем должна совпадать с вашей операцией в Интернет-банке, которую вы хотите подтвердить. Если эта информация не совпадает, не вводите одноразовый пароль и сообщите об этом через телефонный центр МТС Банка!

Для звонков в телефонный центр используйте номер телефона, указанный на вашей карте

Часто мошенники на поддельных сайтах указывают неправильные номера, которые могут быть недоступны или по ним ответит оператор, который будет пытаться вас обмануть. В случае подозрения на мошенничество звоните в телефонный центр МТС Банка только по номеру, указанному на вашей карте!

Используйте только доверенные приложения

Не устанавливайте на компьютер приложения, полученные из неизвестных Вам источников. Помните, что Банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS/MMS/E-mail-сообщения.

Контролируйте состояние своих счетов

Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте работникам Банка обо всех подозрительных или несанкционированных операциях.

Обеспечивайте защиту от фишинга

В целях эффективного противодействия методам социальной инженерии рекомендуем Вам:

- не открывайте присланные электронные письма из недоверенных источников (или от неизвестных адресатов),
- не открывайте ссылки на интернет-страницы, указанные в письмах неизвестных Вам адресатов,
- не скачивайте и не запускайте подозрительные файлы или приложения из недоверенных источников сети Интернет или электронной почты.

Используйте иные защитные меры и механизмы

— Используйте лицензионную операционную систему.
— Своевременно устанавливайте обновления операционной системы своего компьютера.
— По возможности используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты Вашего компьютера — персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «спам»-рассылок и пр.
— Корректно завершайте работу с системой путем выбора соответствующего пункта меню.
— Не используйте на компьютере программы для удаленного доступа (TeamViewer, Mikogo, RAdmin и др.)