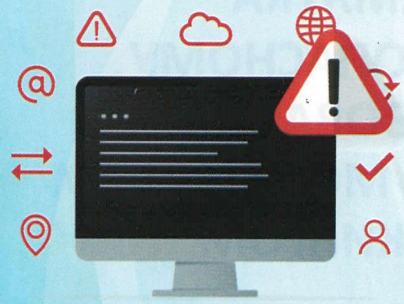
Уважаемые клиенты!

Пожалуйста, ознакомьтесь с несколькими важными правилами работы с банковскими картами, мобильным приложением и интернет-банкингом. Соблюдение этих правил поможет вам в будущем сохранить ваши средства в безопасности и сохранности.

Правила личной кибер-безопасности:

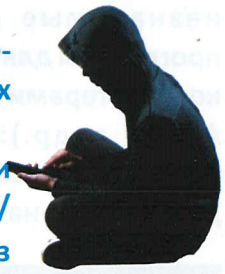


- Не переходите по подозрительным ссылкам: мошенники могут заразить ваш компьютер или телефон вирусом и завладеть вашими данными

- Используйте только официальные приложения организации в AppStore, GooglePlay
- Сообщите организации о смене номера мобильного телефона, т.к. есть риск, что ваши данные попадут новому владельцу
- Проверяйте реквизиты переводов и платежей, которые приходят в СМС от компании
- Запишите номер организации 1122 в адресную книгу своего телефона. Если звонок будет с другого номера, то на экране телефона он отобразится как комбинация цифр, которая отличается от 1122

Для минимизации риска телефонного мошенничества обращаем ваше внимание, что сотрудники компании:

-НЕ осуществляют звонки с просьбой предоставления персональных данных, номеров карт, одноразовых паролей из СМС для подтверждения финансовых операций



-НЕ просят коды из СМС для отмены совершённых «мошеннических операций»

-НЕ просят у вас коды безопасности с обратной стороны карты (CVV/CVC), логин от IMONLINE, коды из СМС, номер банковской карты

Запомните!

Не совершайте никаких операций по инструкциям незнакомого звонящего. Проверьте, не было ли сомнительных операций во время разговора.

При малейших подозрениях сразу заканчивайте разговор и позвоните в организацию по номеру 1122 и сообщите о случившемся. При поступлении звонков с неизвестных номеров от имени «банковских работников», СМС или иных сообщений от якобы «Imon» (например, «Ваша карта заблокирована», «Есть проблемы с проведением операции», «Проблема с мобильным банкингом» и т.п.) ни в коем случае не перезванивайте на указанные в сообщениях номера и не сообщайте свои персональные данные.

Правила безопасности при использовании банковской карты и банкоматов

- Не сообщайте никому свои конфиденциальные данные: пароли, ПИН- и CVV-коды карты, ФИО на карте, срок действия карты и коды из СМС. Даже сотрудникам компании.

- Не храните фото карты на смартфоне и ни под каким-либо предлогом не отправляйте никому фото карты. Мошенники часто просят отправлять фото карты с двух сторон.
- Не держите ПИН - конверт и карту в одном месте.
- При утере банковской карты немедленно сообщите организации об утере и заблокируйте карту через приложение IMONLINE.
- Осмотрите банкомат перед использованием и убедитесь, что на нём нет подозрительных устройств
- Прикрывайте клавиатуру рукой, когда вводите ПИН-код
- Не принимайте помощь от незнакомцев, находясь у банкомата, и не совершайте операции под диктовку