ПАМЯТКА
по профилактике мошенничества с банковскими картами.

Банковская карта - это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

Вам приходит сообщение о том, что Ваша банковская карта заблокирована. Предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда Вы звоните по указанному телефону, то Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации. Злоумышленникам нужен лишь номер Вашей карты и ПИН-код, как только Вы их сообщите, деньги будут сняты с Вашего счета.

Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, Вам ответят, что никаких сбоев на сервере не происходило, а Ваша карта продолжает обслуживаться банком.

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной.

Совершая операции пластиковой картой, следите, чтобы рядом не было посторонних людей. Набирая ПИН-код, прикрывайте клавиатуру рукой.

Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нем телефону.

Если банкомат долгое время находится в режиме ожидания или самопроизвольно перезагружается - откажитесь, от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

Хищение с карт, подключенных к опции бесконтактных платежей. Для проведения оплаты бесконтактной картой рекомендуется просто приложить её к терминалу. Ввод ПИН-кода не требуется, если сумма не превышает 1 000 рублей. При этом количество расходных транзакций не ограничено.

Как обезопасить себя от мошенников:

1. Установить на телефон (компьютер) современное лицензированное антивирусное программное обеспечение.
2. Не устанавливаете и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников:

скачанные с неизвестных сайтов, присланные по электронной почте (подозрительные файлы лучше сразу удалять).

3. Используйте пароли не связанные с Вашими персональными данными.

4. Не сообщать данные карты, пароли и другую персональную информцию.

5. Поставьте лимит на сумму списаний или перевода в личном кабинете банка.

6. По всем возникающим вопросам обращаться в банк, выдавший карту.

7. Не выполнять никаких срочных запросов к действию, в том числе по установке каких бы то ни было приложений.

8. Не перезванивать по номерам и не переходить ни по каким ссылкам, которые приходят на e-mail или по SMS.

9. Обращать на все сообщения от банка (например, если они содержат грамматические ошибки.

10. При потере карты немедленно ее заблокируйте и обратитесь в ближайший офис банка.

Отдел по антитеррористической работе и
взаимодействия с правоохранительными
органами АМС МО Пригородный район