**ВНИМАНИЕ!**

**КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ!**

На территории Республики Башкортостан, в частности в г. Уфе и Уфимском районе участились случаи совершения хищений денежных средств с банковских карт.

**Распространенные случаи совершения хищений:**

**1)** При использовании банковской карты для оплаты товара в продовольственном или ином магазине, а также в кафе преступником может являться кассир или обслуживающий персонал, которому Вы передаете свою карту. В данном случае злоумышленник может переписать реквизиты карты, требуемые для осуществления перевода денежных средств с карты на карту или для оплаты какого-либо продукта в сети Интернет, после чего вернет Вам карту и через какое-то время, что бы снять с себя подозрения, начнет использовать полученные реквизиты в корыстных целях.

**Необходимо**: пресекать попытки задержки карты на кассе или какой-либо иной фиксации реквизитов карты, а также не передавать карту третьим лицам, а производить оплату при личном присутствии.

**2)** При оплате товара в сети Интернет, когда Вы ввели все данные с карты на «Фишинговом» сайте (*сайт-подделка, внешне не отличаемый по оформлению, но имеющий сомнения в адресной строке, например вместо www.media-markt.ru будет выглядеть как www.media-matkr.ru*). В таком случае на сайте Вы вводите свои реквизиты, доступ к которым в последующем получают третьи лица – разработчики данного «Фишингового» сайта.

**Необходимо:** Убедиться в правильности написания сайта в адресной строке. При наличии сомнений, запросить в поисковой системе информацию о случаях мошенничества с данного сайта, а также проверить сайт по отзывам.

**3)** В случаях, когда Ваша банковская карта привязана к социальным сетям, Ваши страницы также могут быть подвержены хакерским атакам для получения доступа к реквизитам Ваших карт.

**Необходимо:** Использовать пароль с высокой степенью защиты, с применением заглавных и строчных букв, а также символов и цифр. Или отключить банковскую карту от страницы в сети Интернет.

**4)** Имеют место случаи, когда граждане, пользуясь изначально одним абонентским номером, привязанным к банковской карте, начинают использовать другой, а старый не отключают. После какого-то времени данный абонентский номер вновь выставляется на продажу сотовой компанией, и новый владелец номера начинает получать сведения о зачислении денежных средств, а также получает доступ к их использованию.

**Необходимо:** При смене сим-карты уведомлять об этом банк, при этом желательно делать это, находясь в офисе банка при личном контакте, а не по телефону «Горячей линии».

**5)** В настоящее время широкое распространение получил способ хищения денежных средств с банковской карты посредствам «заражения» мобильного телефона вредоносным программным обеспечением (вирусом). Данному способу подвержены в основном владельцы смартфонов на базе операционной системы «Android», являющиеся клиентами ПАО «Сбербанк» и пользующиеся услугой «Мобильный банк». В таком случае вирус делает запросы о балансе на карте и осуществляет перевод денежных средств в другие регионы на подставные карты клиентов банка, а также стирает направляемые им по средствам СМС- сообщений запросы на номер «900» и ответы с данного номера.

**Необходимо:** Использовать только официальное приложение «Сбербанк Онлайн». Установить в мобильный телефон антивирусные приложения. В случаях, если Вы используете услугу «Мобильный банк» для получения СМС-сообщений о движении денежных средств (в качестве СМС-информатора), Вы имеете право отключить функции перевода денег на другие карты или абонентские номера, с этой просьбой Вы можете обратиться в любое отделение банка.

**6**) В социальной сети «Вконтакте», «Одноклассники» со «страницы» друзей приходят сообщения с просьбой одолжить денежные средства, причем просят перевести денежные средства на банковскую карту того или иного банка, после чего Вы отправляете со своей банковской карты (счета) денежные средства, на карту указанную в сообщении, где в последствии «страница» «Вконтакте» блокируется, а «друг», который Вас просил о просьбе перевода денежных средств оказывается «взломанным».

**Необходимо:** при получении данного рода сообщений, осуществлять телефонный звонок своим друзьям, от которых приходят данные сообщения, ни в коем случае не отправлять денежные средства.

7) За частую граждане, с целью получения денежных средств (кредита), оставляют заявки на получение кредита в сети интернет, которым в последствии от «банков» приходят сообщения с текстом «Вам одобрен кредит, но для получения кредита Вам необходимо оплатить страховой взнос либо налог», после оплаты «страховых взносов» сайт с которого отправляли сообщения и абонентские номера блокируются.

**Необходимо:** не оставлять заявки на получение кредита в сети интернет, так как «банки» работают непосредственно с лицом при оформлении кредита (рассрочки), ни в коем случае не осуществлять переводы денежных средств на банковские карты (счета).

**При совершении в отношении Вас преступления сообщите в ближайший отдел полиции или по телефону «02».**

**ОМВД России по Уфимскому району**