Информация для граждан по предупреждению
хищений с банковских карт:

1. При поступлении звонка, независимо от того кем представляется звонивший (сотрудником банка, или из службы безопасности Центрального банка и др.) и по какому поводу (попытка списания денежных средств, карта заблокирована и др.), ни в коем случае **нельзя** сообщать следующую информацию: **срок действия карты, код безопасности** – три цифры на обороте карты. При обращении мошенник может назвать **имя и отчество** человека, которому звонит и **четыре последних цифры** банковской карты (вариант: первые шесть; первые шесть и четыре последних и др.). Разговор в данном случае необходимо прекратить, при сомнении, самостоятельно обратится на горячую линию банка по телефону, указанному на банковской карте.
2. При поступлении sms – сообщений с номера 900, в случае не проводимой гражданином финансовой операции, незамедлительно рекомендуется обратиться **только** на горячую линию банка по телефону, указанному на банковской карте, или в ближайшее отделение банка. При поступлении sms – сообщений (типа «Ваша карта заблокирована», «осуществлена попытка списания», «на счете зарезервированы средства на покупку ... в сумме ... и др.») с иных номеров по номерам указанным в sms – сообщениях – **не звонить; не перезванивать, на номер с которого поступило sms – сообщение.**
3. В случаях продажи товара гражданином для перевода денежных средств покупателю достаточно знать **только номер карты или номер телефона,** к которому подключена услуга «Мобильный банк». Покупателю этих данных **достаточно.** Никаких дополнительных действий от продавца не требуется. Во всех других случаях – **необходимо прекратить разговор.** Ни при каких условиях не сообщать код безопасности (CVC код – три цифры на обороте карты) и срок действия карты.

Также необходимо помнить, что если даже **на счете банковской карты нет денежных средств,** а на других счетах, открытых в этом банке они есть, то при завладении данными от личного кабинета гражданина, мошенник может дистанционно вывести денежные средства с других счетов, а в некоторых случаях оформить небольшой кредит на гражданина и также его вывести на свои счета. Поэтому никому не нужно сообщать кода, поступающие с номера 900 для завершения финансовой операции. В каждом sms – сообщении, поступившем с номера 900 содержится информация о неразглашении кода третьим лицам. В противном случае банк считает, что финансовая операция совершена самим владельцем банковской карты, денежные средства не возвращает.
4. При звонке неизвестного о якобы ошибочном переводе – не спешить выполнять просьбу звонящего о возврате денежных средств. Гражданину необходимо самому обратится в банк, удостовериться, что такой перевод действительно был, и денежные средства поступили на счет. Не стоит спешить и поддаваться эмоциям.

5. При звонке неизвестного от имени родственника якобы попавшем в полицию (за ДТП, за драку, за наркотики и др.) гражданину также не стоит поддаваться эмоциям, на что обычно давят мошенники, а перезвонить родственнику от чего имени представлялись мошенники. В случае просьбы о переводе (передаче третьим лицам) денежных средств для решения возникших проблем, **немедленно прекратить разговор,** сообщить в полицию.

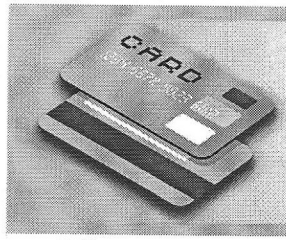
6. При приобретении товара в сети интернет рекомендуется гражданам приобретать его в торговых фирмах, зарекомендовавших себя в течение длительного времени. При приобретении товара по объявлениям размещенных на торговых площадках («Авито», «Юла» др.) есть риск получить товар не соответствующий заказанному, или, после внесения предоплаты, не получить его вообще.

7. При получении сообщения в социальной сети от друга с просьбой одолжить ему денежную сумму - рекомендуется гражданину **перезвонить ему.** Не стесняться уточнить еще раз озвученную просьбу в сети, т.к. мошенник может взломать страницу друга и администрировать ее от имени друга.

Людям пожилого возраста, мошенники могут позвонить: под предлогом выплаты компенсации за ранее приобретенные ими некачественные биологические активные добавки (БАД); компенсации за средства, вложенные в разорившиеся компании («МММ») др. В этом случае мошенники просят граждан оплатить пошлины, страховки, судебные издержки, доставку денежных средств до дома и др. В данном случае разговор с неизвестными нужно прервать или сказать, чтобы позвонили позже, когда придут родственники, необходимо также уведомлять родственников, соседей пожилых граждан о возможных видах мошенничества.

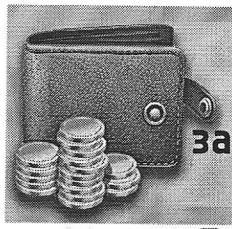
УМВД России по Смоленской области
предупреждает
Не дайте мошенникам шанса!

«Безопасный банковский счёт»
Неизвестный представляется сотрудником банка, обращается к Вам по имени и отчеству, сообщает о несанкционированном списании Ваших средств и предлагает открыть «безопасный» счёт



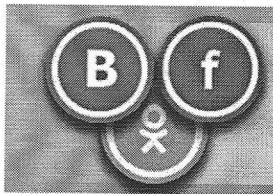
«Ваша карта заблокирована»
SMS-сообщение о блокировке банковской карты, для разблокировки от Вас требуют сообщить ПИН-код, CVV-код и срок действия карты

«Купля-продажа через Интернет»
Продавец просит у Вас предоплату за товар, а при получении денег перестаёт выходить на связь



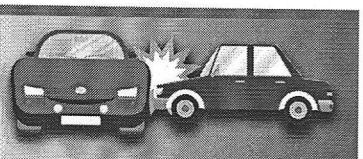
«Компенсация»
Неизвестный сообщает, что Вам положена компенсация за ранее приобретённые БАДы или лекарственные препараты, а для её получения необходимо оплатить пошлину

«Ошибочный перевод»
Неизвестный просит вернуть деньги за якобы ошибочный перевод средств на счёт Вашего телефона или банковской карты



«Помощь другу»
Друг из социальных сетей присылает Вам сообщение с просьбой перевести ему денежные средства

«Родственник в беде»
Неизвестный сообщает, что Ваш родственник стал виновником ДТП или совершил преступление, требует от Вас денежные средства для «решения» проблемы



Будьте бдительны. При совершении в отношении Вас мошеннических действий незамедлительно обращайтесь в полицию!

02 **102**