

ВНИМАНИЕ!

БЕРЕГИТЕ СВОИ ДЕНЬГИ!

УЧАСТИЛИСЬ СЛУЧАИ ХИЩЕНИЯ ДЕНЕГ С БАНКОВСКИХ КАРТ-СЧЕТОВ!



Если вам пришло сообщение в мессенджере, социальных сетях или по электронной почте...



... в котором говорится, что банковская карта заблокирована, и предлагается разблокировать ее, пройдя по ссылке...



... ни в коем случае не переходите по ссылке!
Незамедлительно обращайтесь в службу безопасности банка!

Если вы получили сообщение о блокировке банковской карты:



- не переходите по прикрепленной ссылке, никуда не пересылайте свои данные;



- проверьте баланс своей карты в банкомате, инфокиоске, мобильном или интернет-банкинге;



- обратитесь в службу безопасности банка.

**Главное управление по противодействию киберпреступности
криминальной милиции МВД Республики Беларусь**

ВНИМАНИЕ! МОШЕННИЧЕСТВО!

1 

поступает звонок
с **неизвестного**
номера

2 

звонящий
представляется
вашим
родственником

3 

он говорит,
что **сбил человека**
или из-за него
человек
попал в ДТП

4 

он просит **денег**,
как **компенсацию**
вреда или
чтобы **«замять»** дело

5 

затем звонит
«милиционер»/
«следователь»
и подтверждает
легенду

6 

за деньгами
приезжает
курьер

Мама, папа, я
в беде!

Нужны деньги!
Срочно!

Что делать?

1. немедленно положить трубку
2. самому перезвонить родственнику
3. не передавать курьерам никаких денег
4. сообщить в милицию

не дай себя обмануть!




МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единый
номер **102**


Как не стать жертвой киберпреступника.


ЗАЩИТА БАНКОВСКОЙ КАРТЫ

Наиболее распространенные методы работы злоумышленников

 выманивание реквизитов банковских платежных карт с использованием взломанных аккаунтов знакомых в социальных сетях



 **ЛЖЕПОКУПАТЕЛЬ** - под видом покупателя злоумышленник связывается с продавцом, предлагает внести залог перед покупкой товара, а для получения денежного перевода предоставляет ему ссылку на мошеннический сайт, визуально похожий на официальный сайт банка

 **ВИШИНГ** - представляясь по телефону сотрудником банка, злоумышленник пытается узнать у держателя карты конфиденциальную информацию (ее реквизиты, а также номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды)



НЕ СООБЩАЙТЕ НИКОМУ

- информацию, размещенную на вашей банковской платежной карте (на обеих сторонах): номер, дату, код
- цифровые или буквенные коды
- паспортные данные



ЕСЛИ ВАМ ПОСТУПИЛ СОМНИТЕЛЬНЫЙ ЗВОНОК

- немедленно завершите разговор
- обратитесь в контакт-центр банка, выпустившего карту
- следуйте рекомендациям сотрудника банка



Для защиты денежных средств клиентов у банка есть вся необходимая информация



Работники банка по телефону не должны спрашивать ни реквизиты карты, ни паспортные данные



Не давайте никому свой мобильный телефон и предупредите об этом ваших близких, особенно детей и лиц пожилого возраста

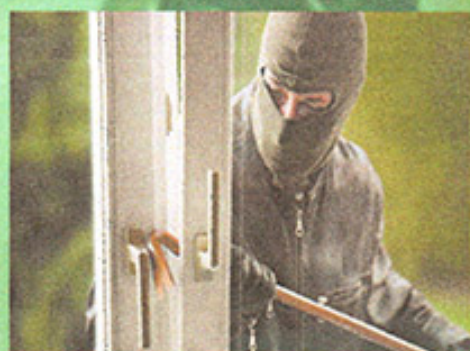
А ВЫ ЗАЩИТИЛИ СВОЕ ЖИЛИЩЕ?

В целях предупреждения преступных посягательств, милиция настоятельно рекомендует:



- не приглашать в гости незнакомых граждан;
- не оставлять форточки, входные и балконные двери открытыми;
- уезжая в отпуск или командировку, попросите соседей присматривать за вашей квартирой, регулярно вынимать корреспонденцию из почтового ящика;
- установите металлическую дверь с надежными замками;
- установите на окна металлические решетки или ударопрочную пленку.

Также рекомендуется оборудовать квартиру средствами охранной сигнализации, так как это самое надежное средство предотвращения возможных посягательств на ваше имущество со стороны преступников. Статистика говорит сама за себя: попытки злоумышленников проникнуть в квартиру, оборудованную охранной сигнализацией, терпят фиаско.



Соблюдение вышеуказанных рекомендаций поможет обезопасить вашу квартиру от кражи