## Внимание!Вишинг!Активизировались кибермошенники!

Представляясь сотрудниками контакт-центра или службы безопасности белорусских банков, злоумышленники звонят с подменного номера телефона клиентам этих учреждений.

Последним они сообщают о совершенном в отношении них мошенничестве и под предлогом блокировки счета просят сообщить реквизиты платежных карт. После этого, завладев указанной информацией, похищают денежные средства потерпевших.

В этой связи в МВД предупреждают:
— ни под каким предлогом не передавайте и не сообщайте платежные реквизиты, полный номер карточки и срок ее действия, логин и пароль к интернет-банку, иную персональную информацию;
— не вступайте в переговоры с незнакомцем. Положите трубку и самостоятельно обратитесь в банк по номерам, указанным на официальном сайте;
— применяйте все доступные способы защиты, предлагаемые банками (двухфакторная авторизация, смс-оповещение о расходных операциях, лимит снятия денежных средств и др.);
— используйте сложные пароли доступа к учетным записям электронной почты, к системам «интернет-банкинг», социальным сетям и другим интернет-сервисам;
— не открывайте электронные почтовые сообщения, полученные от неизвестных отправителей и не запускайте их содержимое;
— не переходите по неизвестным ссылкам и не посещайте интернет-ресурсы сомнительного содержания;
— при посещении интернет-сайтов обращайте внимание на
веб-адрес интернет-ресурса.
— Помните: просьба незнакомого абонента о предоставлении конфиденциальной информации свидетельствует о том, что разговор ведется с мошенником!

Сотрудники банка ни при каких обстоятельствах не требуют реквизитов банковских карт или иной конфиденциальной информации!

Популярная схема мошенников — напугать жертву. Сценарии простые:
— «с вашей картой происходят мошеннические транзакции»
— «со счета уже списаны деньги и спасти их можно в считанные минуты»
— «от вашего имени направлена заявка на кредит, нужно срочно ее отменить!»
— «на ваш счет ошибочно зачислен перевод, его нужно вернуть»

Важно! Если с картой действительно происходят мошеннические операции, банк сам может ее заблокировать. В любом случае, все подозрительные ситуации лучше разрешать в отделении банка лично либо самостоятельно позвонить в контакт-центр по номерам, указанным на официальном сайте.