## Не сообщайте кому-либо сведения о банковской карточке, паспортные данные и коды доступа.

В Беларуси участились случаи телефонного мошенничества — вишинга. Мошенники звонят клиентам белорусских банков, представляются сотрудниками службы безопасности либо просто сотрудниками банка, под тем или иным предлогом просят предоставить данные о банковской платежной карточке, паспортные данные, коды, приходящие на телефонный номер, логины и пароли от системы дистанционного банковского обслуживания.

Злоумышленники также могут использовать программы-анонимайзеры. В таком случае при входящем звонке клиент банка будет видеть на своем телефоне номер банка, размещенный на официальном сайте. Вместе с тем мошенники могут подменить не телефонный номер целиком, а одну цифру в нем. Таким образом, клиенту сложнее визуально идентифицировать оригинальность номера банка.
Для большей правдоподобности злоумышленники используют
в качестве фона звонка шум работающего колл-центра банка.

Один из основных сценариев обмана выглядит следующим образом: при звонке злоумышленник представляется работником банка, сообщает, что в отношении счета клиента производятся мошеннические действия. По легенде, чтобы предотвратить несанкционированный перевод либо снятие денег в банкомате, клиенту нужно предоставить информацию о банковской платежной карточке либо другие данные.

Еще один сценарий — злоумышленник звонит держателю карточки и говорит о том, что на его имя якобы оформлен кредит. Для его отмены также нужна уточняющая информация.

*Обращаем Ваше внимание, что при звонке клиенту банк всегда знает всю необходимую информацию. Сообщать кому-либо данные о банковской карточке, паспортные данные, коды категорически запрещено. Как только собеседники начинают узнавать подобную информацию, рекомендуем завершить*

*звонок и перезвонить на номер банка, указанный на его официальном сайте.*

Кроме того, акцентируем внимание, что мошенники выманивают деньги через взломанные страницы или страницы-клоны («фейковые страницы») в социальных сетях — якобы от имени друга приходит сообщение с просьбой дать данные банковской карточки для перевода денег. Злоумышленники также могут притворяться покупателями: под маской заинтересованности они обращаются к продавцу и говорят о намерении купить его товар в интернете. Продавцу предоставляют ссылку, перейдя по которой клиент вводит свои реквизиты, и тем самым передает их злоумышленнику. В дальнейшем мошенник использует их для денежных переводов.

Зафиксировано немало случаев, когда злоумышленники просят мобильный телефон под предлогом звонка, а затем устанавливают на него программное обеспечение для несанкционированных денежных переводов. Волна звонков телефонных мошенников продолжается. Отдел по раскрытию преступлений в сфере высоких технологий рекомендует проявить бдительность, никому не передавать конфиденциальную информацию.

**ОРПСВТ КМ УВД Гомельского облисполкома**

# Десять правил безопасности для детей в Интернете*


* Рекомендации Министерства образования Республики Беларусь

© Инфографика БЕЛТА

# БЫТЬ ХАКЕРОМ: не развлечение, а преступление!

## Уголовная ответственность за киберпреступления наступает:

**Статья 212 УК Беларуси** — **с 14 лет**

**Хищение путем использования компьютерной техники** или введения в компьютерную систему ложной информации наказывается вплоть до лишения свободы на срок **до 3 лет**.

Те же действия, совершенные **повторно или группой лиц по предварительному сговору**, наказываются лишением свободы на срок **до 5 лет**.

Если **хищение крупное**, то предусмотрено наказание в виде лишения свободы на срок **до 7 лет**.

За хищение, совершенное **организованной группой или в особо крупном размере**, грозит **до 12 лет** лишения свободы.

**Статья 349 УК Беларуси** — **с 16 лет**

**Несанкционированный доступ к компьютерной информации**, совершенный из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, наказывается вплоть до лишения свободы на срок **до 2 лет**.

За несанкционированный доступ к компьютерной информации, повлекший по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные **тяжкие последствия**, грозит наказание вплоть до лишения свободы на срок **до 7 лет**.

Управление информации и общественных связей МВД Республики Беларусь

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

Источник: Национальный банк Беларуси.