

### Финансовая безопасность

## МОШЕННИЧЕСКИЕ СООБЩЕНИЯ В МЕССЕНДЖЕРАХ И СМС

**В Беларуси в последнее время участились случаи мошенничества с карточками.**

**Напоминаем о простых способах обезопасить свои финансы:**

### 1. Звонят из банка? Перезвоните сами!

Самый «популярный» способ работы мошенников – представиться работником контактного центра или службы безопасности Банка. Не вступайте в переговоры. Положите трубку и самостоятельно обратитесь в Центр клиентской поддержки БПС-Сбербанка по номерам, указанным на официальном сайте: единому номеру **148**, или по телефону **+375 (29/44/25) 5 148 148 (А1, МТС, Life)**.

Важно! Ни в коем случае не перезванивайте на тот номер, с которого вам поступил звонок. Злоумышленники сейчас используют метод IP-телефонии, который позволяет отображать номера, схожие с номерами Банка.

*Иногда, действительно, требуется получение комментариев от держателя карточки по факту совершения операции, которая является сомнительной для Банка. В таком случае Банк направляет на телефонный номер клиента SMS-сообщение с просьбой перезвонить в Центр клиентской поддержки Банка.*

### 2. Что нельзя говорить даже сотруднику Банка

Есть информация, которую должны знать только вы, Банк никогда не просит клиента предоставить:

- логин и пароль к интернет-банку;
  - кодовое слово и код из смс-сообщения;
  - CVC/CVV-коды;
  - полный номер карточки и срок ее действия.
- Важно! Этой информации достаточно для проведения любых финансовых операций без вашего участия, в том числе открытия кредита или получения кредитного лимита по действующей карте.

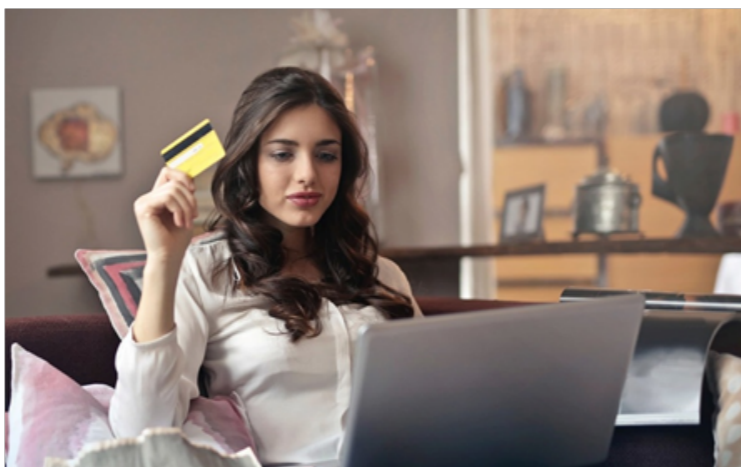
### 3. «С вашей картой большие проблемы!» – Не проглатывайте наживку!

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!»;

*дит, 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 Центр клиентской поддержки по номерам, указанным выше.



### 4. Не переходите по ссылкам в сообщениях!

Еще одна уловка мошенников – представиться потенциальным покупателем товара, объявление о продаже которого было размещено вами в сети интернет (наиболее популярна платформа – kufar.by). По каким-то причинам «покупатель» не может сегодня привезти деньги, но хочет прислать вам залог из другого города по системе дистанционного банковского обслуживания. Для проверки поступления перевода направляет вам ссылку на фишинговый сайт, который очень близок по дизайну на используемый вами интернет-банк. После введения вами в поля фишингового сайта пароля и логина, данные становятся доступны мошеннику.

**Важно!** Не переходите по подозрительным ссылкам. Для веб-версии интернет-банка «Сбербанк Онлайн» используйте только официальный сайт Банка, а для мобильной версии СБОЛ – только мобильное приложение, загруженное из официальных магазинов.

### 5. Подключите услугу «SMS-оповещение».

Это позволит незамедлительно узнать о несанкционированных операциях с использова-

нием вашей карты и оперативно предпринять необходимые действия, чтобы предотвратить хищение.

**6. В случае утери карты** необходимо незамедлительно обратиться в банк для ее блокировки.

**7. Для операций в интернете** заведите отдельную карточку (Visa Virtuo или MasterCard Standard Virtual). Также можно установить лимит на совершение операций в интернете и подключить к карточке технологию «3D Secure».

**8. Совершайте покупки только со своего компьютера или мобильного устройства**, чтобы сохранить конфиденциальность персональных данных (реквизитов карты). Если покупка совершается с использованием чужого компьютера, не сохраняйте на нем персональные данные и другую информацию. После завершения всех операций убедитесь, что персональные данные не сохранились.

**9. Установите на свой компьютер или мобильное устройство антивирусное программное обеспечение и регулярно его обновляйте.** Это поможет защитить себя от вредоносного программного обеспечения.

**10. Если в социальных сетях к вам обращаются друзья с просьбой** помочь перевести деньги на карту, оплатить что-либо и так далее, убедитесь, что этот человек действительно является тем, за кого себя выдает.

**11. Если ваш аккаунт в социальных сетях был взломан**, по возможности оповестите об этом подписчиков вашей страницы и смените пароль.

**12. Прежде чем участвовать** в лотереях, акциях, опросах и так далее, предварительно проверьте статус их легальности.

**Помните! Все перечисленные сценарии мошенничества НЕ относятся к принципу «нулевой ответственности» держателя карточки, так как конфиденциальные данные попадают к злоумышленнику непосредственно от держателя конфиденциальной информации. А это значит, что Банк не компенсирует клиенту понесенный ущерб.**

### памятка

## ПРОФИЛАКТИКА ГРИППА И ОРВИ

**Грипп - острая респираторная вирусная инфекция, которая имеет всемирное распространение, поражает все возрастные группы людей.**

### Как происходит заражение?

Попадая на слизистую оболочку верхних дыхательных путей, вирус внедряется в их эпителиальные клетки, проникает в кровь и вызывает интоксикацию. Создаются условия для активизации других видов бактерий, а также для проникновения извне новых бактерий, вызывающих вторичную инфекцию - пневмонию, бронхит, отит, обострение хронических заболеваний, могут пострадать сердце, суставы.

### Кто является источником инфекции?

Единственным источником и распространителем инфекции является больной человек. **Основным путем распространения вирусов гриппа** считается воздушно-капельное заражение при разговоре, кашле, чихании, а т.ж. контактно-бытовым путем при несоблюдении заболевшим и окружающими его лицами правил личной гигиены, в том числе пользования общими предметами ухода (полотенце, носовые платки, посуда и др.), не подвергавшимся обработке и дезинфекции.

### Как проявляется грипп?

В типичных случаях болезнь начинается внезапно: повышается температура до 38 - 40 градусов, появляется озноб, сильная головная боль, головокружение, боль в глазных яблоках и мышцах, слезотечение и резь в глазах.

### Что делать, если вы заболели?

При первых симптомах необходимо обратиться к врачу. Соблюдайте постельный режим и следуйте всем рекомендациям врача. Самолечение при гриппе недопустимо. Ведь предугадать течение гриппа невозможно, а осложнения могут быть самыми различными.

**Следует помнить, что соблюдение всех мер профилактики защитит от заболеваний гриппом и его неблагоприятных последствий.**

