

ИНФОРМАЦИОННО-ПРОСВЕТИТЕЛЬСКАЯ ПАМЯТКА

для обучающихся VIII–XI классов

КИБЕРБЕЗОПАСНОСТЬ ФИНАНСОВАЯ БЕЗОПАСНОСТЬ ФИНАНСОВАЯ ГРАМОТНОСТЬ

*Как распознать риски, не попасть в руки мошенников
и защитить себя и своих друзей*

НАЗНАЧЕНИЕ ПАМЯТКИ

Материал предназначен для классных часов, факультативных занятий, профилактических бесед, родительских собраний и оформления информационных стендов.

Памятка составлена в официально-деловом стиле, но с наглядной подачей материала, удобной для школьников 8–11 классов.

1. ОСНОВНЫЕ ПОНЯТИЯ

Кибербезопасность — это защита устройств, учетных записей, переписки, паролей и персональных данных от кражи, подмены, взлома и несанкционированного доступа.

Финансовая безопасность — это защита денежных средств, банковских карт, счетов, приложений дистанционного банковского обслуживания и иной финансовой информации от мошеннических действий.

Финансовая грамотность — это умение принимать обоснованные решения в сфере личных финансов, критически оценивать предложения, связанные с деньгами, и избегать рискованных действий.

КЛЮЧЕВОЙ ВЫВОД

Современные мошеннические схемы чаще всего строятся на психологическом воздействии:

создании чувства срочности, страха, доверия, любопытства, жалости или желания быстро заработать.

2. ОСНОВНЫЕ РИСКИ

2.1. Телефонное и мессенджер-мошенничество

Злоумышленники представляются сотрудниками банков, правоохранительных органов, магазинов, служб доставки, технической поддержки, а также родственниками и знакомыми.

Их цель — получить коды подтверждения, реквизиты карты, логины, пароли или заставить совершить перевод денежных средств.

2.2. Фишинг и поддельные сайты

Обучающемуся направляют ссылку на сайт, который внешне похож на официальный ресурс банка, интернет-магазина, образовательного сервиса, социальной сети или доставки.

После перехода у пользователя запрашивают конфиденциальные данные или предлагают установить вредоносное приложение.

2.3. Взлом учетных записей

После получения доступа к почте, мессенджеру, социальной сети или игровому аккаунту злоумышленники могут действовать от имени владельца, просить деньги у его друзей и распространять вредоносные ссылки.

2.4. Опасные онлайн-покупки

Наибольший риск представляют фейковые магазины, продажи через социальные сети и мессенджеры, предоплата непроверенным продавцам, подозрительные ссылки на оплату и искусственно заниженная цена.

2.5. Схемы «легкого заработка»

Подросткам могут предлагать использовать собственную карту, счет, аккаунт, SIM-карту или телефон для получения и перевода чужих денежных средств, а также оформлять на себя финансовые инструменты за вознаграждение.

2.6. Дипфейки и поддельные обращения от имени близких

С использованием современных технологий злоумышленники могут имитировать голос, фото и видео родственников, друзей, одноклассников и иных знакомых лиц.

3. КРАСНЫЕ ФЛАГИ МОШЕННИЧЕСТВА

ПРИЗНАКИ ОПАСНОГО ЗВОНКА ИЛИ СООБЩЕНИЯ

- требуют срочно действовать;
- запрещают советоваться с родителями или друзьями;

ПРИЗНАКИ ОПАСНОЙ ССЫЛКИ, САЙТА ИЛИ ПРЕДЛОЖЕНИЯ

- адрес сайта отличается от официального на 1–2 символа;

- | | |
|---|---|
| <ul style="list-style-type: none">• пугают уголовной ответственностью, потерей денег, опасностью для близких;• просят назвать код из SMS, пароль, реквизиты карты;• требуют установить приложение, включить демонстрацию экрана или удаленный доступ;• предлагают перевести деньги, снять наличные, передать ценности курьеру. | <ul style="list-style-type: none">• ресурс выглядит небрежно или не содержит понятных контактов;• для получения приза просят оплатить комиссию или доставку;• цена товара значительно ниже рыночной;• предлагают «легкий заработок» без навыков, но с использованием личной карты или счета. |
|---|---|

ОСОБЫЙ ПРИЗНАК МОШЕННИЧЕСТВА

Если вас торопят, пугают, уговаривают ничего никому не рассказывать и принять решение немедленно, необходимо сразу прекратить общение и обратиться к взрослому.

4. ЧТО ЗАПРЕЩАЕТСЯ ДЕЛАТЬ

- Сообщать посторонним лицам ПИН-код, CVV/CVC-код, коды из SMS и push-уведомлений, логины и пароли от интернет-банкинга, коды доступа к мессенджерам и социальным сетям.
- Передавать фото паспорта, банковской карты, а также скриншоты банковских приложений и личных кабинетов.
- Переводить деньги на «безопасный», «резервный», «специальный» или иной счет по указанию незнакомых лиц.
- Устанавливать программы удаленного доступа и иные приложения по ссылкам, полученным от незнакомцев.
- Передавать свою банковскую карту, SIM-карту, телефон, учетную запись или доступ к ним другим лицам.
- Соглашаться получать деньги на свой счет с последующим переводом третьим лицам.
- Оформлять кредит, заем, рассрочку, ИП, банковский счет либо иные финансовые инструменты по просьбе посторонних лиц.
- Вносить предоплату за товар или услугу на непроверенных ресурсах и по подозрительным ссылкам.
- Доверять фото, видео, голосовым сообщениям и документам из мессенджеров без дополнительной проверки.

5. ЧТО НЕОБХОДИМО ДЕЛАТЬ

- При подозрительном звонке, сообщении или ссылке немедленно прекратить взаимодействие.
- Проверять информацию только через официальные каналы: приложение банка, официальный сайт организации, номер на обратной стороне банковской карты.
- Сразу сообщать о подозрительной ситуации родителю, законному представителю, классному руководителю, педагогу или иному взрослому, которому доверяете.
- Использовать разные сложные пароли и включать двухфакторную аутентификацию там, где это возможно.

- Скачивать приложения только из официальных магазинов и своевременно устанавливать обновления.
- Проверять адрес сайта, контакты продавца, условия оплаты и возврата перед покупкой товара или услуги в интернете.
- Подключать уведомления по операциям и, по возможности, устанавливать лимиты на переводы и онлайн-платежи.
- Для онлайн-покупок использовать отдельную карту или отдельный счет.

6. ПРАКТИЧЕСКИЕ МЕРЫ ЗАЩИТЫ

ЗАЩИТА УСТРОЙСТВА	ЗАЩИТА АККАУНТОВ	ЗАЩИТА ДЕНЕГ
• надежный пароль или биометрия; • обновления системы; • контроль разрешений приложений; • приложения только из официальных магазинов.	• разные пароли для разных сервисов; • двухфакторная аутентификация; • проверка активных сессий; • никакой передачи кодов и паролей.	• лимиты по карте; • уведомления по операциям; • отдельная карта для онлайн-платежей; • немедленная блокировка карты при риске.

РЕКОМЕНДАЦИЯ ДЛЯ СЕМЬИ

Целесообразно заранее договориться о кодовом слове или контрольном вопросе на случай срочных просьб о переводе денег или иных нестандартных действий.

7. КАК ЗАЩИТИТЬ СЕБЯ И СВОИХ ДРУЗЕЙ

- Не пересылайте подозрительные ссылки, файлы и сообщения даже «ради интереса» или «в шутку».
- Если знакомый внезапно просит перевести деньги, сообщить код или перейти по ссылке, сначала свяжитесь с ним другим способом.
- Предупреждайте одноклассников о рисках «легкого заработка», связанного с использованием карт, счетов и аккаунтов.
- Если друг уже столкнулся с мошенничеством, помогите ему немедленно обратиться к взрослому, прекратить действия и сохранить доказательства.

РЕКОМЕНДУЕМАЯ ФРАЗА ПОМОЩИ ДРУГУ

«Остановись. Давай ничего не будем делать прямо сейчас. Проверим информацию через официальный источник и обратимся к взрослому».

8. АЛГОРИТМ ДЕЙСТВИЙ ПРИ ПОДОЗРЕНИИ НА МОШЕННИЧЕСТВО

Шаг	Действие
1	Прекратить разговор, переписку или переход по ссылке. Ничего не подтверждать и не переводить.
2	Немедленно сообщить о ситуации родителю, законному представителю, педагогу или иному взрослому, которому доверяете.
3	Если затронута банковская карта либо банковское приложение — связаться с банком по официальному номеру и заблокировать карту/доступ.
4	Сменить пароли от почты, мессенджеров, социальных сетей и иных важных сервисов.
5	Сохранить доказательства: скриншоты, ссылки, чеки, номера телефонов, сообщения, голосовые файлы.
6	При наличии признаков преступления обратиться по номеру 102 и подать заявление в установленном порядке.

ЗАПОМНИТЕ

Чем раньше остановлены действия мошенников и чем быстрее об этом сообщено взрослому, в банк и в правоохранительные органы, тем выше вероятность предотвратить ущерб или уменьшить его последствия.

9. КРАТКИЙ ПЕРЕЧЕНЬ ПРАВИЛ ДЛЯ ЗАПОМИНАНИЯ

1. Не доверяйте сообщениям и звонкам, связанным с деньгами, до самостоятельной проверки.
2. Никому не сообщайте коды подтверждения, ПИН-коды, CVV/CVC и пароли.
3. Не переводите деньги по указанию незнакомых лиц.
4. Не устанавливайте программы по просьбе звонящих или пишущих вам лиц.
5. Не соглашайтесь на «легкий заработок», связанный с переводом чужих денег.
6. Не молчите о подозрительных ситуациях — обращайтесь за помощью немедленно.

10. ИНФОРМАЦИОННАЯ ОСНОВА ПАМЯТКИ

Памятка подготовлена на основе открытых просветительских материалов:

- материалы Национального банка Республики Беларусь по финансовой грамотности и защите держателей банковских карт;
- материалы Единого портала финансовой грамотности по противодействию вишингу, фишингу и иным мошенническим схемам;
- материалы платежной системы БЕЛКАРТ по безопасным онлайн-платежам;
- профилактические рекомендации органов внутренних дел Республики Беларусь;
- предоставленный образец: «Памятка по финансовой гигиене. Как не попасть “в руки” мошенников».