

Памятка для 8–11 классов

Кибербезопасность + финансовая безопасность + финансовая грамотность

Понятно, логично и по-белорусски практично: какие есть риски, как не попасть в руки мошенников, как защитить себя, свои деньги, аккаунты и друзей.

Для классных часов и факультативов

С акцентом на Республику Беларусь

Подходит для 8–11 классов

Список красных флагов внутри

1. Зачем нужна эта памятка

Сегодня деньги, переписка, фото, школьные аккаунты, банковские приложения и даже отношения с друзьями связаны с телефоном и интернетом. Поэтому важно уметь:

КИБЕРБЕЗОПАСНОСТЬ

Защищать телефон, аккаунты, пароли, переписку и личные данные.

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

Не отдавать мошенникам деньги, карту, доступ к счету и коды подтверждения.

ФИНАНСОВАЯ ГРАМОТНОСТЬ

Понимать, как устроены платежи, переводы, покупки, сбережения и почему «легкие деньги» часто опасны.

ГЛАВНАЯ МЫСЛЬ

Мошенники чаще ломают не технику, а человека: давят на страх, срочность, жадность, стыд, любопытство и желание помочь.

2. Правило одной минуты: что нужно помнить всегда

ЗАПОМНИ 5 «НЕ»

- Не спешить.
- Не называть коды, пароли, CVV/CVC, ПИН, логины.
- Не переходить по подозрительным ссылкам.
- Не переводить деньги «для проверки», «на безопасный счет», «чтобы спасти родственника».
- Не молчи — сразу расскажи взрослому, которому доверяешь.

НИКОГДА НИКОМУ НЕ СООБЩАЙ

- код из SMS или push-уведомления;
- ПИН-код карты;
- CVV/CVC (3 цифры на обороте карты);
- логин и пароль от интернет-банкинга;
- код восстановления мессенджера;
- полные фото паспорта и банковской карты.

3. Главные риски для школьников 8–11 классов

3.1. Телефонные и мессенджер-мошенники

Звонят или пишут якобы от имени банка, милиции, следственных органов, службы безопасности, популярного магазина, службы доставки или даже «родственника».

КРАСНЫЕ ФЛАГИ

Срочно! Никому не говори Назови код Переведи деньги Установи приложение Выключи демонстрацию экрана

Если тебя торопят, пугают, запрещают советоваться с родителями или друзьями — это почти наверняка мошенничество.

КАК ПОСТУПИТЬ ПРАВИЛЬНО

- Сразу завершить разговор.
- Самостоятельно перезвонить по официальному номеру банка или службы.
- Если говорят, что звонят из милиции или другого госоргана, — не выполнять указания по телефону и сообщить взрослому.

3.2. «Безопасный счет», «специальная операция», «задекларируй деньги»

Это одна из самых опасных схем. Человека убеждают, что деньги надо срочно «спасти», передать курьеру, оставить в условленном месте, перевести на «защищенный» счет или снять наличные «для проверки».

ЗАПОМНИ

Никаких «безопасных счетов», на которые нужно переводить деньги по звонку, не существует. Правоохранительные органы не проводят «специальных» через школьников, родственников и курьеров.

3.3. Фейковая работа и «легкий заработок»

Подросткам могут предлагать:

- «просто принимать деньги на карту и пересылать дальше»;
- «сдать карту в аренду за процент»;
- «оформить счет/ИП/аккаунт за вознаграждение»;
- «быстрый заработок без опыта» через переводы, крипту, обналчивание.

ПОЧЕМУ ЭТО ОПАСНО

Так можно стать звеном преступной схемы: **дропом**, посредником, помощником мошенников. Даже если кажется, что ты «просто помог».

3.4. Фишинг: ссылки, поддельные сайты, QR-коды

Тебе присылают ссылку на «голосование», «выигрыш», «магазин», «проверку аккаунта», «фото», «обновление», «документ», «олимпиаду» или «электронный дневник».

КРАСНЫЕ ФЛАГИ

- адрес сайта выглядит почти как настоящий, но отличается 1–2 символами;
- просят быстро войти через мессенджер, соцсеть или почту;
- после перехода сайт просит коды подтверждения или данные карты;
- QR-код ведет неизвестно куда.

3.5. Взлом аккаунтов и кража переписки

Если мошенник получает доступ к твоему Telegram, Instagram, TikTok, почте или игровому аккаунту, он может:

- просить деньги у твоих друзей от твоего имени;
- получить фото, документы, переписку;
- использовать твой аккаунт для обмана других людей.

3.6. Поддельные друзья, родственники и дипфейки

Мошенники умеют подделывать голос, видео и фото. Тебе могут написать от имени знакомого: «Срочно одолжи», «Помоги перевести деньги», «Скинь код».

ЧТО ДЕЛАТЬ

Не верь сразу. **Перезвони сам** по известному номеру или задай **контрольный вопрос**, ответ на который знает только настоящий человек.

3.7. Покупки в интернете и соцсетях

Опасны фейковые магазины, продажи «с рук», предоплата за товар, которого не существует, и предложения слишком выгодной цены.

КРАСНЫЕ ФЛАГИ

Только предоплата Цена намного ниже рынка Новый аккаунт без истории Торопят оплатить сейчас

Отправляют подозрительную ссылку на оплату

4. Красные флаги мошенничества: общий список

Если тебе звонят или пишут

- требуют срочно действовать;
- запрещают рассказывать родителям или друзьям;
- угрожают, пугают уголовной ответственностью, потерей денег, «опасностью для близких»;
- просят код из SMS, пароль, реквизиты карты, фото паспорта;
- просят установить приложение или дать удаленный доступ к телефону;
- просят включить демонстрацию экрана или камеру;
- просят перевести деньги, снять наличные, передать их курьеру;
- предлагают деньги за использование твоего счета, карты, телефона или аккаунта.

Если это сайт, ссылка или «акция»

- выигрыш обещают без участия;
- для получения приза просят оплатить «комиссию»;
- сайт выглядит небрежно или странно;
- URL отличается от официального;
- нет понятных контактов, условий возврата, истории магазина;
- платежная форма требует лишние данные;
- подозрительный QR-код ведет на неизвестную страницу.

ГЛАВНЫЙ СИГНАЛ ОПАСНОСТИ

Если тебе **страшно, стыдно, неловко или очень хочется успеть первым**, значит пора сделать паузу и проверить информацию.

5. Алгоритм защиты: «СТОП – ПРОВЕРЬ – СПРОСИ – СООБЩИ»

- 1 **СТОП.** Не нажимай, не отвечай, не переводы, не подтверждай.
- 2 **ПРОВЕРЬ.** Посмотри адрес сайта, номер телефона, логично ли то, что от тебя требуют.
- 3 **СПРОСИ.** Обратись к родителю, учителю, классному руководителю, социальному педагогу, старшему родственнику или официальной службе банка.
- 4 **СООБЩИ.** Если есть признаки мошенничества — сообщи в банк, по номеру **102**, а также сохрани скриншоты и переписку.

ФРАЗА-ЩИТ

«Я ничего не подтверждаю по телефону. Я сам(а) перезвону по официальному номеру».

6. Как защитить телефон, аккаунты и карты

6.1. Цифровая гигиена

- ☐ Поставь сложный пароль или код блокировки на телефон.
- ☐ Включи двухфакторную аутентификацию там, где это возможно.
- ☐ Используй разные пароли для важных сервисов.
- ☐ Не передавай никому свои аккаунты, даже «нададолго».
- ☐ Скачивай приложения только из официальных магазинов.
- ☐ Регулярно обновляй систему и приложения.
- ☐ Проверь, какие приложения имеют доступ к камере, микрофону, контактам и сообщениям.
- ☐ Не храни фото карты и паспорта в открытом доступе.

6.2. Финансовая гигиена

- ☐ Подключи уведомления по операциям, если карта есть у тебя или у семьи.
- ☐ Установи лимиты на переводы и онлайн-покупки.
- ☐ Для покупок в интернете используй отдельную карту или отдельный счет.
- ☐ Не носи все деньги на одной карте.
- ☐ Никому не передавай карту и телефон с банковским приложением.
- ☐ Не публикуй в сети скриншоты, где видны реквизиты, штрихкоды, QR, номера заказов, билеты.
- ☐ Если карта потерялась — сразу блокируй ее через приложение или банк.

ПОЛЕЗНО ДЛЯ СЕМЬИ

Договоритесь о **кодовой фразе** на случай срочных просьб о деньгах. Если сообщение якобы от родственника выглядит странно — задайте этот вопрос.

7. Финансовая грамотность без сложных слов

Финансовая грамотность — это не только «уметь считать деньги». Это привычка принимать спокойные и разумные решения.

ПОЛЕЗНЫЕ ПРИВЫЧКИ

- записывай доходы и расходы;
- разделяй «хочу» и «нужно»;
- не покупай на эмоциях;
- оставляй время на проверку продавца;
- сберегай часть денег на цель;
- сначала проверяй безопасность, потом оплачивай.

ЧТО ВАЖНО СТАРШЕКЛАССНИКАМ

- не соглашаться на «подработку», где нужно гонять деньги по счетам;
- не давать пользоваться своей картой, SIM-картой, аккаунтом или кошельком;
- не брать на себя чужие финансовые обязательства;
- не оформлять кредит, рассрочку, заем «по просьбе добродетеля».

Мини-формула разумной покупки

Вопрос	Что проверить
Мне это действительно нужно?	Не покупаю ли я это из-за эмоций, давления, скидки «только сегодня»?
Продавец настоящий?	Есть ли история, отзывы, понятные условия, безопасный способ оплаты?
Я готов(а) потерять эту сумму?	Если нет — нельзя переводить деньги непроверенному человеку или сайту.

8. Как защитить друзей и одноклассников

- Не пересылал подозрительные ссылки даже «ради шутки».
- Если у друга взломали аккаунт — не переводи деньги и предупреди других.
- Объясни знакомым, что «аренда карты» и «прием переводов за процент» — опасная схема.
- Помоги другу проверить сайт, номер телефона, аккаунт магазина.
- Если друг напуган и молчит, не обвиняй его — сначала помоги остановить ущерб и обратиться за помощью.

ФРАЗА ПОМОЩИ

«Давай не будем делать это сейчас. Проверим вместе и спросим взрослого».

9. Что делать, если ты уже попался(ась)

- 1 **Не паникуй и не удаляй переписку.** Скриншоты, номера, чеки и ссылки могут помочь.
- 2 **Сразу скажи взрослому.** Чем раньше, тем больше шансов остановить ущерб.
- 3 **Если речь о карте или банке — срочно свяжись с банком** через официальный номер или приложение и заблокируй карту/доступ.
- 4 **Смени пароли** от почты, мессенджеров, соцсетей и важных сервисов.
- 5 **Проверь устройство:** нет ли подозрительных приложений, удаленного доступа, новых входов в аккаунты.
- 6 **Сообщи по номеру 102** и подай заявление, если есть потеря денег, взлом или вымогательство.

ОЧЕНЬ ВАЖНО

Нельзя скрывать проблему из-за страха, стыда или мысли «сам(а) разберусь». Мошенники рассчитывают именно на это.

10. 10 ситуаций, в которых нужно сразу насторожиться

1. Тебе пишут: «Проголосуй за меня по ссылке».
2. «Ты выиграл приз — оплати только доставку или комиссию».
3. «Срочно скинь код из SMS, мне нужно восстановить аккаунт».
4. «Дай карту/счет, деньги просто пройдут транзитом, ты заработаешь».
5. «На твое имя оформляют кредит, переведи деньги на безопасный счет».
6. «Я твой родственник, у меня беда, никому не говори».
7. «Установи приложение, это защита/документ/проверка/антивирус».
8. «Сними деньги и передай курьеру».
9. «Вот скидка 90% только на 5 минут, плати сейчас».
10. «Подработка: принимать переводы, снимать наличные, переводить дальше».

11. Короткие правила, которые можно повесить в классе

ДЕЛАЙ

- проверяй информацию;
- используй только официальные сайты и приложения;
- советуйся с взрослым, если страшно или непонятно;
- защищай пароли и личные данные;
- сохраняй доказательства мошенничества.

НЕ ДЕЛАЙ

- не сообщай коды и реквизиты;
- не переводи деньги по чужой инструкции;
- не бери «легкие деньги» за карту или счет;
- не ставь программы по указанию незнакомцев;
- не молчи, если что-то случилось.

Лучший антивирус против мошенников — это пауза, проверка и разговор с тем, кому ты доверяешь.

12. Основа памятки и белорусские материалы

Памятка подготовлена с опорой на просветительские материалы, относящиеся к Республике Беларусь, и на предоставленный пользователем файл.

- **Предоставленный файл:** «Памятка по финансовой гигиене. Как не попасть "в руки" мошенников» (PDF, 3 стр.). Из него использованы практические правила: не сообщать коды, не передавать наличные и ценности, не участвовать в "специальных", не устанавливать программы удаленного доступа, не сдавать карту/счет в пользование посторонним, при подозрении обращаться в банк и по номеру 102.

- **Национальный банк Республики Беларусь:** предупреждение о телефонных мошенниках, которые представляют сотрудники банков, запрашивают паспортные данные, реквизиты карт и коды из телефона, а также могут использовать подмену номера.

- **Единый портал финансовой грамотности (НБРБ):** материалы о вишинге, защите банковских карточек, телефонных мошенниках, цифровой финансовой безопасности.

- **Платежная система БЕЛКАРТ:** материалы о безопасных онлайн-платежах и технологии дополнительной аутентификации БЕЛКАРТ-ИнтернетПароль.

- **Материалы МВД/УВД Республики Беларусь:** напоминания о том, что сотрудники правоохранительных органов не дают указаний по телефону и в мессенджерах и что при подозрении на преступление нужно обращаться по номеру 102.

- **Национальный банк + Министерство образования:** учебно-методический комплект «Основы финансовой грамотности» для факультативных занятий школьников.

Рекомендация для образовательного процесса: использовать памятку как основу для классного часа, факультатива, школьной акции по безопасности, стенда в кабинете информатики/экономики или обсуждения с родителями.