

ПАМЯТКА ПО ФИНАНСОВОЙ ГИГИЕНЕ ДЛЯ ШКОЛЬНИКОВ 1–11 КЛАССОВ

Как защитить деньги, карту, телефон, аккаунты и себя от мошенников
Республика Беларусь • версия 2026

Главное правило для любого возраста

Если тебя просят назвать код, перевести деньги, дать карту, установить приложение, перейти по ссылке, забрать пакет или “никому не говорить” — остановись и сразу покажи взрослому, которому доверяешь.

Памятка подходит для младших, средних и старших классов. Ученикам 1–4 классов лучше читать её вместе с родителями или учителем. Ученикам 5–11 классов важно прочитать полностью, особенно разделы про “лёгкий заработок”.

Как читать эту памятку

- Если ты в 1–4 классе: запомни короткие правила, не отвечай незнакомцам про деньги и всегда зови взрослого.
- Если ты в 5–8 классе: внимательно прочитай блоки про сообщения, игры, QR-коды, покупки, аккаунты и “подработки”.
- Если ты в 9–11 классе: обязательно прочитай блоки про дропперство, закладки, крипто-переводы, карты, SIM-карты, ответственность по закону и кредиты.
- Если ты родитель или учитель: используйте памятку для классного часа, беседы дома, родительского собрания или стенда безопасности.

Самая короткая версия

Не знаю — не нажимаю. Не уверен — не перевожу. Попросят код — не называю. Предлагают лёгкие деньги — показываю взрослому. Пугают — кладу трубку и звоню родителям.

БЛОК 1. 10 правил, которые должен знать каждый школьник

- ☐ Никому не называю коды из SMS, push-уведомлений и мессенджеров.
- ☐ Никому не даю свою банковскую карту, телефон, SIM-карту, аккаунт, пароль.
- ☐ Не перевожу деньги незнакомым людям и не принимаю чужие деньги на свою карту.
- ☐ Не перехожу по подозрительным ссылкам из SMS, Telegram, Viber, TikTok, Instagram, игр и почты.
- ☐ Не устанавливаю приложения по просьбе незнакомцев или “работодателей”.
- ☐ Не сканирую случайные QR-коды, особенно если после этого просят карту или пароль.
- ☐ Если друг просит деньги в чате — сначала звоню ему или спрашиваю кодовое слово.
- ☐ Если звонят “из банка”, “милиции”, “школы”, “доставки” и говорят про деньги — зову взрослого.
- ☐ Если предлагают быстрый заработок через карту, переводы, пакеты, посылки, крипту — отказываюсь и показываю взрослому.
- ☐ Если уже ошибся — не скрываю. Чем быстрее рассказать взрослому, тем легче остановить беду.

БЛОК 2. Деньги, карта и телефон: что это значит для школьника

2.1. Карта — это ответственность

- Детская или подростковая карта — это не игрушка. Она связана с банком, родителями и твоими данными.
- Все операции по карте видны банку: где, когда и кому переводили деньги.
- Если через твою карту пройдут чужие или украденные деньги, могут возникнуть серьёзные проблемы у тебя и родителей.
- Даже если карта виртуальная и “её нельзя потрогать”, реквизиты всё равно могут использовать для переводов и покупок.

2.2. Что нельзя делать с картой

- фотографировать карту и отправлять фото кому-либо;

- называть CVV/CVC-код на обратной стороне карты;
- сообщать ПИН-код даже другу;
- давать карту “попользоваться”;
- передавать реквизиты за деньги;
- получать деньги от незнакомцев и переводить дальше;
- снимать деньги в банкомате по заданию из чата;
- привязывать карту к сомнительным сайтам, играм, ботам и приложениям.

2.3. Как пользоваться безопасно

- ☐ Для покупок в интернете лучше иметь отдельную карту с маленькой суммой.
- ☐ Покупки в играх и приложениях согласовываю с родителями.
- ☐ Не сохраняю карту на сомнительных сайтах.
- ☐ Проверяю списания вместе с родителями.
- ☐ Если карта потерялась — сразу говорю родителям.
- ☐ Если пришло странное списание — сразу говорю родителям и в банк.

БЛОК 3. Коды, пароли и аккаунты

Код из SMS — как ключ от квартиры

Если назвать код, чужой человек может войти в аккаунт, подтвердить перевод, сменить пароль, подключить новый телефон или украсть деньги.

3.1. Коды, которые нельзя называть

- код из SMS от банка;
- код из push-уведомления банка;
- код входа в Telegram, Viber, WhatsApp;
- код восстановления пароля;
- код подтверждения покупки, перевода или кредита;
- код для привязки нового устройства;
- одноразовый пароль из приложения-аутентификатора.

3.2. Пароли

- Не используй один пароль везде. Если украдут один — откроют все аккаунты.
- Не ставь пароль “123456”, дату рождения, имя, номер телефона, кличку питомца.
- Не отправляй пароль друзьям “на время”. Дружба может закончиться, а аккаунт останется украденным.
- Включи двухэтапную проверку в мессенджерах и важных аккаунтах вместе с родителями.
- Если кто-то вошёл в твой аккаунт — сразу меняй пароль и заверши все чужие сеансы.

3.3. Аккаунт — это тоже ценность

- Украденный аккаунт могут использовать, чтобы просить деньги у твоих друзей.
- Через аккаунт могут рассылать фишинговые ссылки, рекламу наркотиков, мошеннические вакансии.
- Продажа аккаунта может привести к тому, что действия преступников будут связаны с твоим именем, номером или устройством.

- Не продавай аккаунты игр, соцсетей, мессенджеров, электронные кошельки и SIM-карты.

БЛОК 4. Звонки и сообщения: как мошенники давят на школьников

4.1. Опасные фразы

Что пишут или говорят	Почему опасно	Что сделать
“Срочно назови код, иначе аккаунт удалят”	Тебя торопят, чтобы ты не подумал.	Не называй код. Покажи взрослому.
“Это банк, с карты списывают деньги”	Настоящий банк не просит коды в чате.	Зови родителей. Звонить только по официальному номеру.
“Твой друг попал в беду, нужны деньги”	Аккаунт друга могли взломать.	Позвони другу сам или спроси кодовое слово.
“Никому не говори, это секретная проверка”	Секретность нужна мошеннику.	Сразу расскажи взрослому.
“Ты нарушил закон, но мы поможем”	Тебя пугают, чтобы управлять тобой.	Не спорь. Зови взрослого, при угрозах — 102.
“Работа без опыта, деньги сегодня”	Может быть дропперство или закладки.	Не соглашайся. Покажи переписку.

4.2. Если звонят якобы из банка или милиции

1. Не называй ФИО, паспортные данные, карту, коды.
2. Скажи: “Я сейчас позову родителей”.
3. Положи трубку.
4. Покажи номер и историю звонка взрослому.
5. Взрослый сам позвонит в банк или 102 по официальному номеру.

4.3. Дипфейки: голос и видео могут быть поддельными

- Сейчас можно подделать голос друга, мамы, папы, учителя или директора.
- Если “родственник” плачет, торопит и просит деньги — это может быть подделка.
- Видео в мессенджере тоже не всегда доказывает, что человек настоящий.
- Лучшая защита — перезвонить самому по старому номеру и спросить кодовое слово.

БЛОК 5. Ссылки, QR-коды, игры и приложения

5.1. Ссылки

- Ссылка может вести на поддельный сайт банка, игры, магазина, доставки или соцсети.
- Поддельный сайт похож на настоящий, но крадёт логины, пароли и карты.
- Не переходи по ссылкам “получи приз”, “забери скин”, “верни аккаунт”, “проверь карту”, “получи выплату”.
- Если ссылка пришла от друга, его аккаунт могли взломать.

5.2. QR-коды

- QR-код — это такая же ссылка, только спрятанная в картинке.
- Опасны QR-коды на случайных наклейках, объявлениях, “штрафах”, в чатах, на листовках и в непонятных ботах.
- Если после QR-кода просят ввести карту, пароль или код — остановись.
- Для оплаты лучше открывать приложение банка самому, а не через случайный QR.

5.3. Игры и донаты

- Мошенники обещают бесплатные скины, валюту, робуксы, голду, премиум, аккаунт высокого уровня.
- Часто просят войти через свой аккаунт на “проверочном сайте” — так крадут аккаунт.

- Могут просить карту родителей “только для подтверждения возраста”. Это опасно.
- Не покупай игровые предметы через незнакомцев в чатах. Пользуйся официальным магазином и согласовывай с родителями.

5.4. Приложения

- Не устанавливай приложения по ссылке из чата.
- Не ставь APK-файлы от незнакомых людей.
- Не устанавливай “программу для заработка”, “проверку банка”, “антивирус МВД”, “бот для вывода денег”.
- Приложение может видеть экран, читать сообщения, красть коды и управлять телефоном.

БЛОК 6. Интернет-покупки, доставка и объявления

6.1. Если ты покупатель

- Не отправляй предоплату незнакомому продавцу без проверки.
- Слишком низкая цена — повод насторожиться.
- Не вводи карту по ссылке от продавца.
- Не сообщай код из SMS для “получения товара”.
- Лучше покупать через официальные площадки и безопасные способы оплаты.
- Сохраняй переписку и чеки.

6.2. Если ты продаёшь что-то

- Покупатель может прислать ссылку “получить оплату”. Это часто обман.
- Для получения денег на карту не нужен CVV/CVC и SMS-код.
- Не вводи данные карты на странице, которую прислал покупатель.
- Не отправляй товар, пока не убедился, что деньги действительно поступили.
- Если сомневаешься — покажи переписку родителям.

БЛОК 7. “Лёгкий заработок”: самый опасный раздел для 5–11 классов

Главное

Если заработок начинается со слов “просто дай карту”, “просто прими перевод”, “просто заberi пакет”, “просто купи крипту”, “просто зарегистрируй аккаунт” — это не нормальная работа.

7.1. Почему школьников вовлекают

- Школьникам часто нужны карманные деньги, и мошенники этим пользуются.
- Они обещают лёгкие деньги без опыта и без объяснений.
- Пишут в Telegram, TikTok, Instagram, игровых чатах, школьных чатах, через знакомых.
- Говорят: “тебе ничего не будет”, “ты несовершеннолетний”, “ты просто поможешь”. Это ложь.
- Организаторы прячутся, а школьник оставляет следы: карта, телефон, камеры, переписка, геолокация.

7.2. Опасные виды “заработка”

Предложение	Что может скрываться	Почему нельзя
“Дай карту или реквизиты, заплатим”	Дропперство: через карту гоняют чужие или украденные деньги.	Карту заблокируют, могут быть вопросы банка и милиции, ответственность по закону.

“Прими деньги и отправь дальше”	Транзит преступных денег.	Ты становишься частью цепочки.
“Сними деньги в банкомате и передай”	Обналичивание денег жертвы мошенничества.	Тебя легко найти по камерам и карте.
“Купи крипту на деньги клиента”	Вывод денег через токены/криптовалюту.	Может нарушать правила операций и использоваться для преступных денег.
“Забери пакет, спрячь, сфотографируй место”	Закладки наркотиков или психотропов.	Это очень серьёзный уголовный риск, в том числе для подростков.
“Расклей QR-коды/рекламу канала”	Реклама наркомаркета, фишинга или мошенников.	Можно стать участником распространения незаконной схемы.
“Продай аккаунт/SIM/кошелёк”	Аккаунт используют для обмана людей.	След приведёт к твоему номеру или данным.
“Оформи ИП/фирму/счёт”	Фиктивный бизнес для долгов и вывода денег.	Риски налогов, долгов и ответственности.
“Пиши людям по скрипту”	Фишинг или мошеннический колл-центр.	Даже переписка может быть помощью мошенникам.

7.3. Дропперство простыми словами

- Дроппер — человек, через карту, счёт, кошелёк, SIM-карту или аккаунт которого проводят чужие деньги.
- Мошенники могут платить мало, а через карту проводить большие суммы.
- Фразы: “это зарплата”, “это деньги клиента”, “это для бизнеса”, “просто переведи дальше” — красный флаг.
- В Республике Беларусь за незаконную передачу реквизитов платёжных документов из корыстных побуждений предусмотрена ответственность. За незаконный оборот платёжных инструментов и реквизитов возможна уголовная ответственность.
- Если тебе 14, 15, 16 или 17 лет, это не значит, что “ничего не будет”. Родителям тоже придётся разбираться с последствиями.

7.4. Закладчики и “курьеры”

- Если предлагают “просто отнести”, “просто забрать”, “просто положить в тайник”, “просто сфотографировать место” — это может быть наркотическая схема.
- Нельзя соглашаться даже из любопытства и “один раз”.
- Нельзя хранить чужой пакет “до вечера”.
- Нельзя передавать координаты тайника, фото, адреса, инструкции.
- По отдельным наркопреступлениям в РБ уголовная ответственность возможна с 14 лет. Последствия могут быть очень тяжёлыми: судимость, лишение свободы, проблемы с учёбой и будущей работой.

7.5. Как отказать

- “Нет, я не передаю карту и данные”.
- “Нет, я не принимаю чужие деньги”.
- “Нет, я не забираю пакеты”.
- “Я покажу это родителям/учителю”.
- Не спорь долго. Сделай скриншоты, заблокируй контакт, расскажи взрослому.
- Если угрожают — сразу взрослым и 102.

БЛОК 8. Личные данные, фото и шантаж

8.1. Что нельзя отправлять

- фото паспорта, свидетельства, ученического/студенческого билета;
- фото банковской карты;
- селфи с документом;

- адрес дома, подъезд, номер квартиры;
- расписание, когда дома никого нет;
- геолокацию незнакомцам;
- интимные фото или видео;
- пароли, коды и скриншоты из банковского приложения.

8.2. Шантаж

- Шантажист может угрожать: “разошлю фото”, “скажу родителям”, “выложу в чат”, “напишу в школу”.
- Не плати шантажисту. Часто после оплаты требуют ещё.
- Не отправляй новые фото “чтобы всё удалить”.
- Сохрани переписку и сразу скажи взрослому.
- Если угрожают — можно обращаться в милицию. Виноват тот, кто шантажирует, а не тот, кто попросил помощи.

8.3. Что можно публиковать безопаснее

- меньше личных данных в открытом профиле;
- закрытый профиль для незнакомцев;
- без фото документов, карт, билетов с QR-кодами;
- без адреса и маршрутов;
- без подробностей о деньгах семьи, покупках, поездках и отсутствии дома.

БЛОК 9. Конфликты, давление друзей и школьные чаты

- Иногда опасные предложения приходят не от незнакомцев, а от знакомых: одноклассника, старшего ученика, друга из игры.
- “Все так делают” — не доказательство безопасности.
- “Ты что, слабак?” — манипуляция.
- “Мы тебя исключим из чата” — давление, а не причина рисковать.
- “Если расскажешь — будут проблемы” — угроза, о которой нужно сообщить взрослым.

Что делать, если давят

6. Скажи коротко: “Нет”. Не оправдывайся долго.
7. Выйди из чата или заблокируй человека, если можешь.
8. Сделай скриншоты угроз и предложений.
9. Покажи родителям, классному руководителю, социальному педагогу или другому взрослому.
10. Если речь о наркотиках, деньгах, угрозах — не жди, обращай за помощью сразу.

БЛОК 10. Что делать, если ты уже ошибся

Не скрывай ошибку

Мошенники хотят, чтобы ты молчал. Но молчание помогает им. Чем быстрее ты скажешь взрослому, тем больше шансов остановить ущерб.

10.1. Назвал код или пароль

11. Сразу скажи родителям или учителю.
12. С другого безопасного устройства смените пароль.
13. Завершите все неизвестные сеансы в аккаунте.
14. Если это банк — родители должны срочно позвонить в банк и заблокировать карту/операции.

15. Сохраните номер, чат, ссылку, скриншоты.

10.2. Перевёл деньги или принял чужой перевод

16. Ничего больше не переводить.

17. Сказать родителям.

18. Сохранить чек, переписку, номер карты/телефона получателя.

19. Позвонить в банк.

20. При признаках мошенничества обратиться в 102.

10.3. Передал карту, реквизиты или аккаунт

21. Сразу сказать родителям.

22. Заблокировать карту и сменить пароли.

23. Проверить операции.

24. Не выполнять новые просьбы “куратора”.

25. Сохранить переписку и обратиться за помощью.

10.4. Согласился на опасную “работу”

26. Остановиться сразу. Не ходить на встречи, не брать пакеты, не делать переводы.

27. Сохранить переписку и задания.

28. Рассказать взрослому.

29. Если есть угрозы — 102.

30. Если использовалась карта — срочно банк.

БЛОК 11. Правила по возрастам

1–4 классы: самые простые правила

- Незнакомым про деньги не отвечаю.
- Коды из SMS никому не говорю.
- Если пришла ссылка или QR-код — зову взрослого.
- Если в игре обещают подарок за пароль — не верю.
- Если кто-то просит карту родителей — сразу говорю родителям.
- Если страшно или стыдно — всё равно говорю взрослому. Взрослые помогут.

5–8 классы: добавляются игры, покупки, чаты и первые карты

- Не покупаю скины, валюту и аккаунты у знакомцев.
- Не ввожу логин и пароль от игры на посторонних сайтах.
- Не принимаю деньги на карту для других.
- Не перехожу по ссылкам “получи подарок” и “забери выигрыш”.
- Не продаю аккаунты, SIM-карты и доступы.
- Любую подработку обсуждаю с родителями до ответа.

9–11 классы: добавляются юридические и финансовые риски

- Не оформляю карты, счета, ИП, электронные кошельки и аккаунты для третьих лиц.
- Не участвую в переводах, обналичивании, крипто-операциях “за процент”.
- Не беру кредиты, рассрочки и микрозаймы по просьбе других людей или под давлением.
- Не соглашаюсь на “курьерские” задания с пакетами, наличными и тайниками.
- Понимаю: несовершеннолетний возраст не означает отсутствие ответственности. По ряду преступлений ответственность возможна с 14 лет, а с 16 лет — по многим составам.

- Если предложение выглядит сомнительно, лучше потерять “заработок”, чем получить проблемы с законом.

БЛОК 12. Родителям и учителям: как объяснять без страха и крика

12.1. Что важно сказать детям

- “Ты можешь прийти ко мне с любой ошибкой. Сначала будем спасать ситуацию, потом разбираться”.
- “Если тебя просят молчать — именно тогда нужно сказать взрослому”.
- “Лёгкие деньги через карту, пакеты и переводы — опасно”.
- “Код из SMS нельзя говорить никому, даже если человек представился сотрудником банка”.
- “Если друг просит деньги в чате, его аккаунт могли взломать”.

12.2. Домашние настройки

- ☐ Лимиты на детской карте установлены.
- ☐ Уведомления по операциям приходят родителю.
- ☐ Покупки в играх и приложениях обсуждены заранее.
- ☐ У ребёнка есть правило: подозрительные сообщения показывать взрослому.
- ☐ В семье есть кодовое слово.
- ☐ Раз в месяц проверяются приложения, подписки, активные сессии.
- ☐ Ребёнок знает телефоны родителей и 102.

12.3. Для классного часа

- Разберите 5–7 реальных фраз мошенников и попросите учеников определить красные флаги.
- Отдельно обсудите дропперство: “дать карту” — не безобидная помощь.
- Отдельно обсудите закладки: “просто пакет” может разрушить будущее.
- Покажите, как проверить ссылку и почему QR-код — это тоже ссылка.
- Объясните, что обращаться за помощью не стыдно.

БЛОК 13. Полезные контакты

- Родители или законные представители — первый контакт для школьника.
- Классный руководитель, социальный педагог, школьный психолог — если страшно сказать дома или нужна помощь в школе.
- 102 — милиция, если есть мошенничество, угрозы, вымогательство, наркотики, вовлечение в переводы или опасные задания.
- Банк — номер только с официального сайта, приложения или карты. Не звонить по номеру из подозрительного сообщения.
- Национальный банк Республики Беларусь: nbrb.by.
- Портал финансовой грамотности: fingramota.by.
- Национальный правовой Интернет-портал: pravo.by.
- Национальный центр защиты персональных данных: cpd.by.

Короткая памятка для печати и размещения в классе

СТОП-ПРАВИЛА ШКОЛЬНИКА

1. Код не называю.
2. Карту не даю.
3. Деньги незнакомым не перевожу.
4. Чужие деньги на карту не принимаю.
5. Пакеты и “закладки” не беру.
6. Ссылки и QR-коды проверяю со взрослым.
7. Лёгкий заработок показываю родителям.
8. Ошибся — сразу говорю взрослому.

Ситуация	Что делать
Пришёл код из SMS, а кто-то просит его назвать	Не называй. Покажи взрослому.
Пишет друг и просит деньги	Позвони другу. Спроси кодовое слово.
Звонят из “банка” или “милиции”	Положи трубку. Позови взрослого.
Предлагают заработать через карту	Откажись. Это может быть дропперство.
Просят забрать пакет или спрятать вещь	Откажись. Это может быть наркотическая схема.
Просят установить приложение	Не устанавливай. Покажи взрослому.
Уже сообщил код или перевёл деньги	Сразу скажи взрослому. Чем быстрее — тем лучше.

Лучше показаться осторожным, чем стать жертвой мошенников или участником преступной схемы.