ПАМЯТКА ПО ФИНАНСОВОЙ ГИГИЕНЕ

Подробная версия по блокам: угрозы, признаки обмана, правила поведения, действия при инциденте

Республика Беларусь • 2026

Главное правило всей памятки

Не действуйте под давлением. Сначала остановитесь, затем проверьте информацию через официальный канал и посоветуйтесь с человеком, которому доверяете.

Памятка предназначена для школьников, родителей, педагогов, взрослых граждан и пожилых людей. Текст написан простым языком. Информация о законах дана как ориентир и не заменяет консультацию юриста. Актуальные редакции норм проверяйте на pravo.by.

Как пользоваться памяткой

- Читайте не только свой раздел. Мошеннические схемы часто смешиваются: звонок из “банка” может закончиться кредитом, передачей наличных, установкой удалённого доступа или вовлечением в дропперство.
- Каждый блок построен одинаково: где опасность, как её распознать, что нельзя делать, как поступить правильно, что делать, если ошибка уже произошла.
- Распечатайте короткие чек-листы из конца документа и разместите дома, в классе, кабинете, общежитии или на рабочем месте.
- Для семьи полезно выбрать кодовое слово и заранее договориться: крупные переводы, кредиты и передача наличных никогда не делаются без проверки вторым человеком.

БЛОК 1. Универсальные правила финансовой безопасности

Правило “Пауза — Проверка — Совет”
Пауза: ничего не нажимать и не переводить. Проверка: позвонить по официальному номеру. Совет: обсудить с близким, родителем, учителем, банком, юристом или 102.

1.1. Что нельзя сообщать никому

- коды из SMS, push-уведомлений, приложения-аутентификатора;
- ПИН-код, CVV/CVC-код, срок действия карты, полные реквизиты карты;
- логины, пароли, кодовые слова банка, ответы на секретные вопросы;
- личный номер паспорта, фото/сканы документов, селфи с паспортом без законной и понятной причины;
- коды входа в Telegram, Viber, WhatsApp, электронную почту, соцсети;
- данные для входа в интернет-банк, МСИ, электронные и виртуальные кошельки, криптокошельки;
- коды для привязки нового устройства, восстановления пароля, подтверждения кредита или перевода.

1.2. Что должно насторожить сразу

Признак	Что это значит	Правильная реакция
Срочность: “прямо сейчас”, “у вас 5 минут”	Вас лишают времени на проверку.	Остановиться. Завершить разговор. Проверить отдельно.
Секретность: “никому не говорите”	Вас изолируют от помощи близких.	Обязательно рассказать доверенному человеку.
Страх: “уголовное дело”, “обыск”, “кредит”, “терроризм”	Давление на эмоции.	Не спорить, не оправдываться, звонить 102/официально.
Выгода: “лёгкие деньги”, “без опыта”, “за 10 минут”	Возможное вовлечение в схему.	Отказаться и показать переписку взрослому/специалисту.
Просьба установить приложение	Может быть удалённый доступ или вирус.	Не устанавливать. Проверять через официальный магазин.
Просьба назвать код	Код почти всегда открывает доступ или подтверждает операцию.	Не называть никогда.
Деньги через вашу карту	Ваш счёт может стать частью преступной цепочки.	Не принимать и не переводить.

1.3. Минимальный набор настроек безопасности

☐ Уведомления обо всех операциях по картам и счетам включены.

☐ Лимиты на переводы и снятие наличных установлены.

☐ Для онлайн-покупок есть отдельная карта с небольшим балансом.

☐ На телефоне стоит пароль/биометрия, SIM-карта защищена PIN-кодом.

☐ Пароли к банку, почте и мессенджерам разные.

☐ Двухфакторная защита включена в почте, банке, мессенджерах, соцсетях.

☐ Активные сессии и привязанные устройства проверяются не реже раза в месяц.

☐ В семье есть кодовое слово для срочных просьб о деньгах.

БЛОК 2. Звонки “из банка”, “милиции”, “Следственного комитета”, “Нацбанка”

2.1. Где опасность

- Мошенник представляется сотрудником банка, милиции, КГК, КГБ, Следственного комитета, Нацбанка, налоговой или мобильного оператора.
- Он может знать ваше имя, банк, часть номера карты, адрес, место работы. Это не доказывает, что звонок настоящий: данные могли попасть в утечку или быть взяты из открытых источников.
- Цель — заставить вас назвать код, установить приложение, оформить кредит, перевести деньги, передать наличные курьеру или “помочь следствию”.

2.2. Типичные сценарии

Сценарий	Что говорят	Что хотят получить
“Подозрительная операция”	“Сейчас с вашей карты списывают деньги. Назовите код, чтобы отменить”.	Код подтверждения перевода/входа.
“На вас оформляют кредит”	“Нужно срочно оформить встречный кредит и перевести деньги на резервный счёт”.	Кредитные деньги, которые потом исчезнут.
“Спецоперация”	“Вы помогаете поймать преступников. Никому не говорите”.	Изоляцию от близких и контроль над действиями.
“Вы стали дропом”	“Чтобы доказать невиновность, переведите деньги/назовите данные”.	Деньги и доступы под страхом ответственности.
“Проверка квартиры”	“Найдите наличные, золото, документы. Сейчас приедет курьер”.	Наличные, валюту, драгоценности.
“Помощь родственнику”	“Ваш сын/дочь попали в ДТП, срочно нужны деньги”.	Быстрый перевод или передачу наличных.

2.3. Что нельзя делать

- не продолжать разговор по финансовым вопросам дольше 10–15 секунд;
- не подтверждать личные данные “для проверки личности”;
- не называть коды и пароли;
- не устанавливать программы удалённого доступа;
- не включать демонстрацию экрана во время входа в банк;
- не оформлять кредиты и карты по указанию звонящего;
- не переводить деньги на “безопасные”, “резервные”, “транзитные” счета;
- не передавать наличные курьерам;
- не выезжать к банкомату или в банк по указанию неизвестного.

2.4. Как правильно

1. Завершить звонок. Не спорить и не доказывать.
2. Самостоятельно открыть официальное приложение банка или сайт банка.
3. Позвонить по номеру с банковской карты или официального сайта.
4. Если звучит угроза уголовного дела — звонить 102 или идти в ближайшее подразделение милиции.
5. Сообщить близкому человеку, особенно если вас просили “никому не говорить”.

БЛОК 3. Мессенджеры, соцсети, дипфейки и поддельные документы

3.1. Мессенджеры как зона риска

- В Telegram, Viber, WhatsApp и соцсетях легко подделать имя, фото, должность, документ, печать, форму, аватар и даже голос.
- Сообщение “от директора”, “от учителя”, “от родственника”, “от банка” может быть отправлено со взломанного аккаунта.
- Файл с названием “постановление.pdf”, “повестка”, “договор”, “чек” может быть вредоносным или вести на фишинговую страницу.

3.2. Дипфейки

- Дипфейк — поддельный голос, изображение или видео, созданные с помощью ИИ.
- Мошенникам достаточно коротких видео/аудио из соцсетей, чтобы имитировать голос.
- Особенно опасны звонки якобы от ребёнка, родителя, друга, коллеги или руководителя с просьбой срочно перевести деньги.
- Дипфейк часто сопровождается плохой связью, плачем, шумом, спешкой, запретом перезванивать.

3.3. Защита от дипфейков

☐ Есть семейное кодовое слово.

☐ При любой срочной просьбе о деньгах перезваниваем по старому известному номеру.

☐ Задаём проверочный вопрос, ответ на который нельзя узнать из соцсетей.

☐ Не верим видео и фото в форме без проверки официальным каналом.

☐ Не публикуем лишние аудио/видео с голосом детей и близких.

3.4. Поддельные документы

- Скриншот удостоверения, приказа, постановления, печати или “письма Нацбанка” в мессенджере не является доказательством.
- Документы могут быть нарисованы, склеены из настоящих образцов или сгенерированы ИИ.
- Если документ требует срочно перевести деньги, назвать код, установить приложение или сохранить всё в тайне — это признак обмана.

БЛОК 4. Банковские карты, счета, переводы и наличные

4.1. Карта — это не просто пластик

- Карта связана с вашим счётом и вашей личностью. Все операции оставляют след.
- Передача карты “на время”, “родственнику”, “работодателю”, “покупателю”, “куратору” может привести к блокировке и расследованию.
- Даже виртуальная карта и реквизиты без физического пластика могут дать доступ к операциям.

4.2. Нельзя

- передавать карту, реквизиты, фото карты, CVV, ПИН;
- открывать счёт или карту по просьбе третьих лиц;
- давать доступ к интернет-банку или электронному кошельку;
- получать чужие деньги на свой счёт и переводить дальше;
- снимать чужие деньги в банкомате;
- проводить “тестовые” переводы по инструкции;

- возвращать “ошибочный перевод” на номер/карту, которые назвал незнакомец;
- пользоваться чужой картой без понятного и доказуемого согласия владельца.

4.3. Ошибочный перевод

Как правильно вернуть ошибочно поступившие деньги
Не переводите деньги по просьбе отправителя. Обратитесь в банк или к мобильному оператору. Пусть возврат оформляется официально.

4.4. Наличные и курьеры

- Не передавайте деньги, валюту, золото, украшения, документы “курьеру банка”, “сотруднику милиции”, “адвокату родственника”.
- Не перевозите наличные по городу, стране или за границу по чужому заданию.
- Не соглашайтесь забрать деньги у пожилого человека и положить их на карту/криптокошелёк. Это может быть обналичивание денег жертвы мошенничества.
- Не выполняйте задания “подойди к банкомату”, “пополни карту”, “разбей сумму на части”, “не говори кассиру правду”.

4.5. Безопасная организация своих денег

- Основные накопления храните отдельно от карты ежедневных расходов.
- Для интернет-покупок используйте отдельную карту с лимитом.
- Для крупных сумм включайте дополнительные подтверждения и лимиты.
- Не храните все деньги в одном банке/на одной карте, если это создаёт для вас риск полной потери доступа.
- Регулярно проверяйте операции и уведомления.

БЛОК 5. Кредиты, рассрочки, микрозаймы и долговые ловушки

5.1. Основные опасности

- Кредит, оформленный на вас, обязанность платить создаёт для вас, а не для того, кто “попросил помочь”.
- Мошенники заставляют оформить кредит “для защиты”, “для отмены”, “для проверки”, “для спецоперации”. Это обман.
- Микрозаймы и рассрочки могут казаться небольшими, но несколько мелких долгов быстро превращаются в крупную нагрузку.
- Перекредитование без плана часто усугубляет ситуацию.

5.2. Перед любым кредитом проверьте

☐ Понимаю полную сумму переплаты.

☐ Платёж не ломает мой ежемесячный бюджет.

☐ Есть резерв хотя бы на 1–3 месяца платежей.

☐ Кредит не оформляется под давлением звонящего или знакомого.

☐ Я не беру деньги для передачи третьему лицу.

☐ Договор, ставка, комиссии и штрафы прочитаны.

☐ Есть план, из каких доходов будет погашение.

5.3. Если кредит уже оформили под давлением

6. Не переводите полученные деньги дальше.
7. Сразу свяжитесь с банком и сообщите о мошенническом давлении.
8. Попросите заблокировать операции, если возможно.
9. Сохраните записи, скриншоты, номера, переписку.
10. Обратитесь в 102 и подайте заявление.

БЛОК 6. Сайты, ссылки, QR-коды, приложения и Wi-Fi

6.1. Фишинг

- Фишинг — поддельная страница, которая собирает логины, пароли, коды и данные карт.
- Ссылка может прийти от “банка”, “почты”, “доставки”, “налоговой”, “маркетплейса”, “продавца”, “работодателя”.
- Адрес сайта может отличаться одной буквой, лишним дефисом, странной зоной домена или похожим названием.

6.2. QR-фишинг

- QR-код может вести куда угодно: на оплату, фальшивый сайт, установку приложения, подписку, перевод денег.
- Опасны QR-коды на наклейках в подъездах, транспорте, на объявлениях, “штрафах”, письмах, посылках, в чатах.
- После сканирования всегда смотрите адрес сайта до ввода данных.
- Если QR-код просит ввести карту, CVV, код из SMS или пароль — остановитесь.

6.3. Поддельные приложения и удалённый доступ

- Файл APK, присланный в чат, может быть вирусом.
- Приложение удалённого доступа позволяет видеть экран и управлять устройством.
- Демонстрация экрана во время входа в банк может раскрыть баланс, SMS, push-коды и операции.
- Банк не требует устанавливать AnyDesk, TeamViewer, “защитный модуль”, “антивирус МВД”, “приложение проверки”.

6.4. Правила цифровой безопасности

☐ Открываю банк только через официальное приложение или вручную введённый адрес.

☐ Не перехожу по ссылкам из подозрительных SMS, писем и чатов.

☐ Проверяю домен сайта перед вводом данных.

☐ Не устанавливаю приложения вне официальных магазинов без необходимости и проверки.

☐ Не использую публичный Wi-Fi для банковских операций без защиты.

☐ Регулярно обновляю телефон, браузер, банковские приложения.

☐ Удаляю приложения, которыми не пользуюсь.

☐ Не подтверждаю неожиданные push-запросы на вход.

БЛОК 7. Пароли, почта, мессенджеры и аккаунты

7.1. Почему почта особенно важна

- Через электронную почту часто восстанавливают пароли от банка, соцсетей, маркетплейсов, госуслуг и рабочих сервисов.
- Если мошенник получил доступ к почте, он может менять пароли, читать чеки, находить документы, узнавать ваши контакты.
- Почта должна иметь самый сильный пароль и двухфакторную защиту.

7.2. Правила паролей

- Не используйте один пароль для разных сервисов.
- Не используйте дату рождения, имя, номер телефона, кличку питомца.
- Лучше длинная парольная фраза, чем короткий сложный пароль.
- Храните пароли в менеджере паролей или в другом безопасном месте, а не в заметках без защиты.
- Меняйте пароль сразу, если был подозрительный вход или утечка.

7.3. Мессенджеры

- Не сообщайте код входа в Telegram/Viber/WhatsApp. Это равно передаче аккаунта.
- Включите двухэтапную проверку в мессенджерах.
- Проверяйте активные устройства и завершайте незнакомые сессии.
- Если аккаунт взломали, предупредите контакты: от вашего имени могут просить деньги.

БЛОК 8. Интернет-покупки, объявления и доставка

8.1. Где чаще обманывают

- соцсети и мессенджеры без официальной площадки;
- объявления с очень низкой ценой;
- страницы-клоны известных магазинов;
- поддельные службы доставки;
- фальшивая “безопасная сделка”;
- предоплата за товар, которого нет;
- возврат денег через “ссылку на получение”.

8.2. Что нельзя делать покупателю

- вводить данные карты по ссылке от продавца;
- сообщать коды из SMS для “получения денег”;
- переводить предоплату незнакомцу без проверки;
- уходить из официального чата площадки в мессенджер, если площадка предупреждает об опасности;
- верить скриншоту паспорта продавца как гарантии — документы тоже подделывают.

8.3. Что нельзя делать продавцу

- переходить по ссылке “получить оплату” от покупателя;
- вводить данные карты, CVV и SMS-код для зачисления денег;
- отправлять товар до подтверждённой оплаты в безопасном канале;
- сообщать покупателю лишние персональные данные;
- скачивать “приложение доставки” из чата.

8.4. Безопасная покупка

☐ Проверяю продавца, отзывы, дату создания аккаунта.

☐ Сравниваю цену с рынком.

☐ Использую официальные способы оплаты площадки.

☐ Не ввожу CVV/CVC и SMS-коды для получения денег.

☐ Сохраняю переписку, чеки, объявления и трек-номера.

☐ При сомнении выбираю оплату при получении или личную встречу в безопасном месте.

БЛОК 9. Удалённая работа и вакансии

9.1. Как выглядит опасная вакансия

Фраза в вакансии	Опасность	Что делать
“Без опыта, 500–2000 рублей в день, 10 минут”	Вероятно, незаконная схема или обман.	Не откликаться, проверить компанию.
“Нужно принимать деньги на карту и отправлять дальше”	Дропперство/транзит денег.	Отказаться.
“Оформите карту/кошелёк/аккаунт, мы будем пользоваться”	Передача доступа к финансовому инструменту.	Не оформлять.
“Купите крипту на деньги клиента”	Возможный вывод преступных денег и нарушение правил операций с токенами.	Не участвовать.
“Оплатите обучение/страховку/верификацию”	Выманивание предоплаты.	Проверить договор, не платить сомнительным лицам.
“Скачайте приложение не из магазина”	Риск вируса/удалённого доступа.	Не скачивать.
“Нужен паспорт в чат до собеседования”	Риск кражи персональных данных.	Уточнить законное основание, проверять работодателя.

9.2. Как проверить работодателя

☐ Есть полное название организации, УНП, сайт, адрес, телефон.

☐ Контакты совпадают с официальными источниками.

☐ Договор понятен: должность, обязанности, оплата, сроки.

☐ Нет просьбы использовать личную карту для чужих переводов.

☐ Нет требования платить за трудоустройство.

☐ Собеседование проходит в нормальном деловом формате, а не только в анонимном чате.

☐ Задания не связаны с обманом людей, переводами денег, обходом правил площадок.

БЛОК 10. “Быстрые заработки”, которые могут караться законом РБ

Самое важное
Незнание всей схемы не всегда спасает. Если вы дали карту, приняли деньги, сняли наличные, отнесли пакет или помогли скрыть следы, ваши действия могут оцениваться как участие или помощь.

10.1. Дропперство

- Дропперство — использование карты, счёта, электронного кошелька, SIM-карты, аккаунта или документов человека для перевода, хранения, обналичивания или вывода чужих денег.
- Часто вовлекают школьников, студентов, безработных, пожилых людей: обещают небольшое вознаграждение и говорят, что “ничего делать не надо”.
- Типичные роли: открыть карту; передать реквизиты; принять перевод; снять наличные; купить криптовалюту; переслать деньги; оформить SIM или аккаунт; пройти верификацию лицом.

Признаки дроп-схемы

- платят за открытие карты или счёта;
- просят прислать фото карты, паспорт, селфи, логин/пароль;
- обещают процент за переводы;
- запрещают рассказывать банку настоящую цель операций;
- просят дробить суммы;
- говорят “если спросят — это долг/покупка/зарплата”;
- деньги приходят от разных людей и быстро уходят дальше.

Риски по закону

- В РБ предусмотрена административная ответственность за незаконное предоставление реквизитов платёжных документов из корыстных побуждений (ориентир: ст. 12.35 КоАП).
- Незаконный оборот платёжных инструментов, средств платежа и их реквизитов может влечь уголовную ответственность (ориентир: ст. 222 УК).
- Если через карту проходят деньги от мошенничества, могут возникать вопросы о соучастии, пособничестве, легализации преступных доходов и иных составах.
- Банк может заблокировать карту, счёт, операции и запросить объяснения. Репутационные последствия могут мешать учёбе, работе, кредитам.

10.2. Закладчики, курьеры и “посылки”

- Предложения “забрать пакет”, “положить в тайник”, “сделать фото места”, “передать посылку”, “ничего не спрашивать” могут быть связаны с незаконным оборотом наркотиков.
- Опасны не только сами закладки. Риск создают упаковка, хранение, перевозка, пересылка, передача координат, фотоотчёты, администрирование магазина, реклама канала.
- Фразы “ты несовершеннолетний — ничего не будет”, “там не наркотики”, “ты просто курьер” — ложное успокоение.

Риски по закону

- Незаконный оборот наркотических средств, психотропных веществ, их прекурсоров и аналогов преследуется по УК РБ (ориентир: ст. 328).
- По отдельным составам, связанным со сбытом, уголовная ответственность возможна с 14 лет.
- Последствия могут быть крайне тяжёлыми: судимость, лишение свободы, проблемы с учёбой, работой, семьёй и будущим.

10.3. Курьеры наличных

- “Забери деньги у клиента”, “передай пакет”, “положи в банкомат”, “получи процент” — это может быть часть мошенничества против пожилых людей или других жертв.
- Курьер часто виден на камерах, оставляет маршрут, телефон, переписку, банковские операции. Организаторы остаются в тени, а курьер становится первым, кого находят.
- Нельзя соглашаться даже “один раз”.

10.4. Крипто-переводы “для клиента”

- Схема: на вашу карту приходят деньги, вы покупаете токены/криптовалюту и переводите на чужой кошелёк.
- Или наоборот: вы принимаете криптовалюту и переводите белорусские рубли/валюту на чужие карты.
- Такие операции могут использоваться для вывода похищенных денег и обхода контроля.
- В РБ операции с цифровыми знаками имеют специальные правила. Нарушения могут влечь административную, налоговую и иную ответственность (ориентир: ст. 12.36 КоАП, ст. 13.3 КоАП, налоговые нормы — по ситуации).

10.5. Продажа аккаунтов, SIM-карт, электронных кошельков

- Аккаунт, оформленный на вас, могут использовать для обмана людей, рассылки фишинга, регистрации кошельков, вывода денег, угроз и шантажа.
- SIM-карта может использоваться для подтверждения операций, регистрации аккаунтов и получения кодов.
- Если аккаунт связан с вашим номером, документами или лицом, вопросы придут к вам.
- Не продавайте и не передавайте доступы даже за небольшую сумму.

10.6. Фиктивные ИП, фирмы и “номинальный директор”

- Предложение “открой ИП/ООО, мы всё сделаем, тебе процент” опасно.
- На оформленное на вас лицо могут повесить долги, налоги, незаконные операции, фиктивные сделки, вывод денег.
- Нельзя подписывать документы, договоры, доверенности и банковские заявления, если вы не понимаете реальной деятельности.

10.7. Фишинговые задания и “работа оператором”

- Иногда предлагают писать людям по готовому тексту, размещать объявления, делать сайты-клоны, обзванивать “клиентов”, собирать коды, проверять карты.
- Даже если вы “только переписывались”, это может быть часть мошенничества.
- Не выполняйте задания, где нужно вводить людей в заблуждение, скрывать правду, собирать данные карт и коды.

10.8. Реклама незаконных каналов

- Расклейка QR-кодов, граффити, публикация ссылок, репосты, привлечение людей в закрытые каналы могут быть не безобидной рекламой.
- Если канал связан с наркотиками, мошенничеством, фишингом, незаконными ставками или продажей данных, распространитель также рискует.
- Не рекламируйте то, чего не понимаете и что скрывает владельцев.

10.9. Как отказаться и защитить себя

11. Не вступайте в спор с “куратором”. Коротко: “Не интересно”.
12. Не отправляйте документы, карту, селфи, адрес.
13. Сделайте скриншоты предложения, никнейма, ссылки, номера.
14. Заблокируйте контакт.
15. Если угрожают — сообщите взрослым, администрации учебного заведения, в 102.
16. Если уже передали данные — срочно обратитесь в банк, заблокируйте карту и смените пароли.

БЛОК 11. Инвестиции, финансовые пирамиды, ставки и “гарантированный доход”

11.1. Красные флаги

- обещают высокий доход без риска;
- давят: “мест осталось мало”, “вход только сегодня”;
- просят привлечь друзей и родственников;
- не объясняют, откуда берётся прибыль;
- деньги переводятся на личную карту, криптокошелёк или через анонимный сервис;
- “аналитик” просит установить AnyDesk/TeamViewer или показать экран;
- для вывода прибыли требуют оплатить налог, комиссию, страховку, верификацию;
- предлагают взять кредит для инвестиций.

11.2. Пирамиды и псевдоинвестиции

- Пирамида платит старым участникам за счёт новых, а не за счёт реальной прибыли.
- Пока деньги поступают, кажется, что всё работает. Когда поток новых участников заканчивается, выплаты прекращаются.
- Ранний “успешный вывод” часто делают специально, чтобы человек внёс больше или привёл близких.
- Не вкладывайте деньги, если не понимаете продукт, риски, юридическое лицо, договор и способ вывода.

11.3. Ставки, казино, “договорные матчи”

- “100% прогноз”, “договорной матч”, “бот обыгрывает казино” — типичные приманки.
- Сначала могут показать маленькую прибыль, потом попросить пополнить больше.
- Азарт и желание отыграться приводят к долгам.
- Нельзя брать кредиты, продавать вещи или занимать деньги для ставок.

БЛОК 12. Личные данные, документы и приватность

12.1. Почему личные данные ценны

- По данным из соцсетей мошенник может сделать звонок убедительным: назвать школу, родственников, поездки, покупки, место работы.
- Фото паспорта может использоваться для регистрации аккаунтов, попыток получения услуг, шантажа.
- Номер телефона и дата рождения помогают восстанавливать доступы и подбирать ответы на секретные вопросы.

12.2. Что не публиковать

- паспорт, водительское удостоверение, студенческий/ученический билет с данными;
- банковские карты, чеки с QR-кодами, билеты, посадочные талоны;
- адрес проживания, график отсутствия дома;
- фото детей с привязкой к школе, секции, маршруту;
- много аудио и видео с голосом, если в этом нет необходимости;
- документы о доходах, кредитах, недвижимости, наследстве.

12.3. При отправке документов

☐ Понимаю, кому отправляю и зачем.

☐ Есть официальный канал или защищённый кабинет.

☐ Можно закрыть лишние данные, если они не нужны.

☐ На копии можно написать цель и дату: “Только для ...”.

☐ Не отправляю документы в анонимный чат или неизвестному работодателю.

☐ Сохраняю доказательства передачи и условия обработки данных.

БЛОК 13. Дети, подростки и школьники

13.1. Главные риски для школьников

- поиск “лёгкого заработка” в Telegram и TikTok;
- передача карты или аккаунта за деньги;
- участие в переводах, обналичивании, крипто-операциях;
- закладки и “курьерские” задания;
- скачивание приложений и игр из сомнительных источников;
- покупки в играх, скины, донаты, фальшивые розыгрыши;
- шантаж интимными фото или перепиской;
- взлом аккаунтов друзей и просьбы о переводах.

13.2. Простые правила для школьника

Если страшно сказать родителям
Скажи учителю, школьному психологу, классному руководителю, старшему родственнику или другому взрослому, которому доверяешь. Молчание почти всегда делает проблему хуже.

- Не называй коды из SMS и push никому, даже другу.
- Не давай карту, телефон, SIM-карту, аккаунт, пароль.
- Не принимай деньги на свою карту для других.
- Не бери пакеты и посылки у незнакомых людей.
- Не ходи по адресам по заданиям из чата.
- Не устанавливай приложения по ссылке “куратора”.
- Не отправляй фото паспорта, карты, лица с документом.
- Если предлагают быстрые деньги — покажи взрослым до ответа.

13.3. Родителям и педагогам

- Не ограничивайтесь фразой “не общайся с мошенниками”. Разберите конкретные сообщения и примеры.
- Договоритесь: ребёнок может прийти с любой ошибкой без немедленного наказания. Сначала безопасность, потом разбор.
- Настройте лимиты на детской карте и уведомления родителю.
- Проверяйте приложения, подписки, активные сессии, привязанные карты.
- Объясните правовые последствия дропперства и закладок простыми словами.
- Разберите, что “я просто помог” не означает “я не отвечаю”.

БЛОК 14. Пожилые родственники

14.1. Почему пожилые люди в зоне риска

- Мошенники используют уважение к “официальным органам”, страх за детей и внуков, доверие к звонкам.
- Пожилого человека могут долго держать на линии, не давая позвонить семье.
- Часто используют курьеров, наличные, “замену денег”, “проверку купюр”, “ДТП родственника”.

14.2. Домашние правила

☐ На видном месте записаны телефоны детей/внуков, банка и 102.

☐ Есть правило: наличные никому не передавать без звонка родственнику.

☐ Есть кодовое слово семьи.

☐ Крупные переводы и снятие наличных обсуждаются с близким человеком.

☐ На карте установлены лимиты и уведомления.

☐ Пожилой родственник знает: банк и милиция не присылают курьера за деньгами.

14.3. Что сказать пожилому человеку простыми словами

- “Если звонят и пугают — клади трубку. Хороший сотрудник не обидится, мошенник будет давить”.
- “Код из SMS — как ключ от квартиры. Его нельзя давать даже работнику банка”.
- “Безопасных счетов по телефону не бывает”.
- “Если говорят, что внук попал в беду, сначала позвони внуку или нам”.
- “Курьер за деньгами от банка или милиции — это обман”.

БЛОК 15. Личный бюджет, расходы и сбережения

15.1. Зачем это относится к безопасности

- Человек без учёта денег чаще берёт срочные кредиты, верит “быстрым заработкам” и сложнее замечает списания.
- Финансовая подушка помогает не принимать опасные решения из-за нехватки денег.
- Понимание расходов снижает риск долговой ловушки.

15.2. Расходы

- Ведите учёт хотя бы по крупным категориям: обязательные платежи, еда, транспорт, связь, здоровье, обучение, развлечения, долги, накопления.
- Проверяйте подписки и автоплатежи.
- Перед крупной покупкой берите паузу 24 часа.
- Сравнивайте цену, гарантию, доставку и условия возврата.
- Не покупайте “на эмоциях” после рекламы, стресса или давления продавца.

15.3. Подушка безопасности

- Минимальная цель — сумма на 1 месяц обязательных расходов. Хорошая цель — 3–6 месяцев.
- Храните резерв отдельно от ежедневной карты.
- Не вкладывайте подушку в рискованные инструменты.
- Пополняйте резерв сразу после дохода.
- Используйте резерв только для реальных непредвиденных ситуаций.

15.4. Планирование целей

☐ Цель записана конкретно: что, сумма, срок.

☐ Понятен ежемесячный взнос.

☐ Деньги на цель отделены от ежедневных трат.

☐ Цель пересматривается раз в 3–6 месяцев.

☐ Рискованные вложения не заменяют накопления на важные цели.

БЛОК 16. Что делать, если ошибка уже произошла

Не удаляйте доказательства
Скриншоты, номера, ссылки, чеки, записи звонков, никнеймы, адреса кошельков и переписка могут быть важны для банка и правоохранителей.

16.1. Сообщили код, пароль или данные карты

17. Сразу заблокируйте карту через приложение или горячую линию банка.
18. Смените пароль от банка, почты, мессенджеров и соцсетей.
19. Завершите все активные сессии на неизвестных устройствах.
20. Проверьте, не добавлены ли новые устройства, номера, карты, доверенные получатели.
21. Позвоните в банк и зафиксируйте обращение.
22. Обратитесь в 102, если есть списание, попытка кредита, угрозы или вовлечение в схему.

16.2. Перевели деньги

23. Позвоните в банк немедленно. Спросите о возможности остановки, возврата или оспаривания операции.
24. Сохраните чек и реквизиты получателя.
25. Сделайте скриншоты переписки, ссылки, профиля, номера телефона.
26. Подайте заявление в милицию.
27. Предупредите близких: мошенники могут использовать ваши контакты.

16.3. Передали карту или реквизиты

28. Заблокируйте карту и доступ к счёту.
29. Сообщите в банк, что реквизиты могли попасть третьим лицам.
30. Смените пароли и проверьте активные устройства.
31. Не пытайтесь “договориться” с куратором и не выполняйте новые задания.
32. Если были операции — сохраните историю и обратитесь за правовой помощью/в 102.

16.4. Установили подозрительное приложение

33. Отключите интернет на устройстве.
34. С другого устройства смените важные пароли.
35. Заблокируйте карты и позвоните в банк.
36. Удалите приложение. Если есть сомнения — обратитесь к специалисту или сбросьте устройство после сохранения данных.
37. Проверьте переадресацию звонков/SMS и настройки SIM.

16.5. Ребёнок попал в схему

38. Сначала остановите дальнейшие действия: карты, чаты, встречи, переводы.
39. Не кричите и не заставляйте удалять переписку.
40. Сохраните доказательства.
41. Свяжитесь с банком, если использовались карты/счета.
42. Обратитесь за консультацией к юристу и/или в правоохранительные органы, особенно при угрозах, наркотиках, переводах денег.
43. Сообщите школе, если вовлечение шло через учеников или школьные чаты.

БЛОК 17. Ежедневные, ежемесячные и семейные чек-листы

17.1. Ежедневно

☐ Не перехожу по подозрительным ссылкам.

☐ Не называю коды и пароли.

☐ Проверяю неожиданные просьбы о деньгах через звонок.

☐ Не принимаю решения о переводах под давлением.

☐ Смотрю уведомления банка о списаниях.

17.2. Раз в неделю

☐ Проверить операции по картам.

☐ Проверить баланс онлайн-карты и лимиты.

☐ Проверить новые подписки и автоплатежи.

☐ Удалить подозрительные письма и сообщения, не открывая вложения.

☐ Обсудить с семьёй один новый пример мошенничества.

17.3. Раз в месяц

☐ Проверить активные устройства в почте, мессенджерах, соцсетях, банке.

☐ Проверить приложения на телефоне и их разрешения.

☐ Сменить слабые или повторяющиеся пароли.

☐ Проверить бюджет: доходы, расходы, долги, накопления.

☐ Проверить лимиты карт и уведомления.

☐ Поговорить с детьми и пожилыми родственниками о новых схемах.

17.4. Раз в полгода

☐ Проверить кредитную историю.

☐ Обновить семейное кодовое слово.

☐ Пересмотреть финансовые цели и подушку безопасности.

☐ Проверить, какие персональные данные доступны в интернете.

☐ Сравнить условия банковских продуктов и отключить ненужные.

БЛОК 18. Полезные контакты и ресурсы в Республике Беларусь

- 102 — милиция. Звоните при мошенничестве, угрозах, вымогательстве, вовлечении в дропперство, закладки, курьерские схемы.
- Ваш банк — номер на банковской карте, в официальном приложении или на официальном сайте. Не используйте номер из подозрительного сообщения.
- Официальный чат-бот МВД в Telegram “Мы всегда рядом” — для сообщений о подозрительных действиях.

- Национальный банк Республики Беларусь: nbrb.by.
- Портал финансовой грамотности: fingramota.by.
- Национальный правовой Интернет-портал: pravo.by — актуальные редакции КоАП, УК и других актов.
- Национальный центр защиты персональных данных: cpd.by.

Короткий лист для печати: “Если звонят/пишут — что делать?”

Ситуация	Действие
Просят код из SMS/push	Не называю. Завершаю разговор.
Звонят из “банка/милиции”	Кладу трубку. Перезваниваю сам по официальному номеру или 102.
Просят перевести на “безопасный счёт”	Не перевожу. Такого способа защиты денег нет.
Просят установить приложение	Не устанавливаю. Проверяю через официальный источник.
Родственник просит деньги срочно	Перезваниваю по сохранённому номеру. Спрашиваю кодовое слово.
Предлагают лёгкий заработок через карту/переводы	Отказываюсь. Это может быть дропперство.
Просят забрать или спрятать пакет	Отказываюсь и сообщаю взрослым/102. Это может быть наркотическая схема.
Уже ошибся	Блокирую карту, меняю пароли, сохраняю доказательства, звоню в банк и 102.

Остановись. Перепроверь. Посоветуйся. Только потом действуй.