

***Беседа со старшеклассниками: финансовые мошенничества —
что это и как защититься***

Мироненкова Любовь Владимировна,

воспитатель

ЧОУ «Газпром школа Санкт-Петербург»,

г. Санкт-Петербург

Финансовые мошенничества — это преступные схемы и уловки, цель которых получить деньги, данные доступа к банковским счетам или личные данные пострадавших. Старшекласснику важно понимать основные виды мошенничества, как они работают и как не стать жертвой.

Основные виды мошенничеств

1. Фишинг

Мошенники присылают поддельные письма, SMS или сообщения в мессенджерах от имени банков, служб доставки или социальных сетей. Цель — заставить перейти по ссылке и ввести логин, пароль или данные карты.

2. Скимминг

Считывание данных с банковской карты с помощью поддельных терминалов или устройств у банкоматов. Затем данные используются для списаний или копирования карты.

3. Телефонные аферы

Звонок якобы от банка, полиции или родственников, которые просят срочно перевести деньги или сообщить код подтверждения.

4. Социальная инженерия

Манипуляция доверием: мошенник выдает себя за сотрудника школы, волонтера, работодателя или друга, чтобы получить деньги или доступ.

5. Инвестиционные и криптомошенничества

Обещания высокой доходности с маленьким риском: пирамиды, фальшивые проекты, мошеннические ICO и т. п.

6. Подделка сайтов и объявлений

Ложные интернет-магазины или объявления о продаже, где после предоплаты товар не приходит.

7. «Работа на дому» и «легкий заработок»

Объявления о быстрых заработках (рассылка спама, ввод капчи, двойная переписка), часто требуют предоплаты или использования личных данных.

Как мошенники действуют: кратко о схемах

- Создают ощущение срочности: «срочно переведите», «секретный код», «счет заблокируют».
- Подделывают внешний вид сообщений и сайтов: логотипы, адреса, номера телефонов.
- Просят сообщить коды из SMS, CVV с карты или реквизиты.
- Просят перевести деньги на «безопасный счет», номера карт в мессенджерах или криптокошельки.
- Используют эмоции: страх, жадность, стеснение.

Как распознать мошенничество: несколько очевидных фактов

- Непрошенные сообщения с просьбой о деньгах или информации.
- Ошибки в тексте, странные ссылки, адреса, не совпадающие с официальными.
- Давление: угрожают штрафами, блокировкой, требуют немедленных действий.
- Предложения «слишком хороши, чтобы быть правдой»: гарантированная прибыль, невероятные скидки.
- Требование оплачивать через анонимные методы (криптовалюта, переводы на карты частных лиц).

Практические правила безопасности

- Никогда не сообщать пароли и коды из SMS даже если звонит «банк».
- Проверять URL сайта: официальный домен банка обычно заканчивается на .ru или известный домен, без лишних символов.
- Не переходить по подозрительным ссылкам и не скачивать файлы от незнакомцев.
- Включить двухфакторную аутентификацию (2FA) в важных аккаунтах.
- Использовать антивирус и обновлять устройство.

- Не переводить деньги незнакомым людям и не использовать сервисы для перевода, если не уверены.
- При сомнениях звонить в банк по официальному номеру на карте или сайте.
- Хранить документы и данные банковских карт в безопасности.

Что делать, если вы стали жертвой

- Немедленно позвонить в банк и заблокировать карту/операции.
- Сообщить о мошенничестве в полицию и в платформу, где это произошло (соцсеть, маркетплейс).
- Сохранить все переписки, скриншоты и номера счетов для доказательств.
- Изменить пароли и проверить счета на посторонние операции.

Советы для школьников

- Не делитесь личной информацией в соцсетях (адрес, телефон, данные родителей).
- Будьте осторожны с новыми знакомствами в интернете.
- Относитесь критически к предложениям легкого заработка.
- Обсуждайте подозрительные ситуации с родителями или учителем.
- Учитесь финансовой грамотности — это защитит в будущем.

Финансовая безопасность — навык, который развивается. Чем больше вы знаете о способах мошенничества, тем меньше шансов попасться на уловки. Будьте внимательны и не торопитесь принимать решения, связанные с деньгами.

Литература

1. В. В. Кузнецов — «Финансовые мошенничества: методы, схемы, противодействие», Москва, 2018. Практическое изложение распространённых схем и мер защиты.
2. Э. А. Павлова — «Финансовая безопасность: риски и предотвращение мошенничества», Санкт-Петербург, 2019. Анализ уязвимостей в банковских и онлайн-сервисах.
3. Д. Н. Смирнов — «Социальная инженерия: как не стать жертвой», 2-е изд., 2021. Практические рекомендации по распознаванию манипуляций.