ОСТОРОЖНО, МОШЕННИКИ!

Как не стать жертвой финансового мошенничества?

Популярные схемы мошенничества:

91%

жителей России сталкивались с попытками мошенничества.

- **73%** звонки от банков и государственных органов
- **63%** предложения заработать на инвестициях
- **46%** сообщения или электронные письма с подозрительными ссылками
- **43%** сообщения или звонки с просьбами помочь родственникам или знакомым
- **28%** обман через фишинговые сайты
- **27%** мошенничество при продаже или покупке товаров в интернете

Звонок от незнакомца



Оставайтесь на связи с реальностью!

Безопасность прежде всего: не доверяйте и проверяйте!

Правила безопасности:

- Не сообщайте незнакомцам персональные данные и коды из СМС
- Положите трубку и позвоните в банк по официальному номеру. Номер указан на оборотной стороне любой карты
- Наберите номер самостоятельно, не перезванивайте обратным звонком

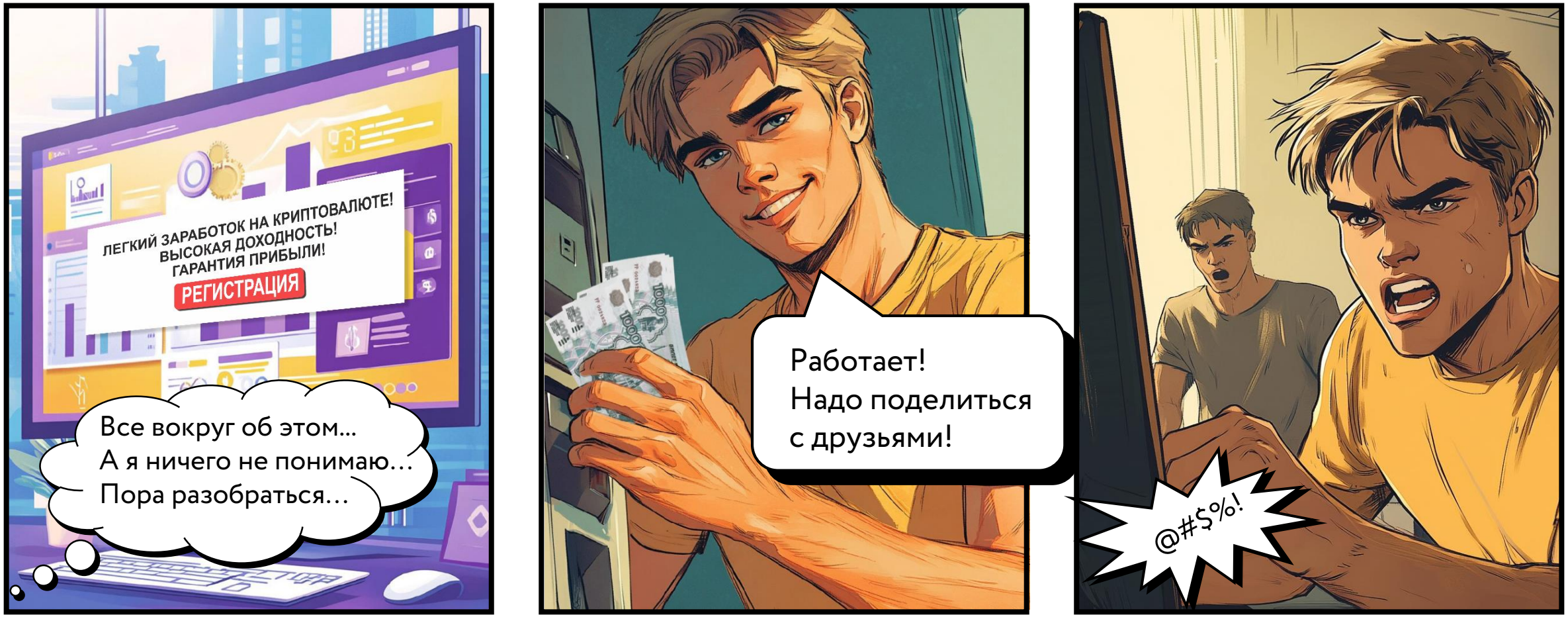


Мошенничество с инвестициями:

- Нелегальный форекс
- Псевдоброкеры
- Финансовые пирамиды

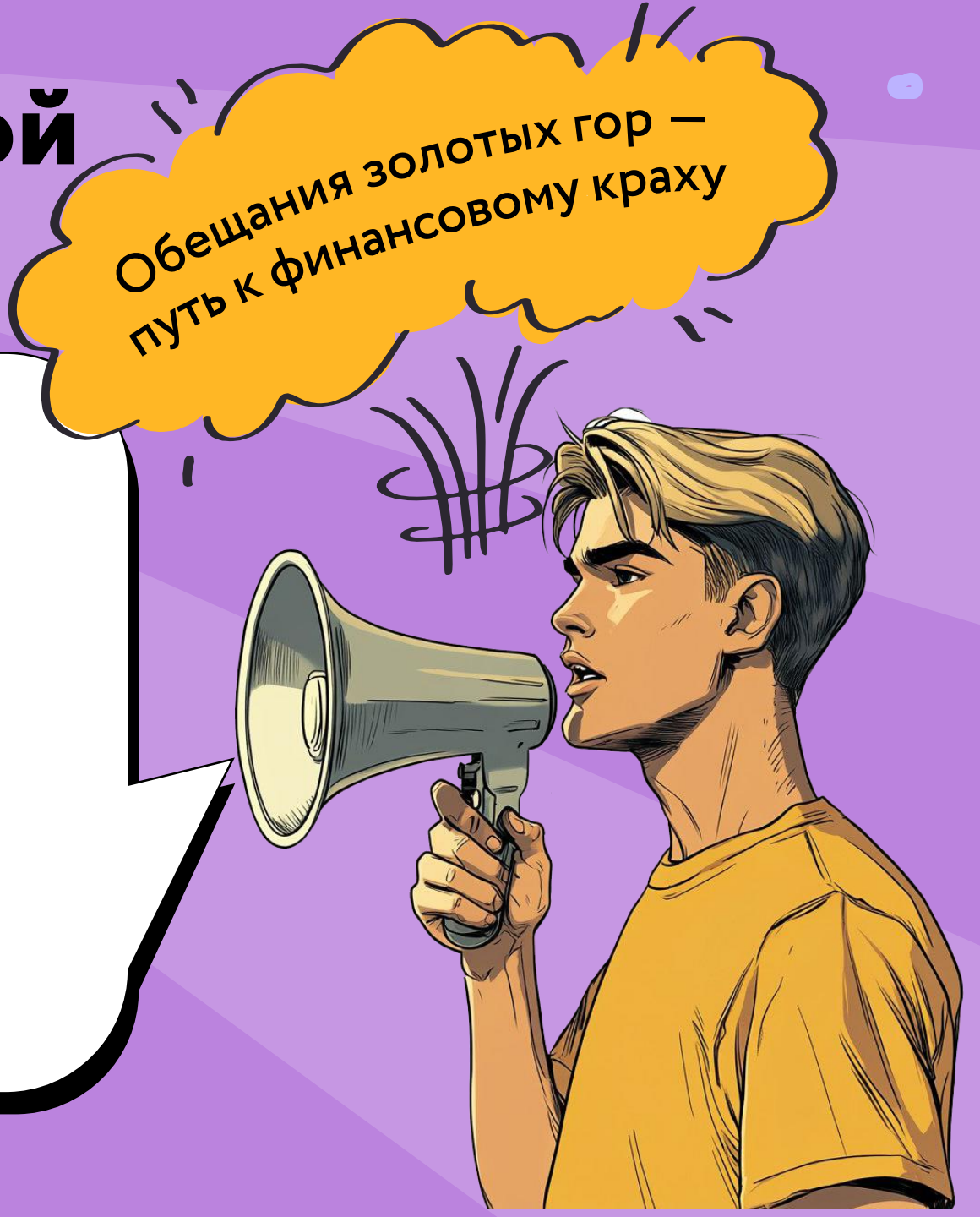


Лёгкие деньги? Нет, не слышали!



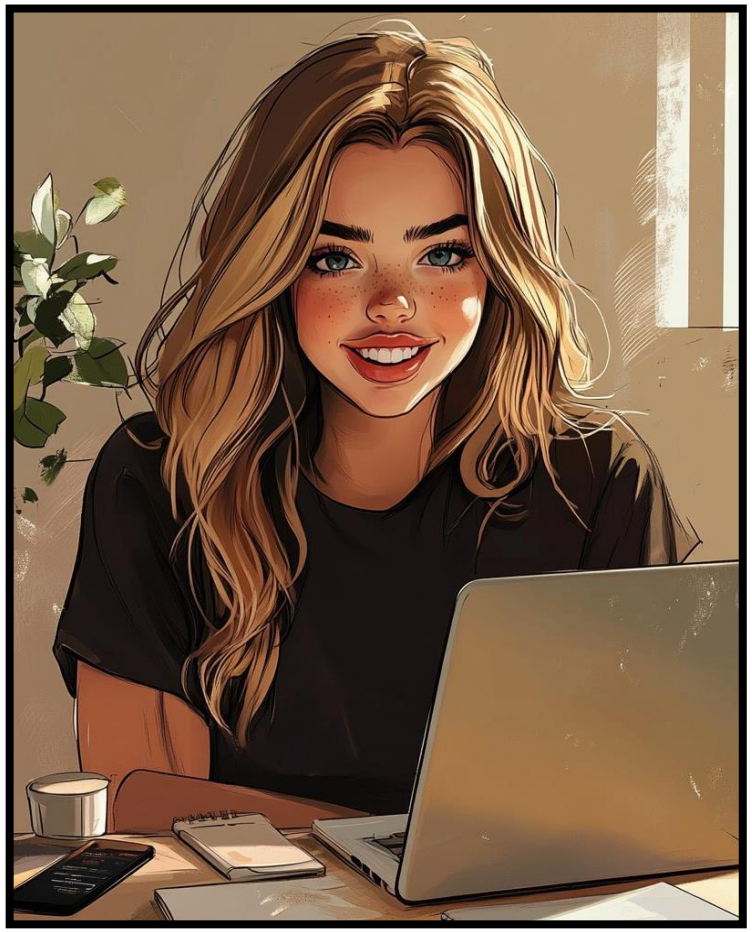
Признаки финансовой пирамиды

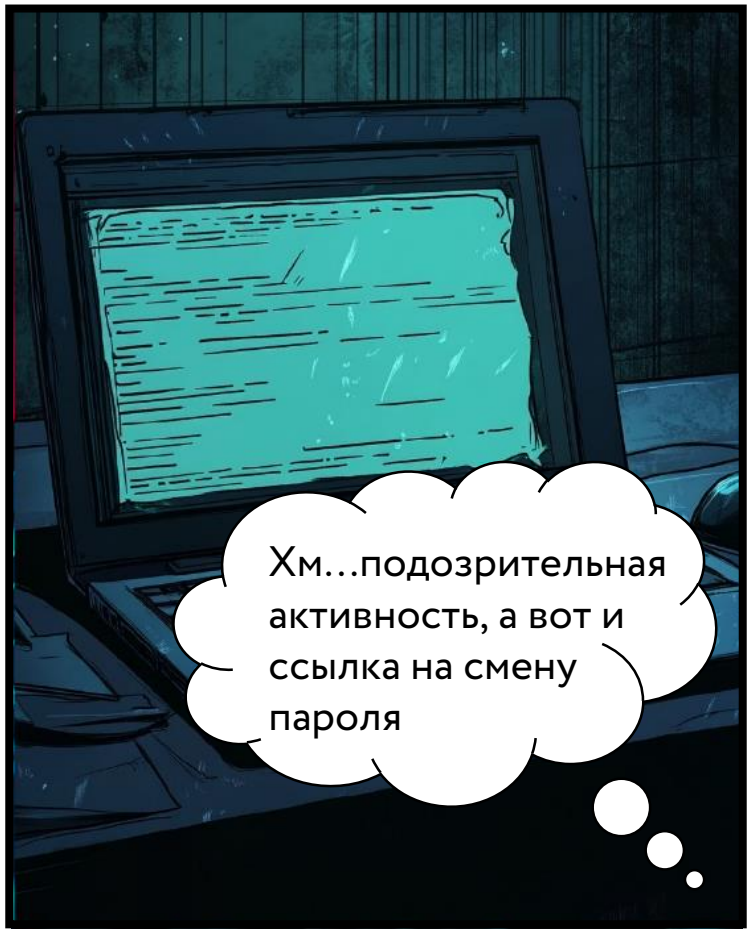
- Обещание сверхдохода
- Отсутствие информации об организации
- Агрессивная реклама
- Бонусы за привлечение друзей

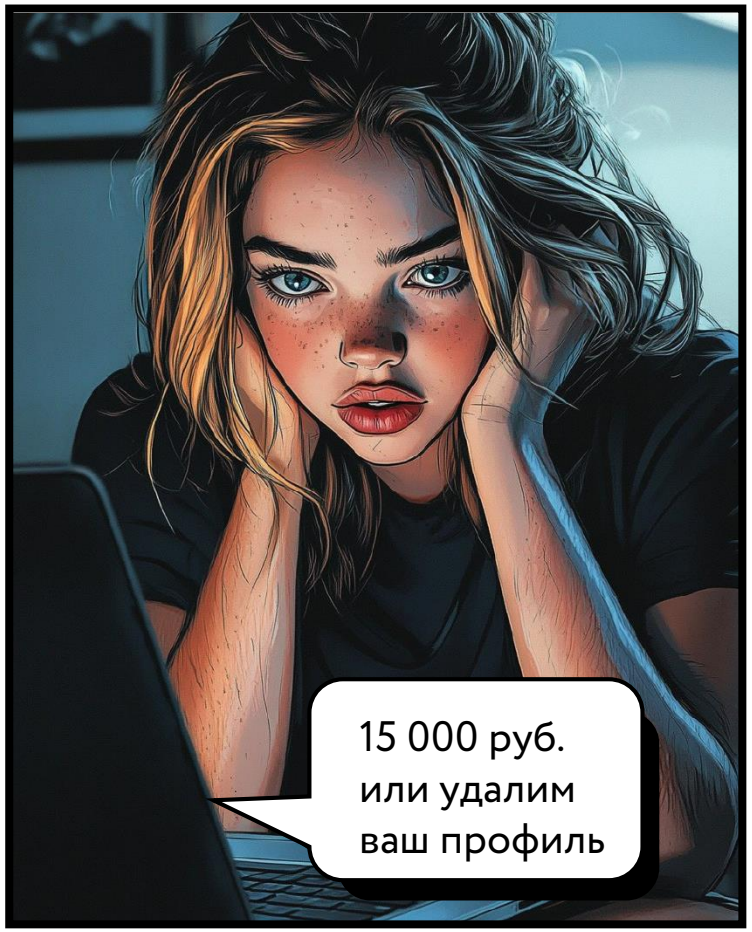


Угнать за 60 секунд

Знакомьтесь, Анна - успешный блогер







История о том, как важно проверять информацию



Правила кибергигиены

- Защитите аккаунты двухфакторной аутентификацией
- Не вводите адрес электронной почты на сомнительных сайтах
- Используйте сложные пароли
- Не переходите по прямой ссылке на другие сайты через профиль в социальной сети
- Избегайте программ накрутки подписчиков и лайков
- Если страницу или почту уже взломали, обратитесь в службу техподдержки



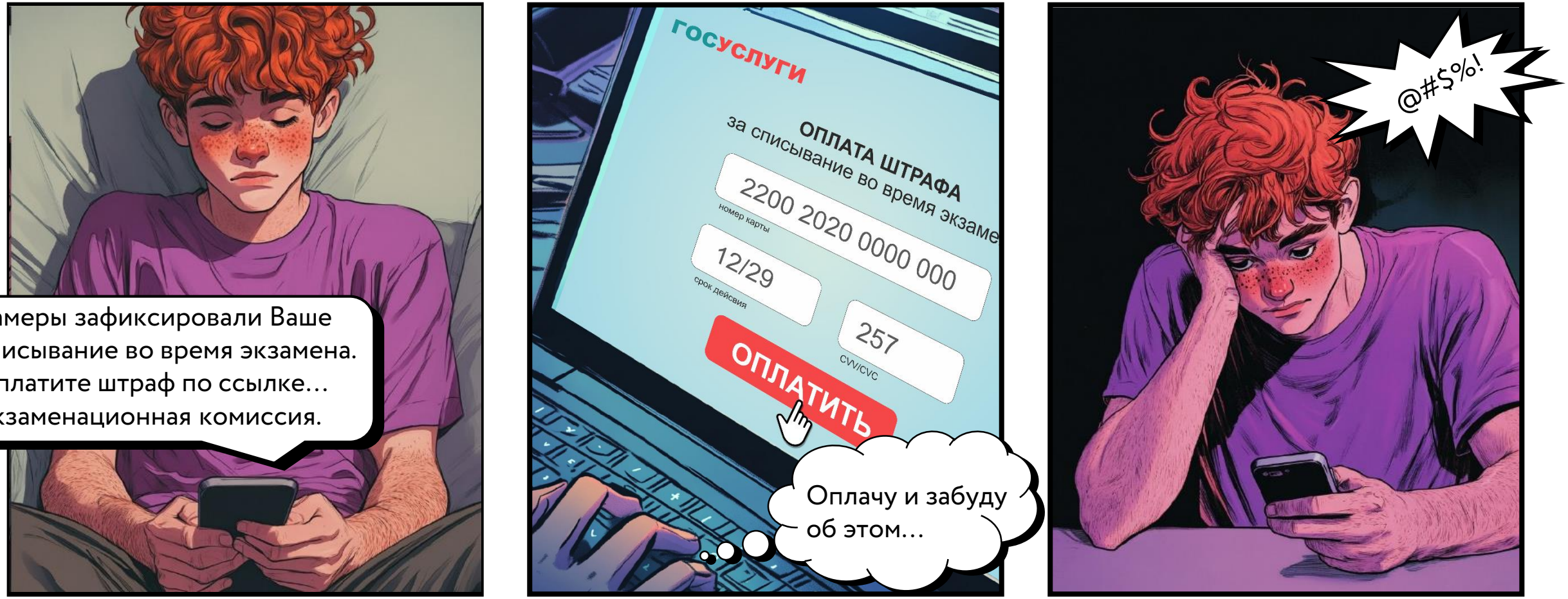
Фишинг

Вид мошенничества, при котором злоумышленники обманным путём выманивают у людей конфиденциальную информацию: личные данные, пароли, коды или реквизиты банковских карт.



Экзамен на бдительность

Тимофей только что вернулся с экзамена по обществознанию…



Сертификат на миллион

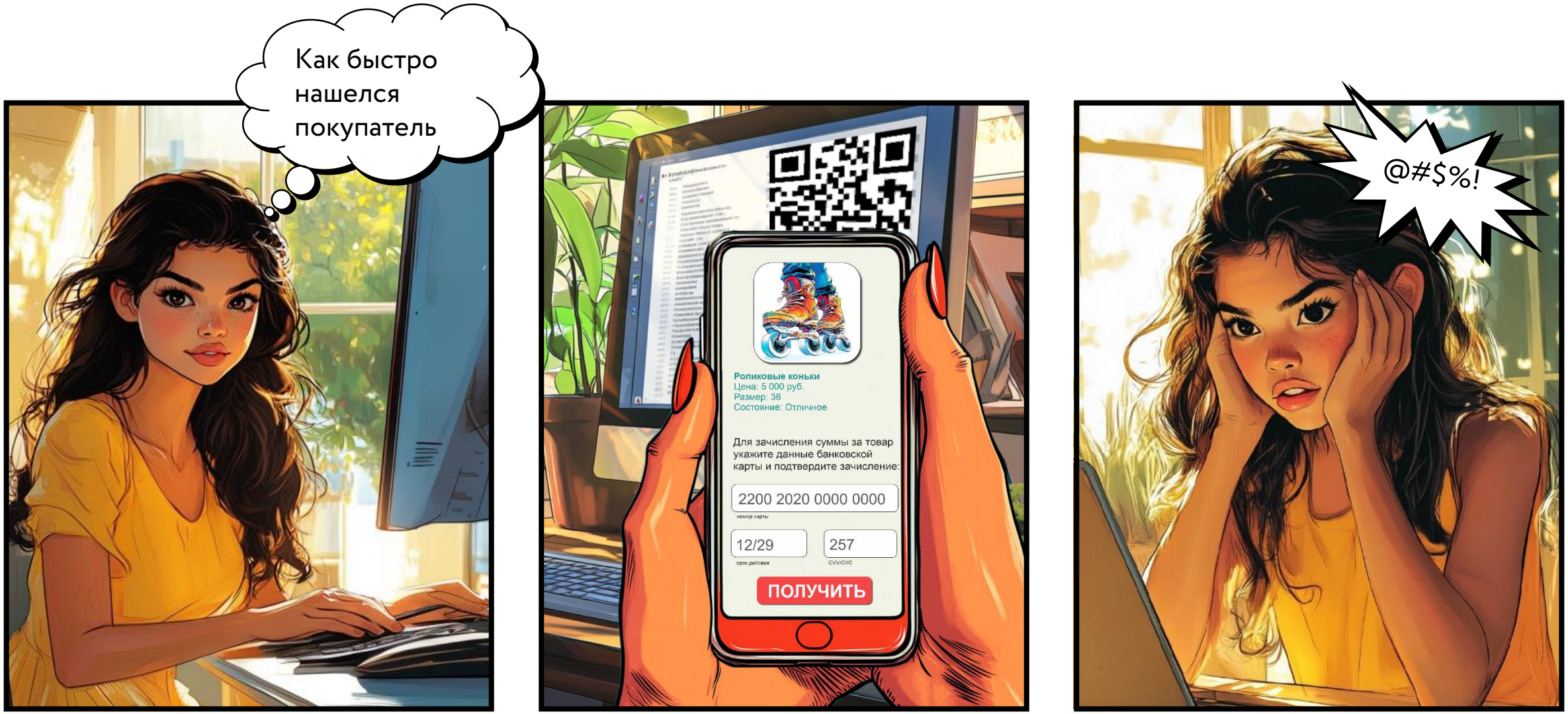


Как не попасться на удочку фишеров

- Установите антивирус и регулярно обновляйте его
- Не переходите по ссылкам из сообщений от незнакомых адресатов
- При переходе на сайт проверяйте адресную строку браузера
- Платите через безопасные страницы
- Для онлайн-покупок и оплаты услуг через интернет используйте отдельную карту

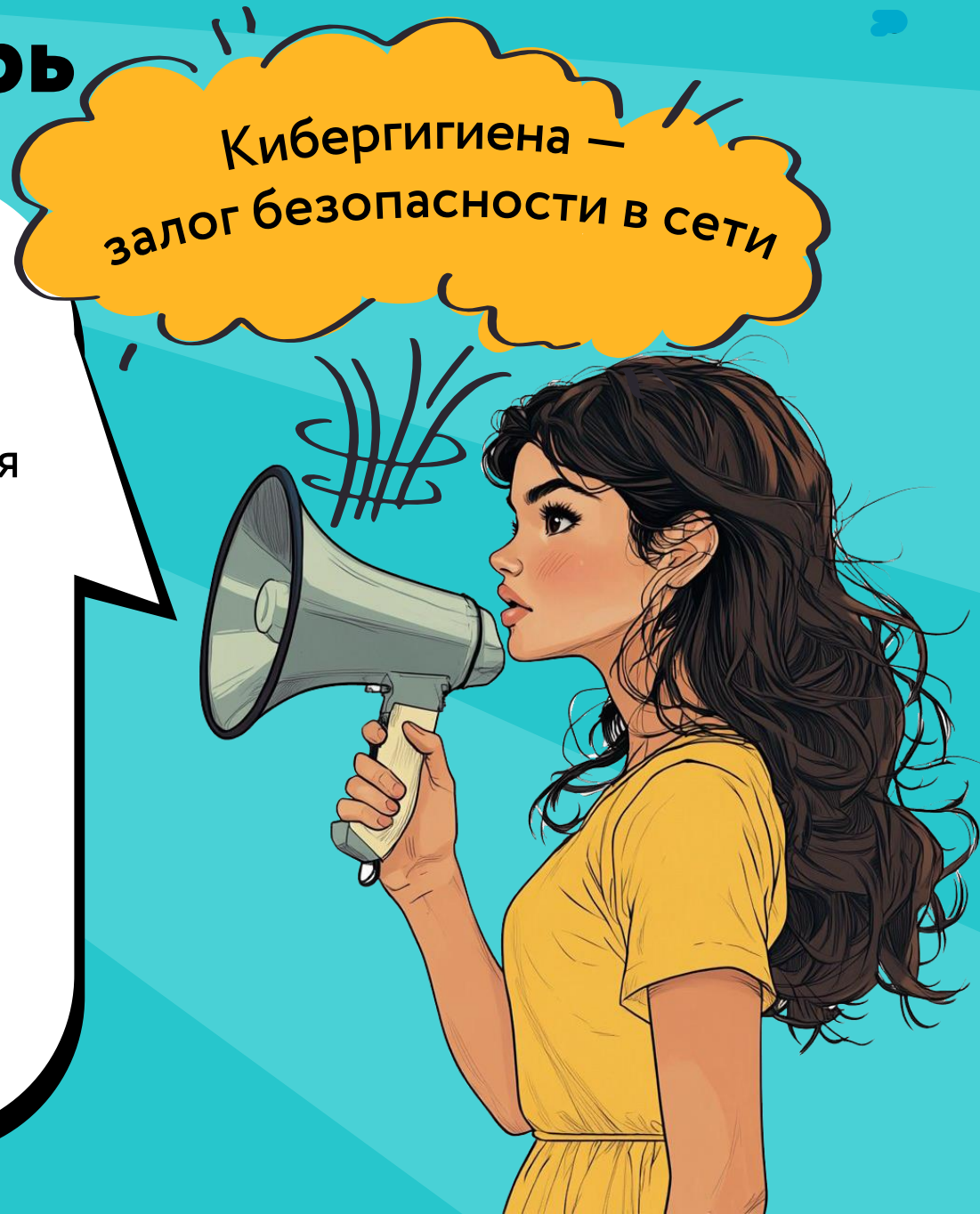


Опасные покупки



Онлайн-шопинг без потерь

- Общайтесь с продавцами и покупателями только во внутреннем чате сайта объявлений
- Оплату проводите через сервис «безопасная сделка»
- Не переходите по сторонним ссылкам, в сторонние мессенджеры и не заполняйте формы на подозрительных сайтах
- Прежде чем вводить данные на сайте, убедитесь, что это не фишинговая страница
- Никому не сообщайте полные реквизиты банковской карты



Пять признаков обмана

1. Инициатива исходит от незнакомцев
2. Внезапное предложение выгоды или угрозы
3. Давление
4. Разговор о деньгах
5. Запрос личных данных

