

# ЦИФРОВОЙ ЩИТ

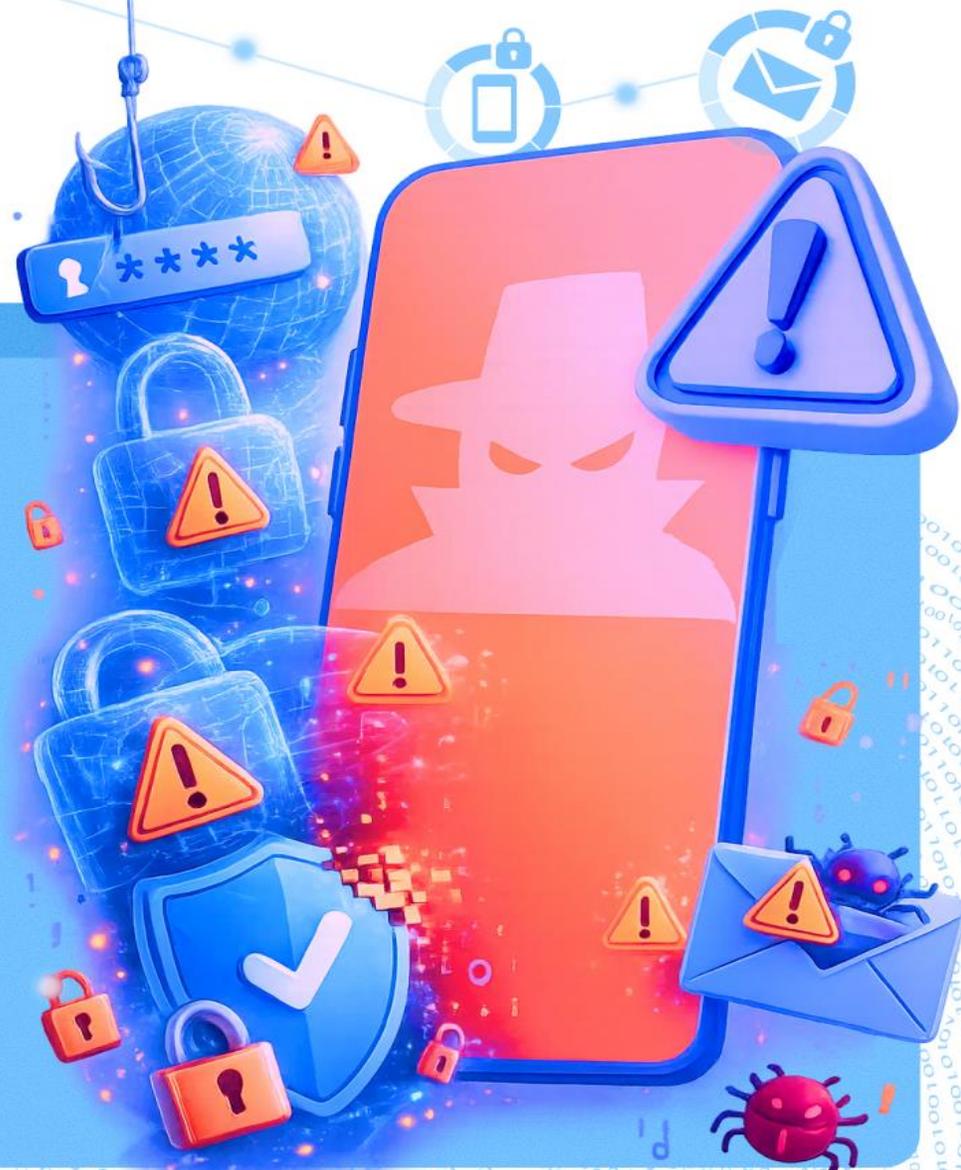
ОСНОВНЫЕ ПРАВИЛА  
БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

ЖИЗНЬ

гражданственность

5-7 классы

РАЗГОВОРЫ  
О ВАЖНОМ





# ЦИФРОВАЯ ГИГИЕНА

1

Используй сильные пароли, подобно такому **?onDggHY5cz9** – в нем сочетание заглавных и строчных букв, цифр, символов.

2

Включай двухфакторную аутентификацию. Даже если пароль утечёт, без дополнительного кода злоумышленник не получит доступ к аккаунту.

3

Устанавливай приложения только из официальных магазинов. Сторонние сайты часто распространяют программы-шпионы, которые перехватывают данные.

4

Не используй публичный Wi-Fi для банковских операций. В открытых сетях данные могут быть перехвачены.

5

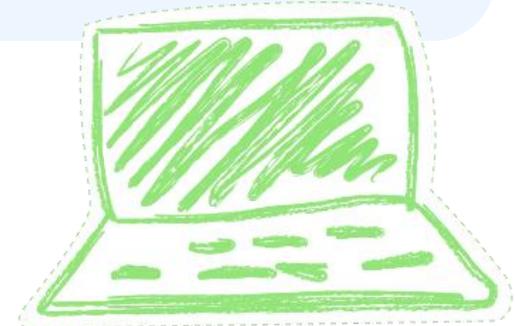
Не отправляй фото документов и коды из СМС. Сотрудники банков или ведомств никогда это не запрашивают.

6

Настрой приватность в соцсетях и мессенджерах. Ограничь круг лиц, которые видят публикации, номер телефона и твою личную информацию.

7

Не переходи по неизвестным ссылкам. Фишинговые сайты выглядят как настоящие банки или «Госуслуги», но созданы для кражи данных.



# СОХРАННОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

## НЕОБХОДИМО

- Не передавать персональные данные подозрительным операторам.
- Периодически менять пароли.
- Сделать отдельную почту для онлайн-магазинов, игровых аккаунтов и других сайтов – не ту, к которой привязаны официальные сервисы.
- Пользоваться отдельной картой для онлайн-платежей.
- Обращать внимание на ссылки и адреса сайтов.
- Пользоваться антивирусной защитой.



## ПОЧЕМУ ВАЖНО ОБЕСПЕЧИТЬ СОХРАННОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ?

### ФИНАНСОВЫЕ ПОСЛЕДСТВИЯ

Мошенник может получить доступ к банковским счетам, картам.

### УГРОЗА КОНФИДЕНЦИАЛЬНОСТИ

Мошенник может получить доступ к личным сообщениям, контактной и другой конфиденциальной информации.

# КИБЕРБУЛЛИНГ, СВАТТИНГ

## КИБЕРБУЛЛИНГ

Оскорбления и угрозы, грубые высказывания, дискриминационные комментарии, угрозы физического насилия в личных или публичных чатах.

### Как защититься?

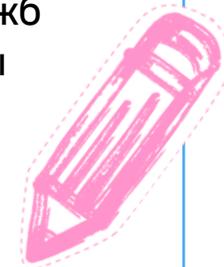
Блокируйте агрессора, не вступая в диалог. При получении угроз насилия — обратитесь в полицию.



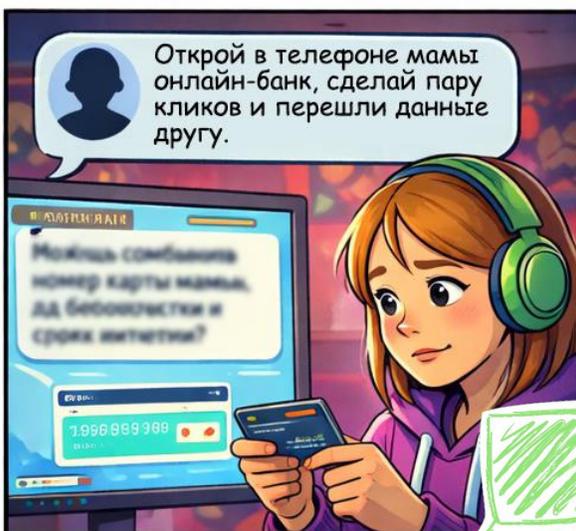
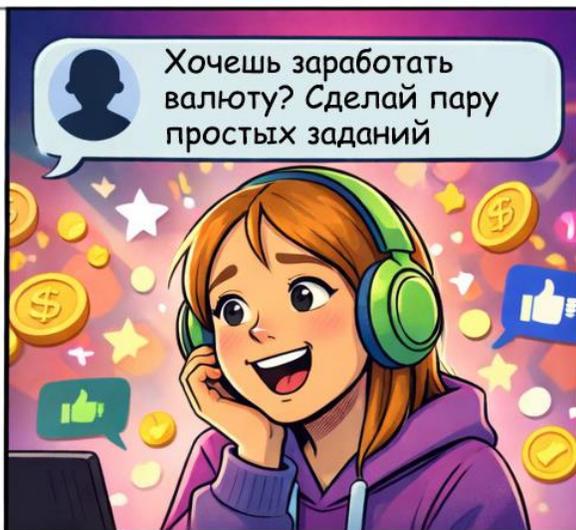
## СВАТТИНГ

Заведомо ложный вызов экстренных служб по адресу другого лица под видом угрозы жизни или террористического акта.

Преследуется по закону: уголовная ответственность по статье 207 УК РФ («Ложное сообщение об акте терроризма»)



# МОШЕННИЧЕСТВО В ДЕЙСТВИИ: РАЗБОР ТИПИЧНЫХ СХЕМ



Света увлеклась Roblox и мечтала купить редкий скин за игровую валюту.

В игровом чате написал незнакомец: «Хочешь заработать валюту? Сделай пару простых заданий».

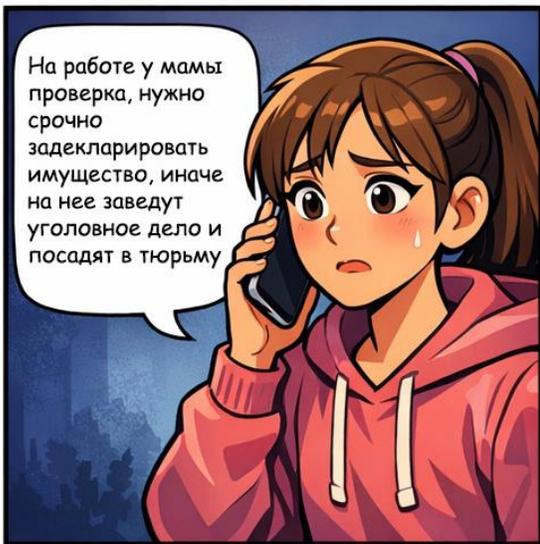
Света согласилась и выполнила. Задания оказались простыми: взять телефон мамы, открыть онлайн-банк, сделать пару кликов и переслать данные «другу».



Что произошло? Какие ошибки совершила девочка?



# МОШЕННИЧЕСТВО В ДЕЙСТВИИ: РАЗБОР ТИПИЧНЫХ СХЕМ



Маше позвонили с номера, на экране высветилось «Полиция». Женский голос представился сотрудницей отдела по борьбе с мошенничеством и спросил: «Горячева Валентина Михайловна вам кем приходится?»

— Мамой.

— На работе у мамы проверка, нужно срочно задекларировать имущество, иначе на нее заведут уголовное дело и посадят в тюрьму.

Чтобы спасти маму, нужно собрать все деньги и ценности, которые есть дома, и передать курьеру.



Теперь Маша гордится, что спасла маму. А что произошло на самом деле?



# МОШЕННИЧЕСТВО В ДЕЙСТВИИ: РАЗБОР ТИПИЧНЫХ СХЕМ



Рома получил сообщение от одноклассника с просьбой проголосовать за него в конкурсе по ссылке.

Перешел, авторизовался через соцсеть, проголосовал. Через пару часов не смог зайти в свой мессенджер, и тут же ему позвонил друг: «Ты просил у меня деньги в долг?»



Что произошло?



# АЛГОРИТМ ПРОВЕРКИ ДЛЯ ПРАКТИЧЕСКОГО ЗАДАНИЯ



ВОПРОС	ЧТО ПРОВЕРЯЕМ	КОММЕНТАРИЙ
Кто отправитель?	Знаком ли этот человек? Почему он мне пишет? Его аккаунт настоящий?	
Куда ведет ссылка?	Совпадает ли адрес с официальным? Нет ли ошибок, лишних символов?	
К чему призывают?	Слова «срочно», «немедленно», «последний шанс», угрозы, «никому не говори»	
Можно ли взять паузу?	Что будет, если подождать, посоветоваться с родителями?	
Есть ли безопасный способ?	Позвонить в банк/ написать в службу поддержки, спросить у взрослых.	

# ПРАВИЛА КИБЕРБЕЗОПАСНОСТИ



1

Никогда не передавать логины, пароли и коды из СМС для двухфакторной аутентификации третьим лицам, под каким бы предлогом их ни просили.

2

Регулярно проверять раздел «Активные сессии» или «Устройства» в настройках мессенджеров, чтобы убедиться, что к аккаунту не подключены посторонние лица.

3

С осторожностью относиться к предложениям о покупке или аренде аккаунтов. Подобные сделки в 100% случаев связаны с противоправной деятельностью.

4

Критически оценивать предложения о «легком заработке» в интернете, которые требуют выполнения простых технических действий с личными данными или социальными сетями.

5

Обязательно рассказывайте взрослым о любых подозрительных предложениях и сохраняйте скриншоты угроз — это ваши доказательства.



# ЕСЛИ ВАМ НУЖНА ПОМОЩЬ



Вы можете позвонить  
по **Единому  
общероссийскому  
телефону доверия**  
или обратиться  
в **ПОЛИЦИЮ**.



**8 800 2000 122**  
НОМЕР С МОБИЛЬНЫХ **124**  
**ТЕЛЕФОН  
ДОВЕРИЯ**  
ДЛЯ ДЕТЕЙ И ИХ РОДИТЕЛЕЙ



росмолодёжь



ИНСТИТУТ ИЗУЧЕНИЯ  
ДЕТСТВА, СЕМЬИ  
И ВОСПИТАНИЯ

# ЦИФРОВОЙ ЦИТ. ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

Постразговор к занятию из цикла «Разговоры о важном»

«Я сам / Я с командой»

## Защитник безопасности в цифровой среде

Суть:

Отработка основных правил безопасности в сети

### Школа КиберБезопасности Движения Первых

Проект дает возможность примерить роль эксперта по кибербезопасности. Все, что нужно: зайти на страницу проекта, выбрать номинацию и погрузиться в теорию на сайте (там множество полезных материалов). Затем каждый участник сможет провести свое мероприятие. Это может быть встреча с одноклассниками, беседа в первичном отделении или просто разговор с друзьями о том, как защитить себя в интернете.

### КиберКвиз Первых

В игровой форме школьники могут изучить культуру безопасности в цифровой среде, узнать какие правила и технологии обеспечивают безопасное пребывание в сети и как проверять информацию на просторах интернета.

### КиберРаскраска Первых

Персонажи раскраски становятся для ребят проводниками в мир безопасного интернета. Знакомство с основными правилами цифровой гигиены происходит через иллюстрации для раскрашивания — это позволяет учиться через игру и творчество.



Школа КиберБезопасности



КиберКвиз Первых



КиберРаскраска Первых

### Сроки проведения

25 февраля — 6 марта 2026 года

### Формат

очный

дистанционный

Всероссийские акции  
Движения Первых

