

Crime & Technology: тема урока английского языка в 7 классе

Crime & Technology: учим английский и правила безопасности в сети



Почему этот урок полезен в 7 классе

Подростки ежедневно пользуются телефонами, мессенджерами и играми, поэтому тема сразу связана с их опытом. На уроке ученики учатся понимать простые тексты, говорить о рисках и объяснять правила безопасности по-английски.



Фишинг: как выглядит опасное сообщение

Похоже на настоящее

Фишинговое сообщение может выглядеть как письмо от банка, магазина или школьного сервиса. Оно часто копирует знакомый стиль, чтобы вызвать доверие и заставить открыть ссылку.

Срочность и давление

Опасный текст обычно торопит пользователя: *your account is blocked, urgent action needed, verify now*. Такие фразы мешают спокойно проверить адрес сайта и детали сообщения.

Запрос личных данных

Мошенники часто просят *code from SMS, password* или *payment details*. Настоящие сервисы не требуют сообщать такие данные через случайные сообщения или неизвестные формы.

Ошибки в адресе

Признаком обмана может быть странный URL, лишний символ в названии сайта или необычное оформление страницы. Даже маленькая ошибка может указывать на поддельный ресурс.

Что делать

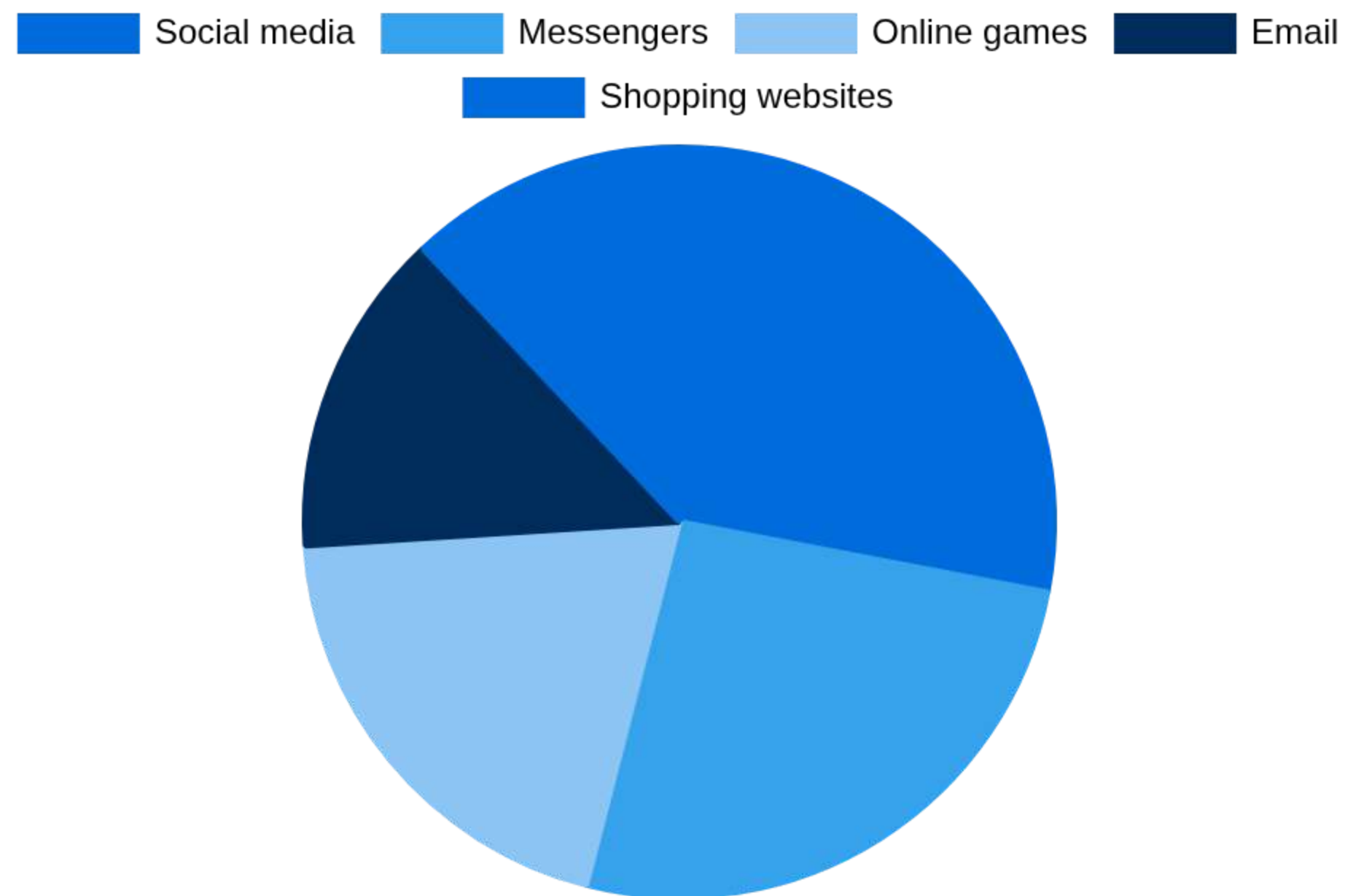
Если сообщение вызывает сомнение, не нужно нажимать link, отвечать или вводить данные. Лучше закрыть его, проверить источник отдельно и сообщить взрослому.



Где чаще всего появляются цифровые угрозы

Подростки чаще сталкиваются с риском там, где много общения и быстрых ссылок: в чатах, играх и социальных сетях.

Мессенджеры и игры дают больше всего возможностей для контакта с незнакомцами, поэтому именно там особенно важны внимательность и проверка сообщений.



Учебная схема по теме безопасности в интернете; оценочное распределение для иллюстрации урока

Как мошенники используют короткие английские фразы



Click here

Эта фраза часто ведет на поддельный сайт или вредную страницу. Она короткая, простая и заставляет действовать сразу, не проверяя адрес и источник.



Verify now

Слова verify now создают впечатление срочной проверки аккаунта. На самом деле они могут использоваться, чтобы выманить пароль, код или другие личные данные.



Win a prize

Фраза win a prize звучит привлекательно и вызывает интерес. Мошенники используют ее в сообщениях о подарках, чтобы человек открыл ссылку и оставил свои данные.



Update your details

Выражение update your details часто встречается в поддельных письмах от якобы официальных сервисов. Оно подталкивает пользователя ввести адрес, номер телефона или данные карты.

Сравнение обычной и цифровой кражи

Ситуация	Что украли	Следы
wallet theft	money, wallet	street
account hack	password, login	screenshots

Таблица показывает, что похищается в реальной и цифровой среде, как это происходит и какие следы остаются.

В цифровых случаях следов обычно больше: переписка, входы в аккаунт и данные устройства помогают восстановить события быстрее, чем при обычной краже.

Digital footprint: цифровой след пользователя

Что остается в сети

После действий в интернете сохраняются время входа, название устройства, переписка, лайки, геолокация, история просмотров и платежи. Эти данные помогают понять, что делал пользователь.

Что публикуют сами подростки

Особенно заметны фото, имя, школа, город и номер телефона. Такие сведения могут показаться безобидными, но они помогают незнакомцам узнать слишком много.

Почему это важно

Цифровой след трудно удалить полностью, потому что копии сообщений и изображений могут сохраняться на серверах и в других устройствах. Поэтому нужно думать перед публикацией.

Опасные детали профиля

Даже маленькая информация может стать полезной для мошенников: дата рождения, любимая игра, номер класса или список друзей. Чем больше данных открыто, тем выше риск.

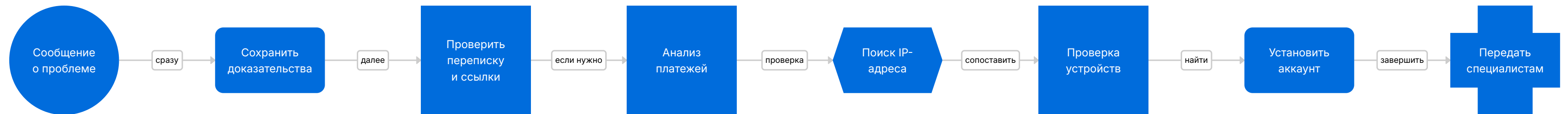
Безопасное правило

Лучше делиться только тем, что действительно нужно, и проверять настройки приватности. Это помогает уменьшить цифровой след и защитить личную жизнь.



Как расследуют интернет-преступление

Этапы работы с сообщением, перепиской и цифровыми следами



Искусственный интеллект: помощь и новые риски

Помощь в защите

ИИ может находить подозрительные операции, фильтровать спам, проверять фотографии и замечать необычные действия в аккаунтах. Это ускоряет реакцию на возможную угрозу.

1

Поддельные видео

Deerfake videos выглядят очень убедительно и могут создавать ложное впечатление, будто человек сказал или сделал что-то на самом деле не происходившее.

2

Фальшивые голоса и фото

Fake voices и realistic fake photos позволяют мошенникам имитировать знакомых людей. Из-за этого школьникам важно перепроверять сообщения, даже если отправитель кажется знакомым.

3

Главный вывод

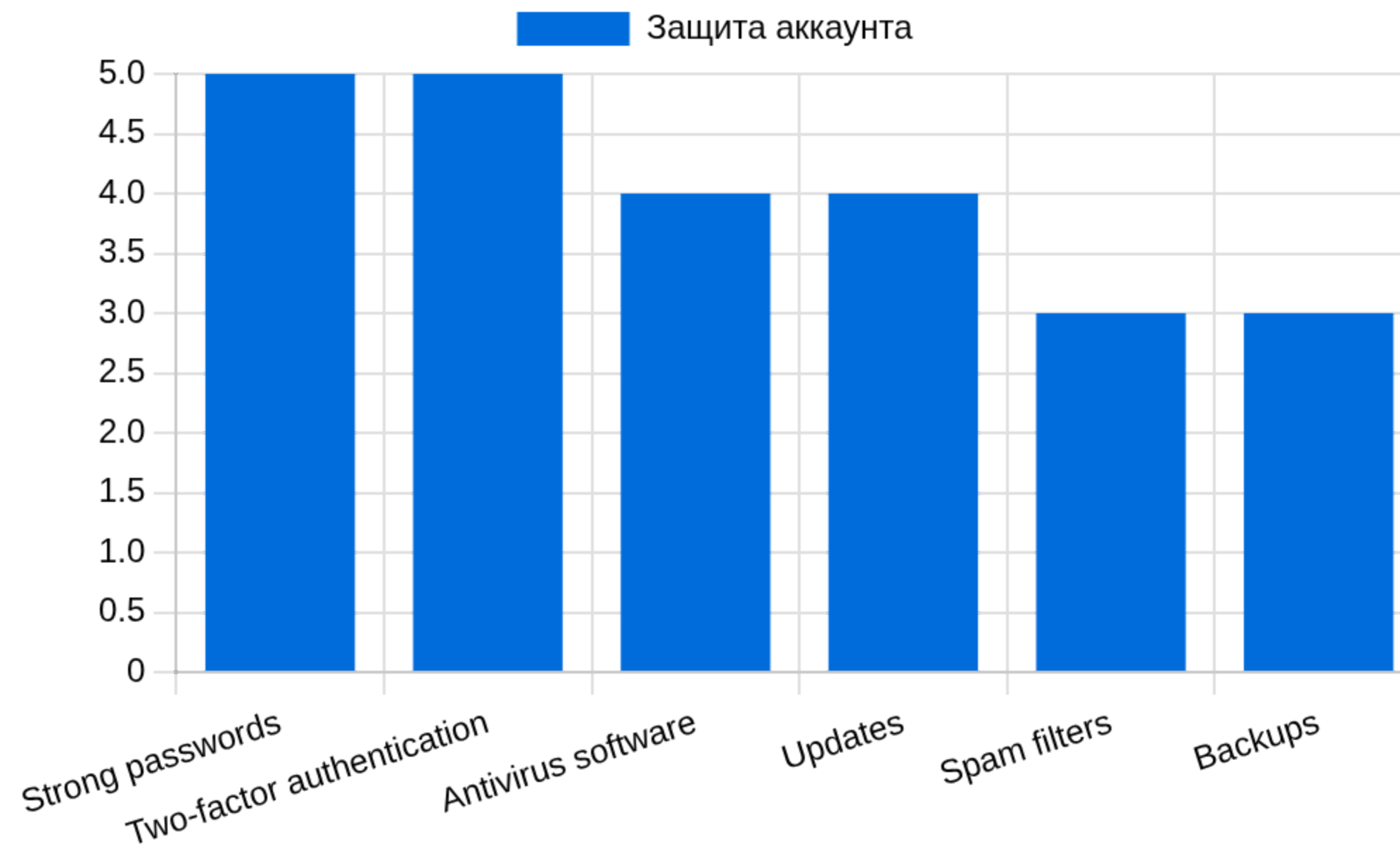
Чем точнее технологии, тем внимательнее должен быть пользователь. Если сообщение вызывает сомнение, лучше остановиться, проверить источник и не делиться личными данными.

4

Способы защиты аккаунтов

Надёжные меры работают лучше вместе: один пароль легко узнать, а дополнительные настройки снижают риск взлома и потери доступа к аккаунту.

Самые сильные меры для школьников — уникальные пароли и двухфакторная защита; обновления тоже важны, потому что закрывают уязвимости.



Biometrics: удобство и ограничения

Быстрый вход

Отпечаток пальца и распознавание лица помогают быстро открыть телефон без длинного пароля. Это удобно, когда устройство нужно разблокировать часто и без лишних действий.

Ограниченная замена

Если пароль можно изменить, то биометрические данные сменить намного труднее. Поэтому при утечке отпечатка или изображения лица риск остаётся надолго.

Личные данные

Биометрия связана с персональной информацией, поэтому её нельзя передавать посторонним или сохранять в ненадёжных приложениях. Важно понимать, где и как эти данные используются.

Нужна защита вместе

Биометрия не заменяет осторожность: полезны блокировка экрана, обновления и проверка приложений. Лучше рассматривать её как дополнительный способ защиты, а не единственный.



Правила безопасного поведения в сети на английском языке

Тема	Safe action	Unsafe action
password	use strong password	share password
link	check address	click unknown link
personal data	keep private	publish school/home
code/contact	ask adult	send code / reply

Материалы урока по теме crime & technology

Сравнение безопасных и опасных действий помогает запомнить полезные английские фразы must / must not, should / should not в реальных ситуациях.

Безопасное поведение в сети сводится к трём привычкам: не делиться секретами, проверять адреса и не отвечать незнакомцам.

Cyberbullying: основные проявления



Оскорбления

Обидные сообщения в чате или комментариях могут быстро повторяться и усиливаться. Даже короткая фраза способна задеть человека, если её видят многие одноклассники.



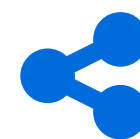
Угрозы

Цифровая травля часто включает угрозы и давление, чтобы заставить человека молчать или подчиниться. Такие сообщения важно сохранять как доказательство и сразу сообщать взрослым.



Фейковые аккаунты

Ложные профили используют чужие фото и имена, чтобы обмануть или высмеять человека. Они помогают скрыть автора, но цифровые следы всё равно могут остаться.



Распространение фото

Пересылка личных фотографий без разрешения нарушает границы и может причинить серьёзный вред. Чем быстрее остановить распространение, тем меньше людей увидят материал.



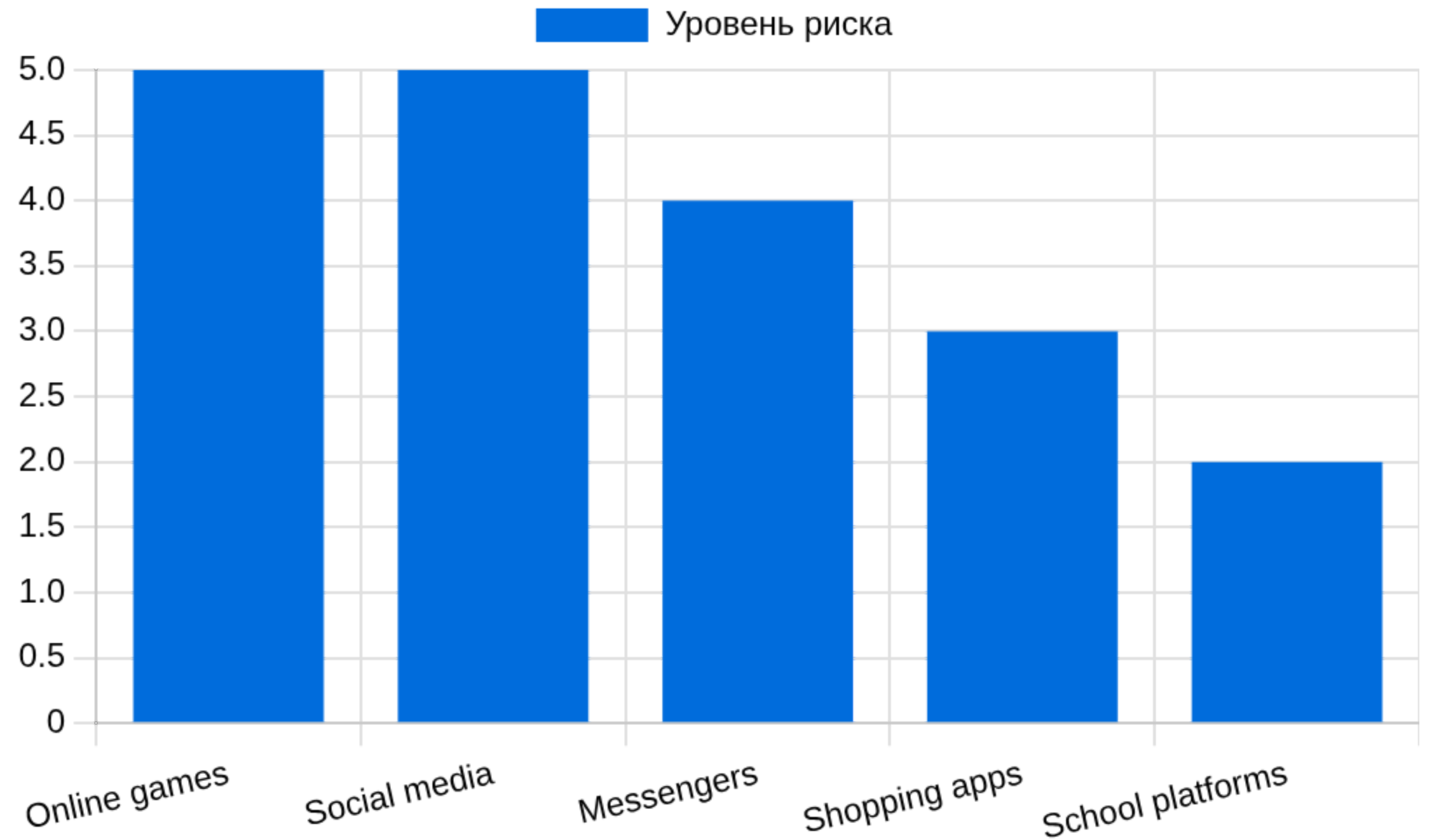
Что делать

Самые важные действия — report, block, save evidence и ask for help. Эти слова полезно знать на английском, потому что они описывают понятные шаги защиты.

Где подростки чаще сталкиваются с риском

Опасность растёт там, где легко написать незнакомцу, получить ссылку или перейти в личный чат. В играх и соцсетях это происходит особенно быстро.

Игры и социальные сети дают самый высокий риск, а значит, там особенно важно не делиться кодами, фото и личными данными.



Что делать при подозрении на мошенничество

Последовательность действий при подозрительном сообщении или ссылке.



Даже одно опасное действие в сети может привести к серьёзным последствиям, потому что сообщения, аккаунты и файлы оставляют цифровой след.

3

**основных цифровых
правонарушения особенно опасны
для школьников: мошенничество,
взлом аккаунтов
и распространение вредоносных
программ.**

Как технологии помогают полиции и экспертам

1. Камеры и места

Камеры наблюдения помогают восстановить маршрут человека и сопоставить место события со временем. Это особенно полезно, когда нужно проверить, где именно произошёл инцидент.

2. Базы данных

Проверка по базам данных позволяет находить совпадения между именами, номерами и другими сведениями. Так специалисты быстрее связывают разные эпизоды в одно дело.

3. Платежи и устройства

Анализ платежей и проверка устройств показывают, куда были отправлены деньги и с какого телефона или компьютера выполнялось действие. Эти следы часто оказываются решающими.

4. Удалённые файлы

Восстановление удалённых файлов помогает вернуть переписку, фото или документы, которые могли быть спрятаны или удалены. Это даёт экспертам дополнительные доказательства.



Полезные технологии защиты: что они предотвращают

Технология	What it protects against	How it helps
password manager	weak passwords	stores unique passwords
antivirus	harmful files	blocks threats
updates	security holes	fixes vulnerabilities
backup	file loss	saves copies
two-factor authentication	stolen password	adds extra step

Сводная таблица показывает, какие угрозы закрывают базовые цифровые инструменты и почему они особенно полезны для школьников.

Простые инструменты защиты закрывают самые частые риски: слабые пароли, вредоносные файлы, уязвимости и потерю данных.

Итог урока: английский язык помогает говорить о безопасности в цифровом мире

На уроке ученики увидели, что слова crime, scam, account, data, protect и report нужны не только для чтения текстов, но и для безопасного поведения в интернете.