РАБОЧИЙ ЛИСТ ДЛЯ ШКОЛЬНИКОВ

БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

каменный город

КИБЕР-ОСТОРОЖНОСТЬ: СОВЕТЫ ПО ОНЛАЙН-БЕЗОПАСНОСТИ

Запомни!

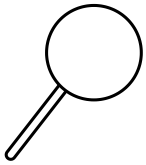
💡 Интернет помнит всё — удалённые фото и сообщения можно восстановить.

💡 Анонимность в сети — миф, всегда можно вычислить, кто писал сообщения или публиковал посты.

💡 Если что-то смущает — спроси у взрослых.

ПАРОЛИ И НАСТРОЙКИ ВАЖНЫ.

Подбирай сильные пароли и никогда не давай их никому. Также регулярно проверяй настройки конфиденциальности.

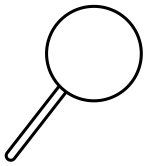


СЛЕДИ ЗА ТЕМ, ЧТО СКАЧИВАЕШЬ.

Некоторые программы и приложения содержат вредоносный код, чтобы украсть информацию. Скачивай файлы только с надежных сайтов.

БУДЬ ОСТОРОЖНЕЕ С СОЦИАЛЬНЫМИ СЕТЯМИ.

Не делись личной информацией и не отправляй личные фото незнакомцам.



ПОКУПАЙ БЕЗОПАСНО.

Совершай покупки на безопасных веб-сайтах, читай отзывы и задавай вопросы.

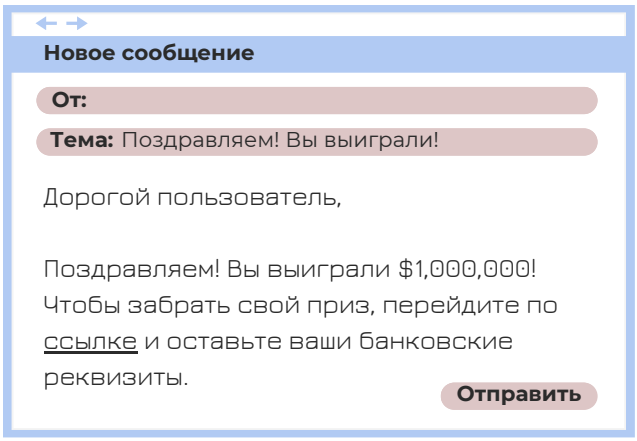
ДУМАЙ ПЕРЕД ПОСТОМ.

Если не хочешь, чтобы это увидели члены семьи, друзья или потенциальные работодатели, не публикуй это.

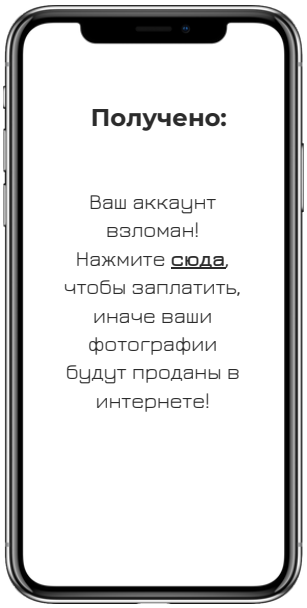
ОНЛАЙН-БЕЗОПАСНОСТЬ

Фишинг — это когда мошенники обманом заставляют вас раскрывать личную или финансовую информацию, выдавая себя за доверенное лицо, компанию или веб-сайт.

Нужно ли ответить на это электронное письмо? Почему?



Тебе пришло следующее текстовое сообщение на телефон. Что следует делать или не делать?



ФИШИНГ ИЛИ НЕТ

Перед тобой 4 примера сообщений. Определи, какие из них фишинговые (мошеннические), а какие — настоящие. Объясни, по каким признакам это можно определить.

Привет! Твой аккаунт выиграл iPhone 15. Перейди по ссылке и заполни форму, чтобы получить приз: [bit.ly/iph0ne-win]

Уважаемый пользователь! Ваш аккаунт во «ВКонтакте» был взломан. Для защиты перейдите по ссылке и смените пароль: [vk-security.ru]

Ваш заказ №45678 отправлен. Трек-номер для отслеживания: 123456789. Подробности: [ozon-track.ru]

Этот чат будет удалён из-за нарушений. Чтобы восстановить доступ, отправьте код из SMS, который придёт на ваш телефон.

ОНЛАЙН-БЕЗОПАСНОСТЬ

Небезопасный просмотр веб-страниц может подвергнуть ваше устройство риску заражения вирусами или установке вредоносных программа, а также действия мошенников, поставив под угрозу ваши личные данные.

Безопасно ли подключаться к этому Wi-Fi? Почему?

Безопасен ли этот сайт? Объясни, почему?

https://реальнохорошийсайт.ру

Отметь наиболее подходящие варианты паролей. Вычеркни небезопасные варианты:

password123	G!v3M3M@rshm@ll0ws
John123	qwerty

ОНЛАЙН-БЕЗОПАСНОСТЬ

Для защиты личных данных **не публикуй** в интернете свой **адрес, телефон, школу и информацию о родителях, фото документов, билетов и банковских карт, текущее местоположение** в реальном времени (например, "Сейчас в кафе"), не передавай пароли — даже друзьям.

Что делать в опасной ситуации: **сохрани скриншоты** переписки, **расскажи** родителям или учителю. Пожаловаться на пользователя можно через настройки соцсети или по телефону горячей линии 8 800 2000-122.

Что нужно сделать, получив такое сообщение?

Привет! Я админ группы твоей школы. Пришли код из SMS, и мы добавим тебя в закрытый чат класса.

Я взломал твою камеру и записал тебя. Пришли 1000 руб., или выложу видео в сеть

После спора в чате одноклассники создали группу, где высмеивают Петю, пишут ему оскорбления. Как правильно реагировать Пете? Кто может ему помочь?

Аня обнаружила фейковый аккаунт с её фото, где пишут гадости от её имени. Что делать, если твой профиль подделывают? Как доказать, что это не ты?

В социальных сетях набирает популярность челлендж: «Выпей бутылку соевого соуса за 10 секунд». Чем опасны такие челленджи? Как понять, что челлендж — это розыгрыш или угроза?

СОЗДАНИЕ НАДЁЖНОГО ПАРОЛЯ

НАДЕЖНЫЙ ПАРОЛЬ

Длинный – от 12 символов.

Содержит **разные типы символов**:

- Заглавные и строчные буквы (A, a)
- Цифры (1, 2, 3)
- Спецсимволы (!, @, #, %)

НЕНАДЕЖНЫЙ ПАРОЛЬ

Простые последовательности (12345, qwerty)

Личная информация (имя, дата рождения, nickname)

Одинаковые или повторяющиеся символы (1111, aaaa)

Задание 1. Придумай 3 надёжных пароля по правилам:

Пароль для почты: _____

Пароль для соцсети: _____

Пароль для игрового аккаунта: _____

Задание 2. Проверь пароль.

Дан пароль: «Кот123». Почему он ненадёжный?

1. _____
2. _____
3. _____

Задание 3. Создай пароль по подсказке.

Придумай пароль на основе фразы. Например, «Я учусь в 7Б классе!» → «YaUchus'v7B%»

Фраза: _____

Пароль:_____

📱 Устанавливай приложения только из официальных магазинов (Google Play, App Store).

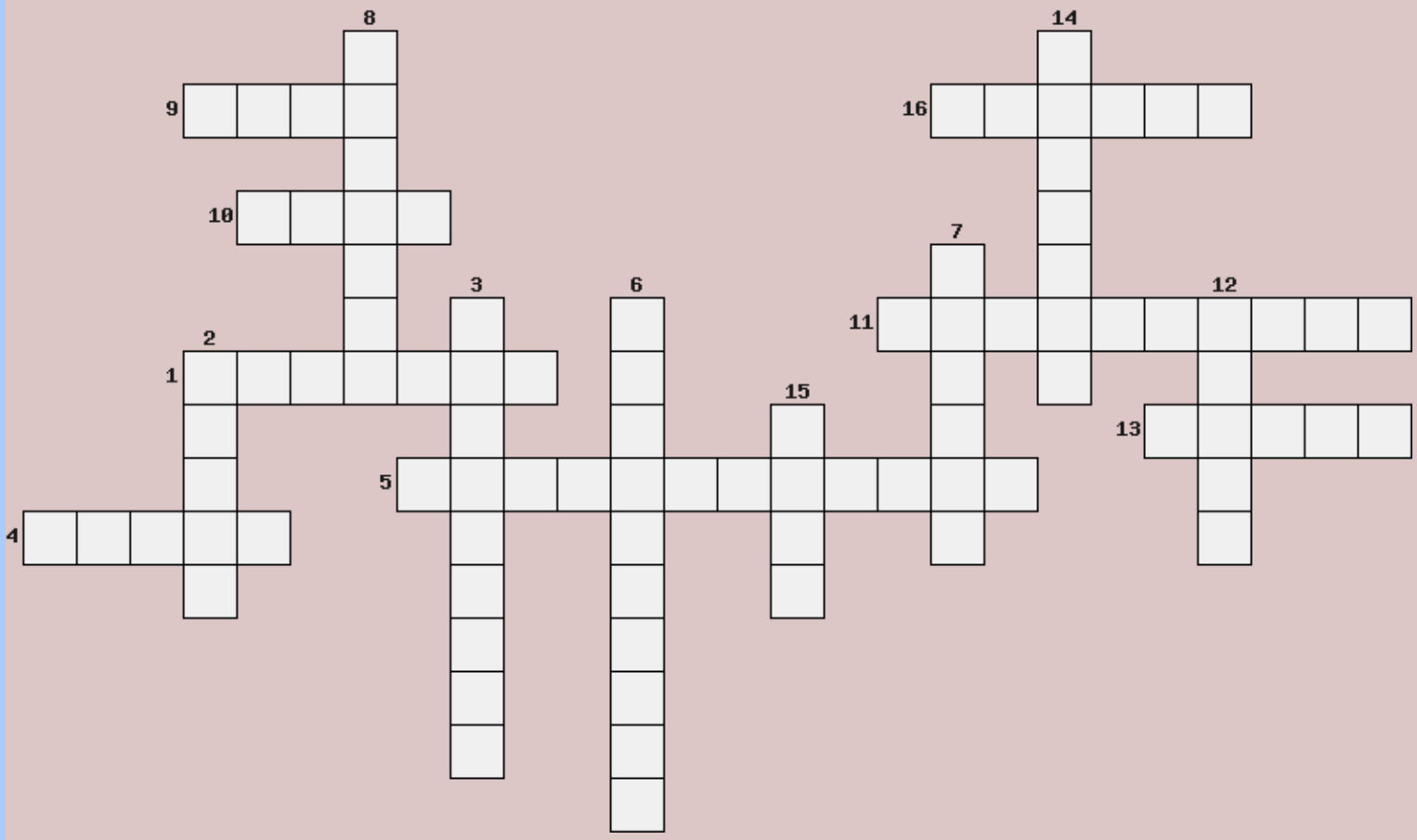
🛡️ Не переходи по подозрительным ссылкам (например, "Получи бесплатный приз!").

💻 Используй антивирус и регулярно обновляй программы.

🚫 Не участвуй в оскорблениях и распространении сплетен.

🛑 Если тебя или кого-то обижают — сохрани скриншоты, заблокируй обидчика, расскажи родителям или учителю.

КРОССВОРД



1. Услуга по предоставлению интернет-сервера и обеспечению его круглосуточной работоспособности.
2. Человек, который взламывает чужие аккаунты и системы.
3. Защитная программа от вирусов.
4. Адрес сайта в интернете, по которому его можно найти в глобальной сети.
5. Оскорбления и преследование в сети.
6. Преобразование данных в код или символы, неразборчивые для неавторизованных лиц, с целью обеспечения конфиденциальности информации.
7. Мошенничество с целью кражи личных данных через поддельные сайты.
8. Учетная запись, регистрационная запись.
9. Поддельный аккаунт в соцсетях.
10. Надоедливая реклама в интернете.
11. Несанкционированная попытка нарушить безопасность компьютерной системы или сети.
12. Вредоносная программа, которая может удалённо управлять вашим устройством.
13. Имя, которое вы выбираете для регистрации в системе.
14. Программа, позволяющая просматривать страницы в сети Интернет
15. Сайт, который маскируется под настоящий, чтобы украсть данные.
16. Секретный набор символов для входа в аккаунт.

ВЕРНО-НЕВЕРНО

Можно публиковать в соцсетях свой домашний адрес и номер школы.	+	-
Если тебе пришло сообщение с угрозами, нужно сохранить скриншот и рассказать взрослым.	+	-
Если в письме обещают бесплатный iPhone за переход по ссылке — это, скорее всего, обман.	+	-
Настоящие банки никогда не просят прислать пароль.	+	-
Лучше не отмечать геолокацию в реальном времени, чтобы посторонние не знали, где ты находишься.	+	-
Если сайт выглядит странно (много всплывающих окон, просьбы ввести данные), лучше его закрыть.	+	-
Вирусы могут заразить телефон, если скачать приложение не из официального магазина.	+	-
Размещать фото друга без его разрешения — это нарушение приватности.	+	-
Пароль «12345» — ненадёжный, его легко взломать.	+	-
Пересылать чужие переписки без разрешения — это нормально.	+	-
Если тебя оскорбляют в сети, лучше ответить тем же, чтобы обидчик отстал.	+	-
Если незнакомец пишет: «Привет, я друг твоего брата», можно доверять и добавлять его в друзья.	+	-

РАБОЧИЙ ЛИСТ ДЛЯ ШКОЛЬНИКОВ

БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ ОТВЕТЫ

Нужно ли ответить на это электронное письмо? Почему?

Нет, это письмо отвечать не нужно.

Это классический фишинг (обман): настоящие конкурсы не требуют банковских реквизитов для выигрыша, подобные письма рассылают мошенники, чтобы украсть деньги или данные.

Подозрительные признаки:

- Слишком хорошее предложение («$1,000,000»).
- Давление («срочно перейдите по ссылке»).
- Ошибки в оформлении (нет названия компании, официального логотипа).

Что делать?

- Не переходить по ссылке и не вводить никакие данные.
- Удалить письмо и пометить как спам.
- Если сомневаетесь, проверьте официальный сайт организаторов конкурса (но здесь явный обман).

Тебе пришло следующее текстовое сообщение на телефон. Что следует делать или не делать?

Это мошенничество: не переходите по ссылке – это попытка запугать и выманить деньги. Не платите – даже если отправить деньги, шантаж не прекратится. Не отвечайте – это подтвердит, что номер активен, и мошенники усилят атаку.

Признаки фейка:

- Угрозы («ваши фото будут проданы») – чтобы вызвать панику.
- Требование денег – настоящие взломщики редко предупреждают о “сливе” фотографий.
- Безликое обращение («Ваш аккаунт») – нет имени, конкретной соцсети.

Что делать?

- Скриншот – сохраните доказательство.
- Блокировка номера – чтобы избежать новых угроз.
- Проверка аккаунтов: смените пароли во всех соцсетях, включите двухфакторную аутентификацию.

Если угроза кажется реальной (например, вас шантажируют реальными фото):

- Обратитесь в полицию (ст. 163 УК РФ – вымогательство).
- Подайте жалобу на сайт МВД или через приложение «Госуслуги»

Фишинг или нет?

Фишинг – обещает бесплатный iPhone, ссылка ведёт на подозрительный сайт.

Фишинг – домен «vk-security.ru» не официальный, настоящий — только «vk.com».

Нет – похоже на настоящее уведомление (но лучше проверить домен).

Фишинг – мошенники пытаются получить код доступа к аккаунту.

Безопасно ли подключаться к этому Wi-Fi? Почему?
Нет, небезопасно без дополнительных мер защиты.

Почему это рискованно: перехват данных (злоумышленники в той же сети могут «прослушивать» ваш трафик: логины, пароли, переписку), особенно опасно, если сайты не используют HTTPS (нет замка в адресной строке).

Мошенники создают Wi-Fi с названиями вроде «Airport_Free» или «Starbucks_Guest» – подключившись, вы попадаете на поддельный сайт для кражи данных.

Ваши данные могут перенаправляться через устройство хакера перед отправкой на сервер, к тому же в открытых сетях выше риск подхватить вирус или троян.

Безопасен ли этот сайт? Объясни, почему?

Данный сайт взят для примера как безопасный.

1. Проверьте адрес (URL)
   - Ошибки в названии: Например, «yandex.ru» vs «yandexk.ru» (подделка).
   - Кириллица в домене: сайты на .ру могут быть легальными, но мошенники тоже используют русские буквы для обмана («сбербанк.рф» vs «сбербанк.рус»).
2. Протокол HTTPS:
   - Надежные сайты используют HTTPS (🔒 в адресной строке).
   - Если сайт только HTTP – данные передаются без шифрования.
4. Контент и оформление:
   - Ошибки: кривой дизайн, битые ссылки, агрессивная реклама.
   - Подозрительные предложения: «Срочно введите пароль!», «Вы выиграли iPhone!».
5. Отзывы и репутация: поищите отзывы, проверьте сайт через VirusTotal.