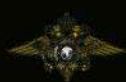




МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ



Первые



росмолодёжь



АЛЛЯНС
ПО ЗАЩИТЕ ДЕТЕЙ
В ЦИФРОВОЙ СРЕДЕ

РОССИЯ –
СТРАНА
ВОЗМОЖНОСТЕЙ

добро.рф



Билайн™

ШКОЛА КИБЕРБЕЗОПАСНОСТИ ДВИЖЕНИЯ ПЕРВЫХ



БУДЬВДВИЖЕНИИ.РФ



Сценарий мероприятия

Цель: познакомить участников с концепцией антискама

Задачи:

- дать определение антискаму и показать его роль в современном обществе;
- познакомить с основными угрозами в интернете (фишинг, мошенничество и т.д.);
- обучить базовым правилам кибербезопасности для себя и других;
- развить критическое мышление и навыки распознавания онлайн-угроз;
- как себя обезопасить и предотвратить проблему.

Целевая аудитория:

- Возраст 11-13 лет (обучающееся 5-6 классов)
- 25 человек

Формат и продолжительность:

- формат: интерактивный семинар с элементами тренинга и групповой работы;
- продолжительность: 45 минут (один урок)

Часть 1. Вступление (5 мин)

- приветствие, знакомство, объявление темы;
- мини-опрос: «Что вы знаете об антискаме»/скаме;
- постановка целей и задач мероприятия.

-Добрый день, мы команда Киберволонтеров. Эта встреча организована для того, чтобы обезопасить Вас в интернете. Кто-нибудь может дать определение слову «антискам»? ...Антискам нужен для защиты от мошенничества, противодействию.

Теоретический блок (10 мин)

- начало кейса (показ видео о реальных историях подростков, попавших в такую ситуацию)
- повторение что такое антискам;
- основные угрозы в сети: фишинг, мошенничество, деструктивные сообщества;
- как защитить себя и близких.

-По всему миру огромное количество реальных историй, когда подростки попадали в ловушку мошенников и несли после уголовную

ответственность... Самый простой пример: Вы получаете уведомление «Срочно! Ваш аккаунт может быть заблокирован»- это фишинг. А сейчас предлагаем проверить свои знания и поучаствовать в практикуме. Вы поделены на 3 команды по рядам, каждой мы выдадим распечатки на разные виды угрозы и команде нужно найти мошенника, объяснить свой выбор и составить план действий, для предотвращения мошеннической схемы.

Часть 3. Практикум (20 мин)

Работа в малых группах (4–5 человек):

Группа 1: «Найди фишинговое письмо»

Получает 5 распечаток электронных писем: 4 — легитимные (от банка, интернет-магазина, соцсети, сервиса доставки), 1 — фишинговое.

Задача: найти подозрительное письмо и отметить его признаки (например:

- ошибки в адресе отправителя;
- тревожные формулировки («срочно», «ваш аккаунт заблокирован»);
- ссылки, не совпадающие с официальным доменом;
- грамматические ошибки;
- просьба ввести логин/пароль по ссылке).

Результат: группа называет фишинговое письмо и кратко объясняет выбор (2–3 признака).

Группа 2: «Как помочь пострадавшему»

Получает сценарий ситуации (например, подросток получает подозрительные сообщения в соцсети) и 4 карточки с вариантами действий:

- 2 карточки — правильные (обратится к маме/учителю);
- 2 карточки — неправильные (ответить, начать диалог, соглашаться на его предложения).

Задача: выбрать верные шаги и расположить их в порядке действий.

Результат: группа представляет алгоритм помощи (3–4 шага) и объясняет, почему отвергла неверные варианты.

Группа 3: «Найди мошеннический сайт»

Получает скриншоты 4 сайтов: 3 — безопасные (официальный банк, госуслуги, крупный маркетплейс, новостной портал), 1 — мошеннический (копия банка или соцсети).

Задача: определить подозрительный сайт и назвать его признаки (например:

- отсутствие HTTPS и значка замка в адресной строке;

- орфографические ошибки на главной странице;
- слишком выгодные предложения («удвоим ваш вклад за час»);
- нет контактных данных или пользовательского соглашения;
- дизайн, отличающийся от оригинала).

Результат: группа показывает «опасный» сайт и называет 2–3 характерных признака.

Завершение практикума (5 мин)

Каждая группа по очереди представляет итоги: показывает пример (письмо/сайт), называет признаки угрозы или зачитывает памятку.

Ведущий кратко резюмирует: подчёркивает ключевые признаки угроз и универсальные правила безопасности, благодарит группы за работу.

Часть 4: Понимание представления подростков о защите

(как они уже сейчас могут защитить не только себя, но и других)

- неделя кибербезопасности;
- конкурс плакатов «Безопасный интернет»;
- мастер-класс для родителей или младших классов;

Часть 5. Заключение практикума (5 мин)

- рефлексия: «Что нового я узнал? Что могу сделать уже сейчас?»;
- вручение памяток и буклетов;

Используемые методы и формы работы

- лекция с визуальной поддержкой (презентация, видео);
- мини-опрос и обсуждение;
- групповая работа с кейсами;
- анализ реальных примеров (фишинговые письма, подозрительные сайты);
- мозговой штурм;
- рефлексия и обратная связь.

Перечень дидактических материалов

- мультимедийное оборудование (проектор, экран, компьютер);
- видеоролик о реальных примерах;
- распечатки кейсов (фишинговые письма, скриншоты мошеннических сайтов,);
- бланки для групповой работы;

- памятки «Правила кибербезопасности»;

Ожидаемые результаты

- участники понимают, что такое антискам;
- освоены базовые навыки распознавания онлайн-угроз (фишинг, мошенничество,);
- сформированы навыки оказания первой помощи в цифровой среде (советы близким, сообщение о противоправном контенте);
- часть участников выражает готовность присоединиться к киберволонтерским инициативам;
- повышена общая цифровая грамотность и ответственность в сети.

Используемые информационные источники

1. Федеральный закон «О благотворительной деятельности и добровольчестве (волонтерстве)» № 135-ФЗ;
2. сайт Роскомнадзора (правила подачи сообщений о противоправном контенте);
3. сайт «Лига безопасного интернета» (методики, кейсы, акции);
4. материалы МВД РФ по профилактике киберпреступлений;
5. образовательные программы «Кибербезопасность для школьников» от IT-компаний;
6. методические рекомендации по организации волонтерской деятельности в сфере кибербезопасности (Минобрнауки РФ);
7. открытые базы данных и тренажеры по киберграмотности (например, проекты «Цифровой ликбез»).



КАК НЕ ПОПАСТЬСЯ НА МОШЕННИКОВ В ИНТЕРНЕТЕ



ПАМЯТКА ДЛЯ ШКОЛЬНИКОВ 5–8 КЛАССОВ



1. ПРОВЕРЯЙ ОТПРАВИТЕЛЯ

Мошенники маскируются под банки, магазины, школы. Адрес их ссылок может быть похожим на настоящий, но в нем есть малозаметные отличия от оригинала.

Пример:

 [secure-bank.com](#)
 [secure-bank.ru](#)

2. НЕ ПЕРЕХОДИ ПО ССЫЛКАМ ИЗ СООБЩЕНИЙ

Неизвестные ссылки могут вести на фишинговые сайты – они крадут логины, пароли и данные карт.



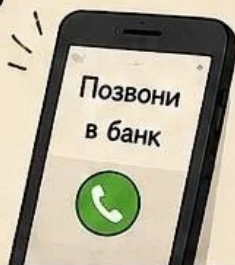
3. НЕ СООБЩАЙ ЛИЧНЫЕ ДАННЫЕ

Никогда и никому не говори: пароли, коды из СМС, номер карты, срок действия, CVV/CVC.

Настоящие службы никогда это не просят!

4. ПРОВЕРЯЙ ИНФОРМАЦИЮ

Если что-то пугает или срочно просят что-то сделать – это повод насторожиться! Перепроверь информацию на официальном сайте или спроси у взрослых.



5. ДУМАЙ ГОЛОВОЙ!

Мошенники давят на эмоции: «срочно», «иначе потеряете деньги», «ваш аккаунт заблокируют». Сделай паузу и подумай: это правда или обман?



ЗАПОМНИ ПРАВИЛО:

Не уверен – не переходи, не сообщай, не торопись!
Сомневаешься – спроси у взрослого!

