

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ
«ГУБЕРНСКИЙ КОЛЛЕДЖ Г. СЫЗРАНИ»

УТВЕРЖДАЮ
Директор ГБПОУ «ГК г. Сызрани»
_____ П.В. Салугин
«_____» _____ 2025 г.

Программа
профориентационной каникулярной смены
«Информационная безопасность»
для обучающихся 5-7-х классов
общеобразовательных организаций по специальности
**10.02.05 Обеспечение информационной безопасности
автоматизированных систем**

Форма реализации программы: *смешанная (очно-заочная)*

Автор-составитель:
Киреева Марина Владимировна, преподаватель

г. Сызрань, 2025

Пояснительная записка

В настоящее время подготовка конкурентноспособных специалистов, отвечающих требованиям рыночной экономики, является важной задачей системы образования. Поэтому много внимания уделяется профориентационной работе с обучающимися. В государственном бюджетном профессиональном образовательном учреждении Самарской области «Губернский колледж г. Сызрани» (далее – ГБПОУ «ГК г. Сызрани») профориентационная работа направлена на повышение уровня информированности обучающихся общеобразовательных организаций о востребованных на региональном рынке труда профессиях и специальностях, на формирование позитивного имиджа системы профессионального образования.

Настоящая программа «Информационная безопасность» направлена на повышение уровня информированности обучающихся общеобразовательных организаций о специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Программа является инклюзивной, доступна для обучающихся с ОВЗ, инвалидностью (нарушения слуха, нарушения опорно-двигательного аппарата, функций нижних конечностей, кровообращения) в составе групп полной включенности.

Цель программы – ознакомление обучающихся общеобразовательных организаций с профессиональным контекстом специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Задачи программы:

- 1) ознакомление обучающихся общеобразовательных организаций
 - с производственно-технологическим процессом;
 - с трудовым процессом;
 - с профессионально-важными качествами работника;
 - с организационной культурой ООО «Реклама»;
- 2) ознакомление обучающихся с условиями получения образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в ГБПОУ «ГК г. Сызрани» – организатора ПКС;
- 3) получение обучающимися общеобразовательных организаций практического опыта выполнения трудовых действий по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем;

4) предоставление обучающимся общеобразовательных организаций возможности рефлексии полученного опыта.

Целевая аудитория: обучающиеся 5-7 классов общеобразовательных организаций Самарской области.

Количество часов на освоение программы:

всего – 8 часов, в том числе:

– ознакомление с условиями получения профессионального образования в ГБПОУ «ГК г. Сызрани», реализующего программу ПКС – *1,5 академических часа*;

– мастер-класс в учебных мастерских «Основы кибербезопасности: как защититься в Интернете»; практико-ориентированного задания «Составление карьерной карты по специальности» – *1 академический час*;

– получение школьником опыта выполнения элементов профессиональной деятельности на базе ГБПОУ «ГК г. Сызрани» (профессиональная проба «Распознавание фишинговых писем») – *2 академических часа*;

– наблюдение школьником за деятельностью специалиста на рабочем месте, за технологическим процессом, работой оборудования; знакомство профессиональными требованиями к работникам, с организационной культурой ООО «Реклама» – *1,5 академических часа*;

– интерактивное мероприятие: деловая игра «Обеспечиваем безопасность» – *1 академический час*.

– рефлексия – *1 академический час*.

Продолжительность программы: 4 дня.

Академический час: 40 минут.

Ожидаемые результаты:

– формирование у обучающихся общеобразовательных организаций общего представления о профессиональном контексте специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем);

– получение обучающимися общеобразовательных организаций опыта выполнения практических заданий по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем;

– формулирование обучающимися общеобразовательных организаций отношения к представленной профессиональной деятельности (ее элементам).

Тематический план

№ п/п	Тема	Количество часов	Организационная форма деятельности
1.	День 1. ПКС на базе ГБПОУ «ГК г. Сызрани» - знакомство со специальностью 10.02.05 Обеспечение информационной безопасности автоматизированных систем	3	Очная форма
1.1	Инструктаж по технике безопасности	<i>0,2 часа</i>	Очная форма инструктажа в ГБПОУ «ГК г. Сызрани»
1.2.	Общая характеристика специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем - условия обучения (сроки и формы обучения); - порядок поступления на обучение	<i>0,5 часа</i>	Очная презентация специальности
1.3.	Характеристика содержания труда	<i>0,5 часа</i>	Очная экскурсия в ГБПОУ «ГК г. Сызрани»
1.4.	Условия обучения специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем	<i>0,5 часа</i>	Очная экскурсия по мастерским ГБПОУ «ГК г. Сызрани»
1.5.	Мастер-класс в учебных мастерских «Основы кибербезопасности: как защититься в Интернете»	<i>0,5 часа</i>	Наблюдение и анализ организации технологического процесса и элемента профессиональной деятельности
1.6.	Карьерная карта специальности	<i>0,5 часа</i>	Выполнение практико-ориентированного задания «Составление карьерной карты по

			специальности» в очной форме
1.7.	Рефлексия школьников своего участия в первом дне ПКС	0,3 часа	Заполнение листа рефлексии. Выявление отношения обучающихся к эмоциональному состоянию, отношению к информационному содержанию
2.	День 2. ПКС – профессиональные пробы в ГБПОУ «ГК г. Сызрани»	2	Очная форма
2.1	Инструктаж по технике безопасности	0,2 часа	Инструктаж в ГБПОУ «ГК г. Сызрани» перед выполнением профессиональных проб
2.2.	Кейс производственных задач	0,5 часа	Решение производственных задач
2.3.	Практическое ознакомление с элементами профессиональной деятельности	1 час	Профессиональная проба «Распознавание фишинговых писем» на базе ГБПОУ «ГК г. Сызрани»
2.4.	Рефлексия школьников своего участия во втором дне ПКС	0,3 часа	Заполнение листа рефлексии. Выявление отношения обучающихся к эмоциональному состоянию, отношению к информационному содержанию
3.	День 3. ПКС - знакомство с предприятием ООО «Реклама»	1,5	Дистанционная форма (очная форма по согласованию)
3.1.	Основные сведения об ООО «Реклама»: основные виды	0,5 часа	Экскурсия на предприятие ООО

	деятельности, продукция, перспективы развития		«Реклама» в дистанционной форме, просмотр видеороликов
3.2.	Функциональные обязанности специалиста, рабочее место, оборудование	0,5 часа	Наблюдение за технологическим процессом, работой оборудования на предприятии ООО «Реклама»
3.3.	Организационная культура ООО «Реклама», меры поддержки молодых специалистов	0,4 часа	Интервью с профессионалом - представителем предприятия ООО «Реклама»
3.4.	Рефлексия школьников своего участия во втором дне ПКС	0,1 часа	Заполнение листа рефлексии. Выявление отношения обучающихся к эмоциональному состоянию, отношению к информационному содержанию
4.	День 4. ПКС – деловая игра в ГБПОУ «ГК г. Сызрани»	1,5	Дистанционная форма
4.1.	Требования к индивидуальным особенностям человека, медицинские противопоказания	1 час	Деловая игра «Составление портрета специалиста»
4.2.	Рефлексия школьников своего участия в ПКС	0,5 часа	Заполнение листа рефлексии (прием «Лестница успеха»). Составление письменного отзыва о ПКС

* профессиональная проба прописывается в Программе профессиональной пробы – в приложении 1.

Условия реализации программы

Требования к материально-техническому обеспечению:

Программа ПКС «Информационная безопасность» реализуется на базе ГБПОУ «ГК г. Сызрани» и предприятия ООО «Реклама» (по договоренности).

Программа ПКС «Информационная безопасность» предполагает наличие следующих требований к помещениям:

- Лаборатория информационных технологий, сетей и систем передачи информации, программирования и баз данных, программных и программно-аппаратных средств защиты информации № 205;
- площадка предприятия ООО «Реклама».

Перечень оборудования, инструментов, материалов, необходимых для реализации программы ПКС, в том числе профессиональной пробы, в расчете на количество участников ПКС:

- персональный компьютер в сборе.

Реализация инклюзивной ПКС не предусматривает создание особых условий для школьников с ОВЗ, инвалидностью.

Информационное обеспечение:

- перечень мультимедиа-разработок – презентация PowerPoint «Профессиональное образовательное учреждение Губернский колледж г. Сызрани – твой путь к успеху»,
- виртуальная экскурсия на предприятие ООО «Реклама»: <https://reklabank.ru/o-nac/>
- имиджевый ролик рекламного агентства: <https://rutube.ru/video/b99af58858a755b1c53f9891abfb4a46/>
- интервью с профессионалом <https://rutube.ru/video/7a7f325fb3acfb8ed3bac3c1686b2e44/?r=plemwd>
- карьерная карта обучающегося по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем;
- видеофильм: «Информационная безопасность» <https://rutube.ru/video/0b48a0e76b5edb7e727305a5e80203a1/?r=plemwd>

Кадровое обеспечение:

специалисты ГБПОУ «ГК г. Сызрани», имеющие опыт работы в области профессиональной ориентации обучающихся общеобразовательных организаций и опыт работы с лицами с ОВЗ, инвалидностью – Киреева Марина Владимировна;

сотрудники ООО «Реклама» (по согласованию).

Аннотация

Профориентационная каникулярная смена знакомит школьников с профессиональным контекстом профессий и специальностей, востребованных на региональном рынке труда. Наряду с этим решаются задачи содействия профессиональному самоопределению школьников, организации их досуга, полезной познавательной занятости в каникулярное время.

Для обучающихся 5-7 классов особенно актуальны вопросы профессионального выбора. Профориентационная каникулярная смена «Информационная безопасность» направлена на профессиональную ориентацию обучающихся и представляет собой практико-ориентированные профориентационные мероприятия, направленные на знакомство со специальностью 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Попробовать себя в роли техника по защите информации в процессе прохождения профессиональных проб – отличная возможность почувствовать творческий настрой специальности.

Программа содержит экскурсии на предприятие ООО «Реклама», учебные мастерские ГБПОУ «ГК г. Сызрани», профессиональные пробы, мастер-классы, деловые игры, рефлекссию.

Описание профессиональной пробы

«Распознавание фишинговых писем»

Введение (7 мин).

Интернет — это огромное пространство, где можно найти много интересного и полезного: игры, учебные материалы, фильмы, музыку и многое другое. Но, как и в реальной жизни, в интернете тоже есть свои опасности. И чтобы защитить себя, нужно знать несколько простых правил.

1. Личные данные — это не для всех

Когда вы регистрируетесь на сайтах или в социальных сетях, вам часто предлагают ввести свои данные: имя, фамилию, адрес, номер телефона. Но не все сайты заслуживают доверия. Мошенники могут использовать ваши данные для обмана или кражи.

Поэтому:

– Никогда не делитесь своими личными данными с незнакомыми людьми или на подозрительных сайтах.

– Используйте сложные пароли и не пишите их на видных местах.

– Проверяйте, кто просит у вас информацию. Если это незнакомый человек или сайт, лучше не отвечать.

2. Осторожно с ссылками и вложениями

В интернете часто можно встретить письма или сообщения с интересными предложениями: «Вы выиграли миллион!», "Получите бесплатный подарок!" или «Ваш аккаунт заблокирован, перейдите по ссылке». Но такие письма могут быть ловушкой. Это называется фишинг — когда мошенники пытаются обманом заставить вас перейти на поддельный сайт и ввести свои данные.

– Не переходите по подозрительным ссылкам и не открывайте вложения от незнакомых отправителей.

– Проверяйте адрес сайта: если он выглядит странно или отличается от официального, это может быть мошенничество.

3. Будьте осторожны в социальных сетях

Социальные сети — это отличное место для общения, но и здесь нужно быть внимательными. Никогда не добавляйте в друзья незнакомых людей, особенно если они просят вас о чем-то странном. И не забывайте, что всё, что вы публикуете, может увидеть кто угодно.

– Настройте приватность своего профиля, чтобы только друзья могли видеть ваши публикации.

– Не публикуйте личные данные и фотографии, которые могут использовать против вас.

4. Вирусы и вредоносные программы

Иногда, когда вы скачиваете файлы или программы из интернета, можно случайно загрузить вирус. Вирусы могут повредить ваш компьютер, украсть данные или даже заблокировать доступ к вашим файлам.

– Скачивайте программы и файлы только с проверенных сайтов.

– Используйте антивирус на своем компьютере, чтобы защитить его от угроз.

5. Критическое мышление

Самое главное — это умение думать и анализировать. Не верьте всему, что видите в интернете. Если что-то кажется слишком хорошим, чтобы быть правдой, скорее всего, это обман.

– Думайте, прежде чем действовать. Если что-то вызывает сомнения, лучше проверить информацию или спросить у взрослых.

– Общайтесь только с теми, кого знаете. В интернете много людей, которые могут притворяться кем-то другим.

С развитием цифровых технологий и увеличением числа пользователей интернета дети всё чаще сталкиваются с угрозами кибербезопасности. Фишинговые письма стали одним из наиболее распространённых способов мошенничества, направленного на кражу личных данных. Поскольку школьники активно пользуются электронными почтовыми сервисами и социальными сетями, умение распознавать такие угрозы становится жизненно

важным навыком. Этот урок позволит учащимся лучше понимать опасности, связанные с фишингом, и научит их защищать свои личные данные в сети.

Постановка цели и задачи в рамках пробы (5 мин)

Цель: Формирование навыков распознавания фишинговых писем среди электронной почты.

Задачи:

1. Изучение признаков фишинга (поддельных электронных писем).
2. Развитие критического мышления и внимательности при работе с электронной почтой.
3. Обучение методам проверки подлинности сообщений и сайтов.
4. Воспитание осторожности в интернете.

Пошаговое выполнение задания

1. Теоретическая часть (10 минут)

Ребята, представьте себе такую ситуацию: вы получаете письмо якобы от вашего любимого магазина или банка, в котором говорится, что ваш аккаунт заблокирован, и чтобы его восстановить, нужно срочно перейти по ссылке и ввести свои данные. Звучит тревожно, правда? Но самое интересное, что это письмо вовсе не настоящее! Это называется фишинг.

Фишинг — это способ обмана, когда злоумышленники присылают вам поддельные письма, замаскированные под официальные сообщения от известных компаний или организаций. Цель фишинга — заставить вас раскрыть свои личные данные, такие как пароли, номера карт или другие важные сведения. Эти данные потом могут использовать для кражи денег или другой личной информации.

Теперь давайте разберемся, почему так важно уметь распознавать такие письма. Представьте, что вы получили письмо, которое кажется настоящим, но на самом деле оно подделка. Если вы перейдете по ссылке и введете свои данные, то можете потерять доступ к своим аккаунтам, а иногда даже деньги!

Кибермошенники становятся всё хитрее, и каждый день придумывают новые способы обмануть людей. Поэтому умение видеть разницу между

настоящими и фальшивыми письмами помогает защитить ваши личные данные и избежать неприятностей.

Чтобы научиться распознавать фишинговые письма, нужно обращать внимание на несколько важных деталей. Вот основные признаки, которые помогут вам отличить настоящие письма от поддельных:

1. Необычный адрес отправителя

Когда вы получаете письмо, первым делом посмотрите на имя и адрес отправителя. Например, если письмо пришло якобы от Сбербанка, но адрес выглядит странно (например, `sberbank@mail.ru` вместо официального `@sberbank.ru`), скорее всего, это фишинг.

2. Ошибки в тексте

Мошенники часто спешат и допускают ошибки в тексте: грамматические, орфографические или стилистические. Настоящие компании стараются отправлять письма без ошибок, потому что заботятся о своей репутации.

3. Срочные просьбы действий

Часто в фишинговых письмах используются фразы вроде «Немедленно войдите в систему», «Ваш аккаунт будет заблокирован через час», «Ваши данные были украдены». Мошенники хотят напугать вас и заставить быстро реагировать, не задумываясь.

4. Невероятные предложения

Будьте осторожны, если вам предлагают неожиданно большие выигрыши, бесплатные подарки или что-то слишком хорошее, чтобы быть правдой. Например, письмо с заголовком «Вы выиграли миллион рублей!» почти наверняка является фишингом.

Теперь вы знаете, на что стоит обратить внимание, чтобы не попасться на удочку мошенников. Помните, что ваша безопасность в интернете зависит от вашей внимательности и умения анализировать информацию.

2. Практическое задание (20 минут)

Преподаватель раздает каждому ученику набор из нескольких писем (распечатанные листы с примерами реальных и поддельных писем), где нужно определить, какие из них являются фишингом.

Письмо №1:

От кого: info@bank.ru

Текст: «Ваш аккаунт заблокирован! Перейдите по ссылке и введите пароль для разблокировки».

Ответ: Фишинг — подозрительная ссылка и срочность.

Письмо №2:

От кого: news@company.com

Текст: «Уважаемые клиенты, напоминаем вам о продлении подписки до конца месяца».

Ответ: Настоящее письмо.

Письмо №3:

От кого: support@yandex.ru

Тема: Ваш Яндекс.Почта-аккаунт был взломан

Текст: Здравствуйте!

Мы обнаружили подозрительную активность на вашем почтовом ящике. Чтобы подтвердить вашу личность и предотвратить дальнейшие проблемы, пожалуйста, перейдите по этой ссылке и введите свои данные: [ссылка].

Спасибо за понимание, Служба поддержки Яндекс.Почта

Ответ: Фишинг. Адрес отправителя подозрительный, ссылка ведет на сторонний сайт.

Письмо №4:

От кого: news@school.ru

Тема: Новое расписание уроков

Текст: Уважаемые родители и ученики!

Сообщаем вам, что с понедельника вводится новое расписание уроков. Подробную информацию вы можете найти на нашем сайте school.ru в разделе «Расписание».

С уважением, администрация школы.

Ответ: Настоящее письмо от школы с информацией о расписании

Письмо №5:

От кого: bank@security.com

Тема: ВАЖНО: Ваша карта заблокирована

Текст: Уважаемый клиент!

Из-за подозрительной активности ваша банковская карта была временно заблокирована. Для её активации перейдите по следующей ссылке и подтвердите свои данные: [ссылка].

Не откладывайте, иначе карта останется заблокированной навсегда!

С уважением, служба безопасности банка.

Ответ: Фишинг. Срочная просьба действий, угроза блокировки карты.

Письмо №6:

От кого: noreply@amazon.com

Тема: Заказ №12345 отправлен

Текст: Добрый день!

Ваш заказ №12345 успешно обработан и отправлен. Вы можете отслеживать статус доставки на нашем сайте amazon.com.

Благодарим за покупку! Команда Amazon.

Ответ: Настоящее уведомление от Amazon о статусе заказа.

Письмо №7:

От кого: info@paypal.ru

Тема: Подтверждение платежа

Текст: Приветствуем вас!

Для завершения операции по переводу средств нам необходимо подтвердить вашу личность. Пожалуйста, перейдите по ссылке и введите свой пароль: [ссылка].

Ваш PayPal.

Ответ: Фишинг. Просьба ввести пароль по ссылке.

Письмо №8:

От кого: promotion@google.com

Тема: Вы выиграли Google Pixel!

Текст:Поздравляем!

Вы стали победителем нашего конкурса и выиграли новый смартфон Google Pixel. Чтобы получить приз, заполните форму на нашем сайте: [ссылка].

С наилучшими пожеланиями, команда Google.

Ответ: Фишинг. Невероятное предложение выиграть Google Pixel.

Письмо №9:

От кого: no-reply@facebookmail.com

Тема: Изменение пароля Facebook

Текст:Дорогой пользователь!

Ваша учетная запись Facebook требует изменения пароля. Пожалуйста, пройдите по ссылке и следуйте инструкциям: [ссылка].

Спасибо, Facebook Team.

Ответ: Фишинг. Запрашивает изменение пароля через ссылку.

Письмо №10:

От кого: admin@vkontakte.su

Тема: Активация аккаунта

Текст:Здравствуйтесь!

Для подтверждения вашей личности и активации аккаунта VKontakte, пожалуйста, перейдите по следующей ссылке и введите свои данные: [ссылка].

С уважением, команда VKontakte.

Ответ: Фишинг. Подозрительный домен vkontakte.su.

Письмо №11:

От кого: service@ok.ru

Тема: Новый функционал ОК.ru

Текст: Добро пожаловать!

На платформе ОК.ru появился новый функционал. Чтобы ознакомиться с ним, пожалуйста, обновите свои настройки, перейдя по ссылке: [ссылка].

С уважением, команда ОК.ru.

Ответ: Фишинг. Просят обновить настройки через ссылку.

Письмо №12:

От кого: helpdesk@instagram.org

Тема: Восстановление доступа

Текст: Уважаемый пользователь Instagram!

Мы заметили необычную активность на вашем аккаунте. Чтобы восстановить доступ, пожалуйста, пройдите по ссылке и введите свои данные: [ссылка].

Спасибо, служба поддержки Instagram.

Ответ: Фишинг. Требуют ввода данных через ссылку.

Письмо №13:

От кого: notification@email.mail.ru

Тема: Сообщение от друга

Текст: Здравствуйте!

Ваш друг отправил вам важное сообщение. Чтобы прочитать его, пожалуйста, авторизуйтесь на нашем сайте: [ссылка].

С уважением, Mail.ru Group.

Ответ: Фишинг. Авторизация через подозрительную ссылку.

Письмо №14:

От кого: news@twitter.com

Тема: Новые функции Twitter

Текст: Приветствуем вас!

Мы рады представить вам новые функции Twitter. Чтобы узнать больше и активировать их, пройдите по ссылке: [ссылка].

С уважением, команда Twitter.

Ответ: Фишинг. Активация новых функций через ссылку.

Письмо №15:

От кого: noreply@apple.com

Тема: Ваша покупка в Apple Store

Текст: Добрый день!

Ваш заказ №98765 успешно оформлен и отправлен. Вы можете отслеживать статус доставки на нашем сайте apple.com.

Благодарим за доверие, Apple Store.

Ответ: Настоящее подтверждение покупки в Apple Store.

Письмо №16:

От кого: office365@microsoft.com

Тема: Важное обновление Office 365

Текст: Уважаемый пользователь Microsoft Office 365!

Произошли важные обновления в нашей системе. Чтобы продолжить работу, пожалуйста, обновите свои настройки, перейдя по ссылке: [ссылка].

С уважением, Microsoft Office 365.

Ответ: Фишинг. Обновление настроек через подозрительную ссылку.

Письмо №17:

От кого: alert@netflix.com

Тема: Информация о платеже

Текст: Уважаемые пользователи Netflix!

Ваша подписка была успешно продлена. Спасибо за использование наших услуг!

С уважением, команда Netflix.

Ответ: Настоящая информация от Netflix о продлении подписки.

Письмо №18:

От кого: account@outlook.com

Тема: Проблемы с входом в Outlook

Текст: Уважаемый пользователь Outlook!

Мы зафиксировали попытку входа в ваш аккаунт с неизвестного устройства. Чтобы подтвердить свою личность и продолжить работу, пожалуйста, пройдите по ссылке и введите свои данные: [ссылка].

С уважением, служба поддержки Outlook.

Ответ: Фишинг. Вход через подозрительную ссылку.

Ученики отмечают признаки фишинга на каждом письме и записывают свои выводы.

3. Анализ результатов (10 минут)

Обсуждение с учениками результат их работы:

- Какие письма оказались настоящими
- Почему ученики считали некоторые письма фишинговыми
- Как правильно действовать, когда получаешь подозрительное письмо?

4. Рекомендации для наставника

1. Организация процесса:

– Использование наглядных материалов (распечатки писем, презентации).

- Стимулирование обсуждения между учениками.
- Поощрение самостоятельного мышления и критики.

2. Контроль и оценка:

- Проверка правильности анализа каждого письма.
- Оценка способности учеников находить ключевые признаки фишинга.

3. Рефлексия (8 минут):

Что нового вы узнали? Расскажите, какие новые знания вы получили?

Какие трудности возникли при выполнении задания?

Как вы будете применять эти знания в реальной жизни?

Что было самым интересным на уроке?

Какие вопросы у вас остались?

Как вы оцениваете свою работу на уроке по шкале от 1 до 5?

Ребята, интернет — это замечательный инструмент, который может помочь вам учиться, развлекаться и общаться. Но чтобы он оставался безопасным, нужно быть внимательными и осторожными. Всегда помните о простых правилах, которые мы сегодня обсудили, и не стесняйтесь обращаться за помощью к взрослым, если что-то вызывает сомнения.

Берегите себя и свои данные!

Инфраструктурный лист

1. Компьютеры для демонстрации примеров писем.
2. Распечатки писем с признаками фишинга.
3. Презентация с основными тезисами урока.
4. Маркеры или цветные карандаши для выделения ключевых моментов

в письмах.

Приложение и дополнения

1. Дополнительный материал:

Краткий гайд по проверке подлинности ссылок.

№ п/п	Шаг	Действие
1.	Изучите адрес	Проверьте доменное имя, наличие орфографических ошибок и протокол HTTPS
2.	Наведите курсор	Посмотрите полный адрес ссылки во всплывающей подсказке
3.	Используйте сервисы	Воспользуйтесь VirusTotal или Google Safe Browsing для проверки
4.	Осторожно с сокращёнными ссылками	Используйте расширители URL для просмотра полного адреса
5.	Проверяйте источник	Обратите внимание на контекст получения ссылки
6.	Следите за уведомлениями браузера	Не игнорируйте предупреждения о небезопасных сайтах
7.	Обратитесь за помощью	Спросите мнение взрослого или опытного пользователя, если сомневаетесь

Примеры распространенных мошеннических схем.

№ п/п	Название схемы	Описание	Пример
1.	Фишинг	Получение личных данных через поддельные сайты или письма	Письмо от банка с просьбой обновить данные счета
2.	Вишинг (голосовой фишинг)	Телефонные звонки с целью выманивания личных данных	Звонок от «службы безопасности» с требованием предоставить данные карты

3.	Скимминг	Кража данных платежной карты с помощью устройств, установленных на банкоматах	Устройство на банкомате, считывающее данные карты
4.	Лотерейные мошенничества	Ложные уведомления о выигрыше с требованием уплаты комиссии	Письмо о выигрыше автомобиля с предложением оплатить сбор
5.	Техническая поддержка	Обман под видом помощи от техподдержки с целью получения удаленного доступа	Звонок от "специалиста Microsoft" с сообщением о вирусе на компьютере
6.	Романтическое мошенничество	Завоевание доверия через отношения с последующим вымогательством	Знакомство на сайте знакомств с последующей просьбой о деньгах
7.	Финансовые пирамиды	Привлечение инвесторов с обещаниями высокой доходности, основанные на мошенничестве	Проект с доходностью 100% годовых, который на деле оказывается пирамидой
8.	Поддельные интернет-магазины	Сайты, имитирующие реальные магазины, с целью кражи денег	Сайт с привлекательными ценами, после оплаты с которого товар не поступает
9.	Смартфонные приложения-мошенники	Приложения, содержащие вредоносный код для кражи данных	Приложение для редактирования фото, отправляющее платные SMS
10.	Криптовалютные мошенничества	Обещания высоких доходов от инвестиций в криптовалюты с последующим исчезновением средств	Платформа с гарантированными доходами, которая исчезает с деньгами инвесторов