Кураторский час «Кибермошенники: как не стать добычей в цифровом лесу?»

Целевая аудитория: студенты всех курсов

Направление: цифровая грамотность

Продолжительность: 50 - 60 минут

Оборудование: компьютер, проектор, презентация

Количество участников: 20 - 30 человек

Цель: Формирование у студентов устойчивых навыков безопасного поведения в цифровой среде и развитие критического мышления при взаимодействии с онлайн-сервисами.

Задачи:

1. Познакомить студентов с наиболее распространёнными схемами кибермошенничества.
2. Научить определять признаки фальшивых сообщений, сайтов, звонков.
3. Отработать алгоритм действий в случае кибератаки или утечки данных.
4. Повысить цифровую культуру и настороженность в интернете.

Ход работы:

1. Вступление. «Почему мы говорим об этом?» (Слайд 1–2) — 5 мин

Вводное слово куратора:

Здравствуйте, друзья! Сегодняшняя встреча будет о том, как сохранить не только деньги, но и личные данные.

Мы не будем читать лекцию – сегодня в практических примерах вы узнаете, как работают мошенники, какие у них приёмы и как им не попасться.

Интерактивный вопрос (Слайд 2):

Поднимите руку, кто хоть раз получал сообщение о «подозрительном заказе», «блокировке карты» или «выигрыше айфона».

(Пауза — смотрим на аудиторию)

Видите? Это значит, что вы уже потенциальная цель мошенников.

2. Почему студенты — любимая аудитория кибермошенников (Слайд 3) — 7 мин

Всё просто. Во-первых, вы — самое активное поколение в интернете: соцсети, онлайн-покупки, доставки еды, подработки. Вы постоянно что-то ищете, кликаете, переходите.

Во-вторых, многие думают: «У меня на карте 500 рублей, меня красть не будут». Это главный миф! Крадут не только деньги. Крадут ваши данные, ваши аккаунты, доступы к почте и соцсетям, чтобы потом взламывать через вас ваших знакомых. Вы — ценный актив в их глазах.

3. Три основные схемы мошенничества (Слайд 4–5) — 10 мин

Давайте узнаем врага в лицо. Есть три самые популярные схемы, которые работают на студентах.

Первая: «Мама, это я!». Вам в мессенджер пишет друг с просьбой срочно перевести деньги, потому что он «в беде». Здесь мошенники играют на вашем доверии и панике.

Вторая: «Вам полагается выплата или штраф!». Звонок от «банка» или, что страшнее, от «полиции». Здесь работают на страхе и авторитете официальной организации.

И третья, самая коварная: «Вкусная приманка». Фейковый магазин с дикими скидками, сайт-клон известной доставки еды или поддельная страница для оплаты проезда. Тут ловят на вашем желании выгоды и спешке.

Пример для анализа:

СМС: «Ваш счёт заблокирован. Перейдите по ссылке для восстановления».

— Где ловушка? (Ответ: срочность, поддельная ссылка, обычный номер.)

Давайте на примере. Допустим, пришло такое СМС: «Ваш аккаунт заблокирован! Перейдите по ссылке, чтобы восстановить доступ!». Смотрите: во-первых, создается искусственная срочность — «сделай сейчас, иначе будет плохо». Во-вторых, номер отправителя — обычный мобильный, а не короткий номер типа 900. И самое главное — ссылка ведет на сайт, который лишь похож на официальный. Настоящий банк никогда так не пишет.

4. «Ваш цифровой иммунитет» — алгоритм защиты (Слайд 6) — 10 мин

Что же делать? Все просто. Ваша защита — это три кита.

Первый и главный: Пауза. Любое сообщение, которое требует срочных действий, — это красный флаг. Вдохнули, выдохнули. Не паникуем. Если звонят из «банка» — вешаем трубку и перезваниваем по официальному номеру из приложения или с карты.

Второй: Проверяем ссылки. Прежде чем кликнуть, наведите на нее курсор — во всплывающей подсказке вы увидите настоящий адрес. Он явно не будет похож на настоящий? И всегда смотрите на «https://» и замок в адресной строке.

И третий: Включаем «параноика». Запомните раз и навсегда: НИКОГДА и НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ банк не будет просить вас перевести деньги на «страховой» или «безопасный» счет. И уж тем более не будет дистанционно устанавливать вам какое-то ПО. Это всегда — мошенники.

5. Что делать, если попались? (Слайд 7) — 5 мин

- Немедленно звоните в банк, сообщите: «Мои деньги уходят по мошеннической операции».
- Заблокируйте карту.
- Напишите заявление в банк о несанкционированной операции (в течение 24 часов!).
- Смените все пароли.
- При необходимости обратитесь в полицию (ст. 159.6 УК РФ — мошенничество в сфере IT).

6. Интерактив «Верю – не верю» (Слайды 8–13) — 15 мин

А теперь давайте проверим наши знания на реальных кейсах! Я буду зачитывать ситуацию, а вы попробуйте угадать — это мошенническая деятельность или нет?

Далее вы зачитываете ситуации со слайдов 8-13, даете аудитории 10-15 секунд на обдумывание, а затем объявляете правильный ответ и кратко его комментируете, как это сделано на слайдах. Это оживит аудиторию и закрепит материал.

7. Итог. «Запомни главное!» (Слайд 14–15) — 5 мин

Подведение итогов:

- Мошенники — отличные психологи. Они играют на страхе, доверии и спешке.
- Проверяйте каждое сообщение и не спешите нажимать на ссылки.
- Банк, налоговая, полиция — никогда не общаются через мессенджеры.
- Ваши деньги и данные защищены ровно настолько, насколько вы внимательны.