Приложение 3

Кейс-карточки «Цифровые угрозы»

Нижний Новгород, 2025 год

Кейс 1

Сценарий:

Анна получает электронное письмо, которое выглядит как официальное сообщение от ее банка. В письме говорится о подозрительной активности на ее карте и необходимости срочно подтвердить личность, перейдя по ссылке.

От: Support Sber bank_support@mailer.com

Тема: ВАЖНО: Ваша карта будет заблокирована!

Уважаемый клиент! Наша система безопасности зафиксировала подозрительную активность с вашей карты. Для вашей же безопасности мы временно ограничили доступ. Чтобы избежать полной блокировки, вам нужно срочно подтвердить свою личность. Перейдите по ссылке ниже и войдите в свой личный кабинет. http://sberbank.auth-login.site/restore

С уважением, Служба безопасности Сбер.

Вопросы для команды:

1.Какая цифровая угроза описана в этом кейсе?

2.Какие признаки указывают на эту угрозу?

3.Какие действия должна предпринять Анна, чтобы защитить себя?

Кейс 5

Сценарий:

Мария, ученица 10 класса, получает в мессенджере сообщение от неизвестного номера. В сообщении прикреплено короткое видео, на котором она якобы произносит оскорбительные слова в адрес одноклассника и совершает непристойные действия. Видео выглядит очень реалистично. Отправитель требует крупную сумму денег, угрожая в противном случае распространить видео среди всех её контактов и выложить в интернет. Мария в панике, так как точно знает, что никогда ничего подобного не делала, но видео выглядит настолько убедительно, что она боится, что ей никто не поверит.

Вопросы для команды:

1.Какая цифровая угроза описана в этом кейсе? Какие технологии могли быть использованы для создания такого видео?

2.Какие признаки могут указывать на то, что видео является подделкой (deepfake)?

3.Какие правовые нормы нарушены в данной ситуации?

4.Какие действия должна предпринять Мария, чтобы защитить себя и свои права? Куда ей следует обратиться за помощью?

Кейс 2

Сценарий:

Анастасия, ученица 10 класса, получает сообщение в социальной сети от аккаунта, который выглядит как официальная страница известного бренда электроники.

"Поздравляем! Вы покупали у нас наушники и стали одним из 100 победителей нашей акции. Вы получаете новый смартфон и 5000 рублей на счет! Для получения приза перейдите по ссылке и установите наше приложение для верификации: bit.ly/brand_prize_app".

Анастасия, обрадовавшись такому подарку, переходит по ссылке. Вместо страницы с информацией о призе, начинается автоматическая загрузка файла с расширением .apk (для Android) или .exe (для Windows), который называется "BrandPrizeVerifier.apk" или "BrandPrizeVerifier.exe". Она устанавливает это "приложение", не обратив внимания на запрошенные разрешения (доступ к контактам, SMS, галерее, микрофону). Через несколько дней Анастасия замечает, что с её банковской карты, привязанной к телефону, списываются небольшие суммы, а её друзья получают странные сообщения от её имени. Также она обнаруживает, что её личные фотографии и переписки из мессенджеров появились в открытом доступе на каком-то сомнительном сайте.

Вопросы для команды:

1. Какая цифровая угроза описана в этом кейсе?
2. Какие признаки указывают на эту угрозу и как она связана с первоначальной приманкой?
3. Какие действия должна предпринять Анастасия, чтобы защитить себя и свои данные?

Кейс 6

Дмитрий, студент колледжа, видит на остановке общественного транспорта объявление о розыгрыше ценных призов от популярного онлайн-магазина электроники. Для участия нужно отсканировать QR-код и ввести свои данные на сайте. Дмитрий сканирует код, попадает на сайт, который выглядит идентично официальному сайту магазина, и вводит свои ФИО, номер телефона, а также данные банковской карты для «подтверждения участия». Через несколько минут ему приходит СМС о списании крупной суммы с его карты, а затем ещё одно – об оформлении микрозайма на его имя.

Вопросы для команды:

1.Какая цифровая угроза описана в этом кейсе? Как она связана с использованием QR-кода?

2.Какие признаки указывают на то, что сайт был поддельным (фишинговым)?

3.Какие статьи законодательства РФ нарушены действиями мошенников?

4.Какие немедленные действия должен предпринять Дмитрий? Куда ему следует обратиться за помощью и как предотвратить подобные ситуации в будущем?

Кейс 3

Сценарий:

Егор, ученик 9 класса, проводит много времени в TikTok и других социальных сетях. Однажды он натыкается на короткое видео, где некий "эксперт" с серьезным видом утверждает, что новый школьный предмет "Основы цифровой безопасности" на самом деле является скрытой программой для сбора данных о школьниках, а все их телефоны будут подключены к единой государственной системе слежки. Видео быстро набирает просмотры и комментарии, многие из которых выражают панику и возмущение. Егор, обеспокоенный этой информацией, начинает активно обсуждать это с одноклассниками, пересылать видео в школьные чаты. Он видит, что многие его друзья тоже верят этому видео, потому что "эксперт" выглядит убедительно, а в комментариях пишут, что это "правда, о которой молчат".

Вопросы для команды:

1. Какая цифровая угроза описана в этом кейсе?
2. Какие признаки указывают на эту угрозу?
3. Какие действия должен предпринять Егор, чтобы защитить себя и других от манипуляции?

Кейс 7

Сценарий:

Елена, активный пользователь социальных сетей, часто участвует в различных онлайн-челленджах. В одном из них нужно было записать короткое видео, где она произносит фразу «Я доверяю этому приложению» и загрузить его в специальное приложение для «улучшения голоса». Через некоторое время Елене начинают приходить уведомления о попытках входа в её банковское приложение с использованием голосовой аутентификации. А её друзья получают от неё голосовые сообщения с просьбами одолжить деньги, хотя Елена ничего подобного не отправляла

Вопросы для команды:

1.Какая цифровая угроза описана в этом кейсе? Что такое биометрические данные и почему их кража опасна?

2.Какие законы РФ регулируют сбор и использование биометрических данных?

3.Какие действия должна предпринять Елена, чтобы защитить свои данные и предотвратить дальнейшее использование её голоса?

4.Как можно было избежать этой ситуации? Какие меры предосторожности следует соблюдать при использовании приложений, запрашивающих доступ к биометрическим данным?

Кейс 4

Сценарий:

Алина, ученица 9 класса, всегда была активной и общительной. Недавно она случайно услышала сплетню о своей однокласснице Лизе и, не придав этому значения, пересказала её в личном сообщении своей лучшей подруге. Однако подруга, вместо того чтобы сохранить секрет, переслала это сообщение в закрытый групповой чат класса, где состояли почти все ученики. Сплетня быстро разлетелась, и к ней добавились новые, совсем искаженные подробности. В чате начали появляться унизительные мемы и оскорбительные комментарии в адрес Лизы. Лизу стали игнорировать в школе, не приглашать на общие мероприятия, а в чате её сообщения оставались без ответа или сопровождались насмешками. Лиза чувствует себя абсолютно опустошенной, она боится ходить в школу, её успеваемость падает, и она перестала общаться даже с теми, кто раньше был её другом. Алина, увидев, к чему привела её неосторожность, чувствует вину, но боится вмешаться, опасаясь, что сама станет жертвой травли.

Вопросы для команды:

1. Какая цифровая угроза описана в этом кейсе и в чем её сложность по сравнению с прямыми оскорблениями?
2. Какие признаки указывают на эту угрозу и как она развивается?
3. Какие действия должна предпринять Лиза, чтобы защитить себя? Какие действия может предпринять Алина, чтобы исправить ситуацию, не подвергая себя риску?

Кейс 8

Сценарий:

Иван, ученик 9 класса, начал замечать, что проводит всё больше времени в рекомендательных лентах социальных сетей и видеохостингов. Он заходит «на пять минут», чтобы посмотреть одно видео, но алгоритмы постоянно предлагают ему новый, всё более увлекательный контент, и он не может остановиться. В итоге он проводит в сети по 4–5 часов в день, забывая о домашнем задании, спорте и общении с друзьями в реальной жизни. Его успеваемость падает, он чувствует постоянную усталость и раздражительность, но не может самостоятельно «выбраться» из этого круга.

Вопросы для команды:

1.Какая проблема описана в этом кейсе? Как алгоритмы рекомендаций влияют на поведение пользователя?

2.Можно ли считать цифровую зависимость угрозой? Если да, то почему?

3.Какие меры саморегуляции и защиты от манипуляций алгоритмами может предпринять Иван?

4.Какова роль государства и разработчиков платформ в борьбе с цифровой зависимостью и манипуляциями?

Материалы для учителя

Кейс 1: Фишинговое письмо (Email)

Сценарий:

Анна получает электронное письмо, которое выглядит как официальное сообщение от ее банка. В письме говорится о подозрительной активности на ее карте и необходимости срочно подтвердить личность, перейдя по ссылке.

От: Support Sber bank_support@mailer.com

Тема: ВАЖНО: Ваша карта будет заблокирована!

Уважаемый клиент! Наша система безопасности зафиксировала подозрительную активность с вашей карты. Для вашей же безопасности мы временно ограничили доступ. Чтобы избежать полной блокировки, вам нужно срочно подтвердить свою личность. Перейдите по ссылке ниже и войдите в свой личный кабинет. http://sberbank.auth-login.site/restore

С уважением, Служба безопасности Сбер.

Вопросы для команды:

1.Какая цифровая угроза описана в этом кейсе?

2.Какие признаки указывают на эту угрозу?

3.Какие действия должна предпринять Анна, чтобы защитить себя?

Разбор для учителя:

1.Какая цифровая угроза описана в этом кейсе? **Фишинг**

2.Какие признаки указывают на эту угрозу?

- **Адрес отправителя:** mailer.com — это общий почтовый домен, а не официальный домен банка. Настоящий банк использовал бы домен @sberbank.ru;
- **Общее обращение:** "Уважаемый клиент!" — мошенники не знают имени жертвы. Банк всегда обращается по имени и отчеству;
- **Ошибки:** "срочно" — крупные компании вычитывают свои рассылки;
- **Психологическое давление:** Угроза блокировки карты и призыв к срочности заставляют жертву паниковать и действовать необдуманно;
- **Поддельная ссылка:** Домен auth-login.site не имеет отношения к Сбербанку. Он имитирует официальный адрес.

3.Какие действия должна предпринять Анна, чтобы защитить себя?

- Не переходить по ссылке;
- Не вводить свои данные;
- Удалить письмо;

- Сообщить о подозрительном письме в банк (используя официальные контакты, а не те, что указаны в письме).

Кейс 2: Утечка данных через вредоносное ПО (приманка с выигрышем)

Сценарий:

Анастасия, ученица 10 класса, получает сообщение в социальной сети от аккаунта, который выглядит как официальная страница известного бренда электроники.

"Поздравляем! Вы покупали у нас наушники и стали одним из 100 победителей нашей акции. Вы получаете новый смартфон и 5000 рублей на счет! Для получения приза перейдите по ссылке и установите наше приложение для верификации: bit.ly/brand_prize_app".

Анастасия, обрадовавшись такому подарку, переходит по ссылке. Вместо страницы с информацией о призе, начинается автоматическая загрузка файла с расширением .apk (для Android) или .exe (для Windows), который называется "BrandPrizeVerifier.apk" или "BrandPrizeVerifier.exe". Она устанавливает это "приложение", не обратив внимания на запрошенные разрешения (доступ к контактам, SMS, галерее, микрофону). Через несколько дней Анастасия замечает, что с её банковской карты, привязанной к телефону, списываются небольшие суммы, а её друзья получают странные сообщения от её имени. Также она обнаруживает, что её личные фотографии и переписки из мессенджеров появились в открытом доступе на каком-то сомнительном сайте.

Вопросы для команды:

1. Какая цифровая угроза описана в этом кейсе?
2. Какие признаки указывают на эту угрозу и как она связана с первоначальной приманкой?
3. Какие действия должна предпринять Анастасия, чтобы защитить себя и свои данные?

Разбор для учителя:

1. Какая цифровая угроза описана в этом кейсе? **Утечка данных (через вредоносное ПО)**
2. Какие признаки указывают на эту угрозу и как она связана с первоначальной приманкой?

- **Утечка данных:** видимо в магазине произошла утечка данных о покупках Анны, сто и было использовано для вхождения в доверие;
- **Фишинговая приманка:** Сообщение о "выигрыше" и подозрительная ссылка bit.ly/brand_prize_app являются классическими признаками фишинга, целью которого было заставить пользователя установить вредоносное ПО;
- **Вредоносное ПО (Malware):** Файл .apk или .exe под видом "приложения для верификации" является вредоносной программой. После установки она получает несанкционированный доступ к данным на устройстве;
- **Необоснованные разрешения:** Запрос доступа к контактам, SMS, галерее, микрофону для "приложения для верификации" является крайне подозрительным и указывает на вредоносную активность;
- **Несанкционированные списания и рассылка сообщений:** Списание денег с карты и отправка сообщений друзьям от имени Анастасии — это прямые последствия работы вредоносного ПО, которое получило доступ к её финансовым данным и аккаунтам;

- **Публикация личных данных:** Появление фотографий и переписок в открытом доступе свидетельствует о том, что вредоносное ПО собрало и передало личные данные Анастасии злоумышленникам, что и является **утечкой данных**.

3. Какие действия должна предпринять Анастасия, чтобы защитить себя и свои данные?

- **Немедленно удалить вредоносное приложение** с устройства;
- **Отключить устройство от интернета** (Wi-Fi, мобильные данные), чтобы предотвратить дальнейшую передачу данных;
- **Сменить все пароли** от важных аккаунтов (банковские приложения, социальные сети, электронная почта) с другого, безопасного устройства (компьютера или телефона, который не был заражен);
- **Сообщить в банк** о несанкционированных списаниях и заблокировать карту;
- **Предупредить друзей** о том, что её аккаунт был скомпрометирован и не реагировать на странные сообщения от её имени;
- **Установить антивирусное ПО** на устройство и провести полное сканирование;
- **Обратиться за помощью к специалистам** по кибербезопасности или в сервисный центр;
- **В будущем быть крайне осторожной** с установкой приложений из неофициальных источников и всегда проверять запрашиваемые разрешения.

Кейс 3: Манипуляция информацией (вирусный фейк в соцсетях)

Сценарий:

Егор, ученик 9 класса, проводит много времени в TikTok и других социальных сетях. Однажды он натыкается на короткое видео, где некий "эксперт" с серьезным видом утверждает, что новый школьный предмет "Основы цифровой безопасности" на самом деле является скрытой программой для сбора данных о школьниках, а все их телефоны будут подключены к единой государственной системе слежки. Видео быстро набирает просмотры и комментарии, многие из которых выражают панику и возмущение. Егор, обеспокоенный этой информацией, начинает активно обсуждать это с одноклассниками, пересылать видео в школьные чаты. Он видит, что многие его друзья тоже верят этому видео, потому что "эксперт" выглядит убедительно, а в комментариях пишут, что это "правда, о которой молчат".

Вопросы для команды:

1. Какая цифровая угроза описана в этом кейсе?
2. Какие признаки указывают на эту угрозу?
3. Какие действия должен предпринять Егор, чтобы защитить себя и других от манипуляции?

Разбор для учителя:

1. Какая цифровая угроза описана в этом кейсе? **Манипуляция информацией (фейковые новости, дезинформация).**
2. Какие признаки указывают на эту угрозу?

- **Эмоциональный контент:** Видео вызывает сильные эмоции (страх, возмущение, паника) и затрагивает чувствительную тему (приватность, слежка);
- **Отсутствие официальных источников:** Информация исходит от анонимного "эксперта" в социальной сети, а не от официальных образовательных учреждений или проверенных СМИ;
- **Призывы к распространению и обсуждению:** Видео активно распространяется и обсуждается, создавая эффект "вирусности" и ложных договоренностей;
- **Использование авторитета ("эксперт"):** Мошенники часто используют псевдоэкспертов или людей, выглядящих авторитетно, чтобы придать своим словам вес;
- **Апелляция к конспирологическим теориям:** Утверждения о "скрытой программе" и "государственной системе слежки" характерны для дезинформации;
- **Комментарии, подтверждающие фейк:** Комментарии типа "правда, о которой молчат" создают иллюзию поддержки и достоверности.

3. Какие действия должен предпринять Егор, чтобы защитить себя и других от манипуляции?

- **Проверить информацию в официальных источниках:** обратиться к официальным сайтам Министерства образования, школы, учителям, чтобы узнать достоверную информацию о новом предмете, такого предмета вообще не существует;
- **Критически оценить источник:** задуматься, кто этот "эксперт", есть ли у него реальные полномочия и доказательства своих слов. Проверить его профиль;
- **Искать подтверждение в нескольких независимых и авторитетных источниках:** не доверять одному видео или сообщению;
- **Не поддаваться эмоциям:** помнить, что эмоционально заряженный контент часто используется для манипуляции;
- **Не распространять непроверенную информацию:** прежде чем делиться, убедиться в её достоверности;
- **Сообщить о фейковом контенте:** пожаловаться на видео администрации социальной сети, чтобы его удалили и предотвратили дальнейшее распространение дезинформации;
- **Обсудить ситуацию со взрослыми:** поговорить с родителями или учителями о своих опасениях и о том, как проверять информацию в интернете.

Кейс 4: Кибербуллинг (распространение слухов и социальная изоляция в групповом чате)

Сценарий:

Алина, ученица 9 класса, всегда была активной и общительной. Недавно она случайно услышала сплетню о своей однокласснице Лизе и, не придав этому значения, пересказала её в личном сообщении своей лучшей подруге. Однако подруга, вместо того чтобы сохранить секрет, переслала это сообщение в закрытый групповой чат класса, где состояли почти все ученики. Сплетня быстро разлетелась, и к ней добавились новые, искаженные подробности. В чате начали появляться унизительные мемы и оскорбительные комментарии в адрес Лизы. Лизу стали игнорировать в школе, не приглашать на общие мероприятия, а в чате её сообщения оставались без ответа или сопровождались насмешками. Лиза

чувствует себя абсолютно опустошенной, она боится ходить в школу, её успеваемость падает, и она перестала общаться даже с теми, кто раньше был её другом. Алина, увидев, к чему привела её неосторожность, чувствует вину, но боится вмешаться, опасаясь, что сама станет жертвой травли.

Вопросы для команды:

1. Какая цифровая угроза описана в этом кейсе и в чем её сложность по сравнению с прямыми оскорблениями?
2. Какие признаки указывают на эту угрозу и как она развивается?
3. Какие действия должна предпринять Лиза, чтобы защитить себя? Какие действия может предпринять Алина, чтобы исправить ситуацию, не подвергая себя риску?

Разбор для учителя:

1. Какая цифровая угроза описана в этом кейсе и в чем её сложность по сравнению с прямыми оскорблениями? **Кибербуллинг**, проявляющийся через **распространение слухов, социальную изоляцию и психологическое давление**. Сложность заключается в том, что это не прямые, однократные оскорбления, а целенаправленная, коллективная травля, которая затрагивает социальный статус жертвы и её психологическое состояние. Она начинается с, казалось бы, невинной сплетни, но быстро перерастает в организованную травлю.
2. Какие признаки указывают на эту угрозу и как она развивается?

- **Распространение слухов:** Началось с пересылки личного сообщения в групповой чат, что привело к быстрому распространению и искажению информации;
- **Социальная изоляция:** Лизу игнорируют в школе и в чате, не приглашают на мероприятия, что является формой исключения из коллектива;
- **Психологическое давление:** Унизительные мемы, оскорбительные комментарии и насмешки в чате создают постоянное негативное воздействие;
- **Коллективный характер:** В травле участвует не один человек, а группа, что усиливает её эффект и затрудняет противодействие;
- **Эмоциональное и академическое воздействие:** Лиза чувствует себя опустошенной, боится школы, её успеваемость падает, что свидетельствует о серьезном психологическом ущербе;
- **Чувство вины и страха у свидетеля:** Алина, как свидетель и невольный инициатор, испытывает вину, но боится действовать, что характерно для ситуаций кибербуллинга, где свидетели часто остаются пассивными из-за страха;

3. Какие действия должна предпринять Лиза, чтобы защитить себя? Какие действия может предпринять Алина, чтобы исправить ситуацию, не подвергая себя риску?

- **Действия Лизы:**
    - **Не отвечать агрессорам:** Любой ответ может быть использован против неё;
    - **Сохранить доказательства:** сделать скриншоты всех оскорбительных сообщений, мемов и фактов игнорирования в чате. Это критически важно;
    - **Покинуть групповой чат:** если это возможно и не приведет к дальнейшей эскалации, временно выйти из чата;
    - **Заблокировать отдельных обидчиков:** если травля исходит от конкретных лиц;

- **Рассказать взрослым:** немедленно обратиться за помощью к родителям, классному руководителю, школьному психологу или другому доверенному взрослому. Это самый важный шаг;
- **Не винить себя:** понять, что она не виновата в происходящем.

- **Действия Алины:**
  - **Поговорить с Лизой:** выразить сочувствие и поддержку, извиниться за свою неосторожность;
  - **Поговорить с доверенным взрослым:** рассказать родителям или учителю о ситуации, объяснить, что произошло, и попросить помощи для Лизы. Это можно сделать анонимно, если Алина боится прямой конфронтации;
  - **Не участвовать в травле:** не ставить лайки, не комментировать, не пересылать унизительный контент;
  - **Поддержать Лизу:** Если Алина чувствует в себе силы, она может публично или лично поддержать Лизу, показав, что не все в классе против неё. Это может быть сложно, но очень важно для жертвы;
  - **Попытаться остановить распространение:** если возможно, попросить других участников чата прекратить травлю, но делать это осторожно, чтобы не стать следующей жертвой;
  - **Помнить о своей ответственности:** понять, что даже невинная сплетня может иметь серьезные последствия в цифровой среде.

Кейс 5: Deepfake-видео и шантаж

Сценарий:

Мария, ученица 10 класса, получает в мессенджере сообщение от неизвестного номера. В сообщении прикреплено короткое видео, на котором она якобы произносит оскорбительные слова в адрес одноклассника и совершает непристойные действия. Видео выглядит очень реалистично. Отправитель требует крупную сумму денег, угрожая в противном случае распространить видео среди всех её контактов и выложить в интернет. Мария в панике, так как точно знает, что никогда ничего подобного не делала, но видео выглядит настолько убедительно, что она боится, что ей никто не поверит.

Вопросы для команды:

1.Какая цифровая угроза описана в этом кейсе? Какие технологии могли быть использованы для создания такого видео?

2.Какие признаки могут указывать на то, что видео является подделкой (deepfake)?

3.Какие правовые нормы нарушены в данной ситуации? (УК РФ, КоАП РФ)

4.Какие действия должна предпринять Мария, чтобы защитить себя и свои права? Куда ей следует обратиться за помощью?

Разбор для учителя

1. Какая цифровая угроза описана в этом кейсе? Какие технологии могли быть использованы для создания такого видео?

В данном кейсе описана угроза кибершантажа с использованием технологии дипфейк (deepfake). Для создания такого видео могли быть использованы нейронные сети и алгоритмы глубокого обучения, которые позволяют синтезировать или подменять человеческое лицо и голос на видео, делая подделку очень реалистичной.

2. Какие признаки могут указывать на то, что видео является подделкой (deepfake)?

Признаки подделки могут включать:

- Неестественная мимика: несоответствие движений губ произносимым словам, странное моргание или его отсутствие;
- Искажения на краях лица: размытость или артефакты в месте соединения лица с волосами или шеей;
- Странное освещение и тени: несоответствие освещения на лице общему освещению в видео;
- Синтетический голос: монотонность, странные интонации или акцент.

3. Какие правовые нормы нарушены в данной ситуации? (УК РФ, КоАП РФ)

- Статья 163 УК РФ «Вымогательство»: требование передачи чужого имущества (денег) под угрозой распространения сведений, позорящих потерпевшего;
- Статья 137 УК РФ «Нарушение неприкосновенности частной жизни»: незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия;
- Статья 128.1 УК РФ «Клевета»: распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию.

4. Какие действия должна предпринять Мария, чтобы защитить себя и свои права? Куда ей следует обратиться за помощью?

Марии следует:

- Не паниковать и не выполнять требования шантажиста;
- Сделать скриншоты переписки и сохранить видео в качестве доказательства;
- Рассказать о случившемся родителям или другим доверенным взрослым;
- Обратиться в полицию (МВД) с заявлением о вымогательстве и клевете;
- Сообщить о шантаже в службу поддержки мессенджера, чтобы заблокировать аккаунт злоумышленника.

Кейс 6: Фишинг через QR-код и поддельный сайт

Дмитрий, студент колледжа, видит на остановке общественного транспорта объявление о розыгрыше ценных призов от популярного онлайн-магазина электроники. Для участия нужно отсканировать QR-код и ввести свои данные на сайте. Дмитрий сканирует код, попадает на сайт, который выглядит идентично официальному сайту магазина, и вводит свои ФИО, номер телефона, а также данные банковской карты для «подтверждения участия». Через несколько минут ему приходит СМС о списании крупной суммы с его карты, а затем ещё одно – об оформлении микрозайма на его имя.

Вопросы для команды:

1.Какая цифровая угроза описана в этом кейсе? Как она связана с использованием QR-кода?

2.Какие признаки указывают на то, что сайт был поддельным (фишинговым)?

3.Какие статьи законодательства РФ нарушены действиями мошенников? (УК РФ)

4.Какие немедленные действия должен предпринять Дмитрий? Куда ему следует обратиться за помощью и как предотвратить подобные ситуации в будущем?

1. Какая цифровая угроза описана в этом кейсе? Как она связана с использованием QR-кода?

В кейсе описана угроза фишинга. QR-код в данном случае используется как средство доставки жертвы на поддельный (фишинговый) сайт, который имитирует официальный сайт магазина.

2. Какие признаки указывают на то, что сайт был поддельным (фишинговым)?

- URL-адрес: скорее всего, адрес сайта отличался от официального (например, sberbank.com вместо sberbank.ru);
- Отсутствие HTTPS: у фишинговых сайтов часто отсутствует защищенное соединение (замочек в адресной строке);
- Требование ввести данные карты для «подтверждения участия»: легитимные розыгрыши обычно не требуют ввода полных данных банковской карты.

3. Какие статьи законодательства РФ нарушены действиями мошенников? (УК РФ)

- •Статья 159.6 УК РФ «Мошенничество
    - в сфере компьютерной информации»: хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

4. Какие немедленные действия должен предпринять Дмитрий? Куда ему следует обратиться за помощью и как предотвратить подобные ситуации в будущем?

Дмитрию следует:

- Немедленно заблокировать банковскую карту, позвонив в банк;
- Обратиться в банк с заявлением о мошеннических операциях и оспорить списание средств;
- Обратиться в полицию (МВД) с заявлением о мошенничестве;
- Связаться с микрофинансовой организацией, чтобы выяснить ситуацию с займом и заявить о мошенничестве.

Чтобы избежать подобных ситуаций в будущем, следует проверять URL-адреса сайтов, на которые ведут QR-коды, и не вводить личные и банковские данные на подозрительных ресурсах.

Кейс 7: Кража биометрических данных и подмена личности

Сценарий:

Елена, активный пользователь социальных сетей, часто участвует в различных онлайн-челленджах. В одном из них нужно было записать короткое видео, где она произносит фразу «Я доверяю этому приложению» и загрузить его в специальное приложение для «улучшения голоса». Через некоторое время Елене начинают приходить уведомления о попытках входа в её банковское приложение с использованием голосовой аутентификации. А её друзья получают от неё голосовые сообщения с просьбами одолжить деньги, хотя Елена ничего подобного не отправляла

Вопросы для команды:

1.Какая цифровая угроза описана в этом кейсе? Что такое биометрические данные и почему их кража опасна?

2.Какие законы РФ регулируют сбор и использование биометрических данных? (ФЗ № 152-ФЗ)

3.Какие действия должна предпринять Елена, чтобы защитить свои данные и предотвратить дальнейшее использование её голоса?

4.Как можно было избежать этой ситуации? Какие меры предосторожности следует соблюдать при использовании приложений, запрашивающих доступ к биометрическим данным?

1. Какая цифровая угроза описана в этом кейсе? Что такое биометрические данные и почему их кража опасна?

Описана угроза кражи и незаконного использования биометрических данных. Биометрические данные — это уникальные физические или поведенческие характеристики человека (отпечатки пальцев, голос, лицо). Их кража опасна, так как они могут быть использованы для получения несанкционированного доступа к финансам, государственным услугам и другим важным системам, защищенным биометрической аутентификацией.

2. Какие законы РФ регулируют сбор и использование биометрических данных? (ФЗ № 152-ФЗ)

Сбор и использование биометрических данных регулируются Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». В частности, статья 11 этого закона устанавливает, что обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных.

3. Какие действия должна предпринять Елена, чтобы защитить свои данные и предотвратить дальнейшее использование её голоса?

Елене следует:

- Немедленно сменить пароли и отключить голосовую аутентификацию в банковском приложении и других сервисах;
- Связаться с банком и сообщить о попытках несанкционированного доступа;
- Предупредить друзей и знакомых о том, что ее голос может быть использован мошенниками;
- Обратиться в Роскомнадзор с жалобой на незаконную обработку ее биометрических данных.

4. Как можно было избежать этой ситуации? Какие меры предосторожности следует соблюдать при использовании приложений, запрашивающих доступ к биометрическим данным?

- Не участвовать в сомнительных онлайн-челленджах, требующих записи голоса или видео;
- Внимательно изучать политику конфиденциальности приложений, прежде чем предоставлять им доступ к камере или микрофону;
- Использовать биометрическую аутентификацию только в официальных и проверенных приложениях (банки, госуслуги).

Кейс 8: Цифровая зависимость и манипуляции через алгоритмы

Сценарий:

Иван, ученик 9 класса, начал замечать, что проводит всё больше времени в рекомендательных лентах социальных сетей и видеохостингов. Он заходит «на пять минут», чтобы посмотреть одно видео, но

алгоритмы постоянно предлагают ему новый, всё более увлекательный контент, и он не может остановиться. В итоге он проводит в сети по 4–5 часов в день, забывая о домашнем задании, спорте и общении с друзьями в реальной жизни. Его успеваемость падает, он чувствует постоянную усталость и раздражительность, но не может самостоятельно «выбраться» из этого круга.

Вопросы для команды:

1.Какая проблема описана в этом кейсе? Как алгоритмы рекомендаций влияют на поведение пользователя?

2.Можно ли считать цифровую зависимость угрозой? Если да, то почему?

3.Какие меры саморегуляции и защиты от манипуляций алгоритмами может предпринять Иван?

4.Какова роль государства и разработчиков платформ в борьбе с цифровой зависимостью и манипуляциями?

1. Какая проблема описана в этом кейсе? Как алгоритмы рекомендаций влияют на поведение пользователя?

В кейсе описана проблема цифровой зависимости. Алгоритмы рекомендаций создают «пузырь фильтров», подбирая контент, который с наибольшей вероятностью удержит пользователя на платформе. Это приводит к тому, что человек теряет контроль над временем, проведенным в сети.

2. Можно ли считать цифровую зависимость угрозой? Если да, то почему?

Да, цифровую зависимость можно считать угрозой, так как она негативно влияет на психическое и физическое здоровье человека, его социальные связи и успеваемость. Она может приводить к прокрастинации, снижению концентрации внимания, тревожности и депрессии.

3. Какие меры саморегуляции и защиты от манипуляций алгоритмами может предпринять Иван?

- Установить лимиты времени на использование приложений;
- Отключить уведомления от социальных сетей и видеохостингов;
- Сознательно разнообразить потребляемый контент, выходя за рамки рекомендаций;
- Найти хобби и занятия в реальной жизни, которые будут приносить удовольствие.

4. Какова роль государства и разработчиков платформ в борьбе с цифровой зависимостью и манипуляциями?

- Государство может вводить законодательные ограничения на использование манипулятивных практик в дизайне интерфейсов, а также поддерживать образовательные программы по цифровой гигиене.
- Разработчики платформ могут внедрять функции контроля времени, делать алгоритмы рекомендаций более прозрачными и предоставлять пользователям больше контроля над своей лентой.